



Guide de mise en œuvre

# Réponse de sécurité automatisée sur AWS



# Réponse de sécurité automatisée sur AWS: Guide de mise en œuvre

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

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

# Table of Contents

Présentation de la solution .....	1
Fonctionnalités et avantages .....	3
Cas d'utilisation .....	4
Concepts et définitions .....	4
Présentation de l'architecture .....	7
Diagramme d'architecture .....	7
AWS Considérations relatives à la conception de Well-Architected .....	9
Excellence opérationnelle .....	9
Sécurité .....	9
Fiabilité .....	10
Efficacité des performances .....	10
Optimisation des coûts .....	10
Durabilité .....	10
Détails de l'architecture .....	11
AWS Security Hub intégration .....	11
Assainissement entre comptes .....	11
Playbooks .....	12
Journalisation centralisée .....	12
Notifications .....	12
AWS services inclus dans cette solution .....	13
Planifiez votre déploiement .....	15
Coût .....	15
Exemple de tableau des coûts .....	15
Exemples de prix (mensuels) .....	20
Coût supplémentaire pour les fonctionnalités optionnelles .....	26
Sécurité .....	27
Rôles IAM .....	27
Soutenu Régions AWS .....	28
Quotas .....	29
Quotas pour AWS les services dans cette solution .....	30
AWS CloudFormation quotas .....	30
Amazon EventBridge réglemente les quotas .....	30
AWS Déploiement du Security Hub .....	30
Stack ou StackSets déploiement .....	31

Déployez la solution .....	32
Décider où déployer chaque stack .....	32
Décider de la manière de déployer chaque stack .....	34
Conclusions de contrôle consolidées .....	34
AWS CloudFormation modèles .....	35
Support pour les comptes d'administrateur .....	35
Comptes membres .....	36
Rôles des membres .....	36
Intégration du système de billetterie .....	37
Déploiement automatisé - StackSets .....	37
Prérequis .....	37
Vue d'ensemble du déploiement .....	38
(Facultatif) Étape 0 : Lancer une pile d'intégration d'un système de tickets .....	40
Étape 1 : Lancez la pile d'administration dans le compte d'administrateur délégué du Security Hub .....	42
Étape 2 : Installation des rôles de correction dans chaque compte membre du AWS Security Hub .....	43
Étape 3 : Lancez la pile de membres dans chaque compte membre et région du AWS Security Hub .....	44
Déploiement automatisé - Stacks .....	46
Prérequis .....	46
Vue d'ensemble du déploiement .....	46
(Facultatif) Étape 0 : Lancer une pile d'intégration d'un système de tickets .....	47
Étape 1 : Lancez la pile d'administration .....	49
Étape 2 : Installation des rôles de correction dans chaque compte membre du AWS Security Hub .....	55
Étape 3 : Lancez la pile de membres .....	56
Étape 4 : (Facultatif) Ajustez les mesures correctives disponibles .....	60
Surveillez la solution avec Service Catalog AppRegistry .....	62
Utiliser CloudWatch Application Insights .....	63
Confirmez les étiquettes de coût associées à la solution .....	64
Activer les balises de répartition des coûts associées à la solution .....	64
AWS Cost Explorer .....	65
Surveillez les opérations de la solution à l'aide d'un CloudWatch tableau de bord Amazon .....	66
Activation CloudWatch des métriques, des alarmes et du tableau de bord .....	66
Utilisation du CloudWatch tableau de bord .....	67

Modification des seuils d'alarme .....	69
Abonnement aux notifications d'alarme .....	71
Mettre à jour la solution .....	72
Mise à niveau à partir de versions antérieures à la v1.4 .....	72
Mise à niveau depuis la version 1.4 et les versions ultérieures .....	72
Mise à niveau depuis la version 2.0.x .....	72
Résolution des problèmes .....	73
Journaux de solutions .....	73
Résolution des problèmes connus .....	74
Problèmes liés à des mesures correctives spécifiques .....	77
PuTS3 échoue BucketPolicyDeny .....	77
Comment désactiver la solution .....	78
Contacter AWS Support .....	79
Créer un dossier .....	79
Comment pouvons-nous vous aider ? .....	79
Informations supplémentaires .....	79
Aidez-nous à résoudre votre cas plus rapidement .....	79
Résolvez maintenant ou contactez-nous .....	80
Désinstallez la solution .....	81
V1.0.0-V1.2.1 .....	81
V1.3.x .....	81
V1.4.0 et versions ultérieures .....	82
Guide de l'administrateur .....	83
Activation et désactivation de certaines parties de la solution .....	83
Exemples de SNS notifications .....	84
Utilisez la solution .....	87
Commencer à utiliser Automated Security Response sur AWS .....	87
Préparez les comptes .....	87
Activer AWS Config .....	88
Activer le hub AWS de sécurité .....	88
Permettre des résultats de contrôle consolidés .....	89
Configuration de l'agrégation de recherche entre régions .....	90
Désignez un compte administrateur Security Hub .....	90
Création des rôles pour les autorisations autogérées StackSets .....	91
Créez les ressources non sécurisées qui généreront des exemples de résultats .....	92
Création de groupes de CloudWatch journaux pour les contrôles associés .....	93

Déployer la solution sur des comptes de didacticiel .....	94
Déployer la pile d'administration .....	94
Déployer la pile de membres .....	94
Déployer la pile de rôles des membres .....	95
Abonnez-vous au SNS sujet .....	96
Corriger les résultats des exemples .....	96
Lancer la correction .....	97
Confirmez que la correction a résolu le problème .....	97
Suivez l'exécution de la remédiation .....	98
EventBridge règle .....	98
Step Functions : exécution .....	98
SSM Automation .....	98
CloudWatch Groupe de journaux .....	98
Activez des mesures correctives entièrement automatisées .....	98
Vérifiez que vous ne disposez d'aucune ressource à laquelle cette constatation peut s'appliquer accidentellement .....	99
Activer la règle .....	99
Configuration de la ressource .....	100
Confirmez que la correction a résolu le problème .....	97
Nettoyage .....	101
Supprimer les exemples de ressources .....	101
Supprimer la pile d'administrateurs .....	101
Supprimer la pile de membres .....	101
Supprimer la pile de rôles des membres .....	102
Supprimer les rôles conservés .....	102
Planifier la suppression KMS des clés conservées .....	103
Supprimer les piles pour les autorisations autogérées StackSets .....	103
Manuel du développeur .....	105
Code source .....	105
Playbooks .....	105
Ajouter de nouvelles mesures correctives .....	176
Présentation .....	177
Étape 1. Créez un runbook sur le (s) compte (s) membre (s) .....	177
Étape 2. Créez un IAM rôle dans le (s) compte (s) membre (s) .....	177
Étape 3 : (Facultatif) Créez une règle de correction automatique dans le compte administrateur .....	178

---

Ajouter un nouveau playbook .....	178
AWS Systems Manager Magasin de paramètres .....	179
SNSsujet - Progrès de la remédiation .....	180
Filtrage et abonnement à un SNS sujet .....	180
SNSRubrique Amazon — CloudWatch Alarmes .....	181
Lancer Runbook sur la base des résultats de configuration .....	182
Référence .....	183
Collecte de données anonymisée .....	183
Ressources connexes .....	184
Collaborateurs .....	185
Révisions .....	186
Avis .....	191
.....	cxcii

# Gérez automatiquement les menaces de sécurité grâce à des actions de réponse et de correction prédéfinies dans AWS Security Hub

Date de publication : août 2020 ([dernière mise à jour](#) : décembre 2024)

Ce guide de mise en œuvre fournit une vue d'ensemble de la réponse de sécurité automatisée sur la AWS solution, de son architecture de référence et de ses composants, des considérations relatives à la planification du déploiement, des étapes de configuration pour le déploiement de la réponse de sécurité automatisée sur AWS le cloud Amazon Web Services (AWS).

Utilisez ce tableau de navigation pour trouver rapidement les réponses aux questions suivantes :

Si tu veux...	Lisez.
Connaître le coût de fonctionnement de cette solution	<a href="#">Coût</a>
Comprendre les considérations de sécurité liées à cette solution	<a href="#">Sécurité</a>
Savoir comment planifier les quotas pour cette solution	<a href="#">Quotas</a>
Découvrez quelles AWS régions sont prises en charge pour cette solution	<a href="#">AWS Régions prises en charge</a>
Consultez ou téléchargez le AWS CloudFormation modèle inclus dans cette solution pour déployer automatiquement les ressources d'infrastructure (la « pile ») de cette solution	Modèles <a href="#">AWS CloudFormation</a>
Accédez au code source et utilisez éventuellement le AWS Cloud Development Kit (AWSCDK) pour déployer la solution.	<a href="#">GitHub référentiel</a>

L'évolution continue de la sécurité nécessite des mesures proactives pour sécuriser les données, ce qui peut rendre la réaction des équipes de sécurité difficile, coûteuse et chronophage. La AWS solution Automated Security Response on vous aide à réagir rapidement pour résoudre les problèmes de sécurité en fournissant des réponses prédéfinies et des actions correctives basées sur les normes de conformité du secteur et les meilleures pratiques.

[Automated Security AWS Response on est une AWS solution qui permet d'AWS Security Hub améliorer votre sécurité et d'aligner vos charges de travail sur les meilleures pratiques du pilier de sécurité Well-Architected \(0\). SEC1](#) Cette solution permet AWS Security Hub aux clients de résoudre plus facilement les problèmes de sécurité courants et d'améliorer leur niveau de sécurité AWS.

Vous pouvez sélectionner des playbooks spécifiques à déployer sur votre compte principal Security Hub. Chaque playbook contient les actions personnalisées nécessaires, les rôles [Identity and Access Management](#) (IAM), les [EventBridge règles Amazon](#), les documents d'automatisation de [AWS Systems Manager](#), les [AWS Lambda](#) fonctions et les éléments [AWS Step Functions](#) nécessaires pour démarrer un flux de travail de correction au sein d'un seul AWS compte ou sur plusieurs comptes. Les correctifs fonctionnent à partir du menu Actions AWS Security Hub et permettent aux utilisateurs autorisés de corriger une découverte concernant l'ensemble de leurs comptes AWS Security Hub gérés en une seule action. Par exemple, vous pouvez appliquer les recommandations du Center for Internet Security (CIS) AWS Foundations Benchmark, une norme de conformité pour la sécurisation des AWS ressources, afin de garantir que les mots de passe expirent dans les 90 jours et d'appliquer le chiffrement des journaux d'événements qui y sont stockés AWS.

#### Note

Les mesures correctives sont destinées aux situations d'urgence qui nécessitent une action immédiate. Cette solution apporte des modifications pour corriger les résultats uniquement lorsque vous l'avez initiée via la console de AWS Security Hub gestion, ou lorsque la correction automatique a été activée à l'aide de la EventBridge règle Amazon pour un contrôle spécifique. Pour annuler ces modifications, vous devez remettre manuellement les ressources dans leur état d'origine.

Lorsque vous corrigez AWS des ressources déployées dans le cadre de la CloudFormation pile, sachez que cela peut provoquer une dérive. Dans la mesure du possible, corrigez les ressources de la pile en modifiant le code qui définit les ressources de la pile et en mettant à jour la pile. Pour plus d'informations, reportez-vous à [Qu'est-ce que la dérive ?](#) dans le guide de AWS CloudFormation l'utilisateur.

Automated Security Response on AWS inclut les correctifs relatifs aux normes de sécurité définies dans le cadre des règles de sécurité suivantes :

- [Center for Internet Security \(CIS\) AWS Foundations Benchmark v1.2.0](#)

- [CISAWSFoundations Benchmark v1.4.0](#)
- [CISAWSFoundations Benchmark v3.0.0](#)
- [AWSBonnes pratiques de sécurité fondamentales \(FSBP\) v.1.0.0](#)
- [Norme de sécurité des données de l'industrie des cartes de paiement \(PCI-DSS\) v3.2.1](#)
- [Institut national des normes et de la technologie \(NIST\) SP 800-53 Rev. 5](#)

La solution inclut également un manuel de contrôle de sécurité (SC) pour la [fonctionnalité de consolidation des résultats de contrôle](#) de AWS Security Hub. Pour plus d'informations, reportez-vous à [Playbooks](#).

Ce guide de mise en œuvre aborde les considérations architecturales et les étapes de configuration pour déployer la AWS solution Automated Security Response on dans le AWS cloud. Il inclut des liens vers des [AWS CloudFormation](#) modèles qui lancent, configurent et exécutent les services de AWS calcul, de réseau, de stockage et autres nécessaires au déploiement de cette solution AWS, en utilisant les AWS meilleures pratiques en matière de sécurité et de disponibilité.

Le guide est destiné aux architectes d'infrastructures informatiques, aux administrateurs et aux DevOps professionnels ayant une expérience pratique de l'architecture dans le AWS cloud.

## Fonctionnalités et avantages

La réponse de sécurité automatisée activée AWS fournit les fonctionnalités suivantes :

Corriger automatiquement les résultats pour des contrôles spécifiques

Activez EventBridge les règles Amazon pour les contrôles afin de corriger automatiquement les résultats relatifs à ce contrôle immédiatement après leur apparition dans AWS Security Hub.

Gérez les mesures correctives sur plusieurs comptes et régions à partir d'un seul emplacement

À partir d'un compte administrateur AWS Security Hub configuré comme destination d'agrégation pour les comptes et les régions de votre organisation, lancez une correction en cas de recherche dans tous les comptes et régions dans lesquels la solution est déployée.

Soyez informé des mesures correctives et des résultats

Abonnez-vous à la SNS rubrique Amazon déployée par la solution pour être averti lorsque des corrections sont initiées et si elles ont réussi ou non.

## Intégrez des systèmes de tickets tels que Jira ou ServiceNow

Pour aider votre organisation à réagir aux mesures correctives (par exemple, en mettant à jour le code de votre infrastructure), cette solution peut envoyer des tickets vers votre système de billetterie externe.

## Utilisation AWSConfigRemediations dans les partitions GovCloud et Chine

Certaines des mesures correctives incluses dans la solution sont des repackages de AWSConfigRemediation documents AWS détenus qui sont disponibles sur la partition commerciale, mais pas en Chine ou GovCloud en Chine. Déployez cette solution pour utiliser ces documents dans ces partitions.

## Étendez la solution avec des correctifs personnalisés et des implémentations de Playbook

La solution est conçue pour être extensible et personnalisable. Pour spécifier une implémentation alternative de correction, déployez des documents et des AWS IAM rôles d'automatisation personnalisés de AWS Systems Manager. Pour prendre en charge un tout nouvel ensemble de contrôles qui n'est pas implémenté par la solution, déployez un Playbook personnalisé.

## Cas d'utilisation

Appliquez la conformité à une norme dans tous les comptes et régions de votre organisation

Déployez le Playbook pour une norme (par exemple, les meilleures pratiques de sécurité AWS fondamentales) afin de pouvoir utiliser les correctifs fournis. Lancez automatiquement ou manuellement des mesures correctives pour les ressources de tous les comptes et régions dans lesquels la solution est déployée afin de corriger les ressources non conformes.

Déployez des correctifs personnalisés ou des Playbooks pour répondre aux besoins de conformité de votre entreprise

Utilisez les composants d'Orchestrator fournis comme framework. Créez des solutions personnalisées pour gérer les out-of-compliance ressources en fonction des besoins spécifiques de votre organisation.

## Concepts et définitions

Cette section décrit les concepts clés et définit la terminologie spécifique à cette solution :

## application

Groupe logique de AWS ressources que vous souhaitez exploiter en tant qu'unité.

## remédiation, manuel de remédiation

Implémentation d'un ensemble d'étapes permettant de résoudre une constatation. Par exemple, une correction pour le contrôle Security Control (SC) Lambda.1 « Les politiques relatives aux fonctions Lambda doivent interdire l'accès public » modifierait la politique de la fonction AWS Lambda concernée afin de supprimer les instructions autorisant l'accès public.

## runbook de contrôle

L'un des documents d'automatisation de AWS Systems Manager (SSM) que l'orchestrateur utilise pour acheminer une correction initiée pour un contrôle spécifique vers le manuel de correction approprié. Par exemple, les correctifs pour SC Lambda.1 et AWS Foundational Security Best Practices (FSBP) Lambda.1 sont mis en œuvre avec le même manuel de correction. L'orchestrateur appelle le runbook de contrôle pour chaque contrôle, nommés respectivement `_Lambda.1` et `ASR AFSBP -SC_2.0.0_Lambda.1`. ASR Chaque runbook de contrôle invoque le même runbook de correction, qui dans ce cas serait `- ASR RemoveLambdaPublicAccess`

## orchestrateur

Les Step Functions déployées par la solution qui prend en entrée un objet de recherche provenant de AWS Security Hub et invoque le manuel de contrôle approprié dans le compte et la région cibles. L'orchestrateur informe également le SNS sujet de la solution lorsque la correction est lancée et lorsque la correction réussit ou échoue.

## norme

Groupe de contrôles défini par une organisation dans le cadre d'un cadre de conformité. Par exemple, l'une des normes prises en charge par AWS Security Hub et cette solution est AWSFSBP.

## contrôle

Description des propriétés qu'une ressource doit ou ne doit pas posséder pour être conforme. Par exemple, le contrôle AWS FSBP Lambda.1 indique que les fonctions AWS Lambda doivent interdire l'accès public. Une fonction autorisant l'accès public échouerait à ce contrôle.

## résultats de contrôle consolidés, contrôle de sécurité, vue des contrôles de sécurité

Fonctionnalité de AWS Security Hub qui, lorsqu'elle est activée, affiche les résultats avec leur contrôle consolidé IDs plutôt IDs que ceux correspondant à une norme particulière. Par exemple, les contrôles AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 et PCI - DSS v3.2.1 S3.1 correspondent tous au contrôle consolidé (SC) S3.2 « Les compartiments S3 devraient interdire l'accès public en lecture ». Lorsque cette fonctionnalité est activée, les runbooks SC sont utilisés.

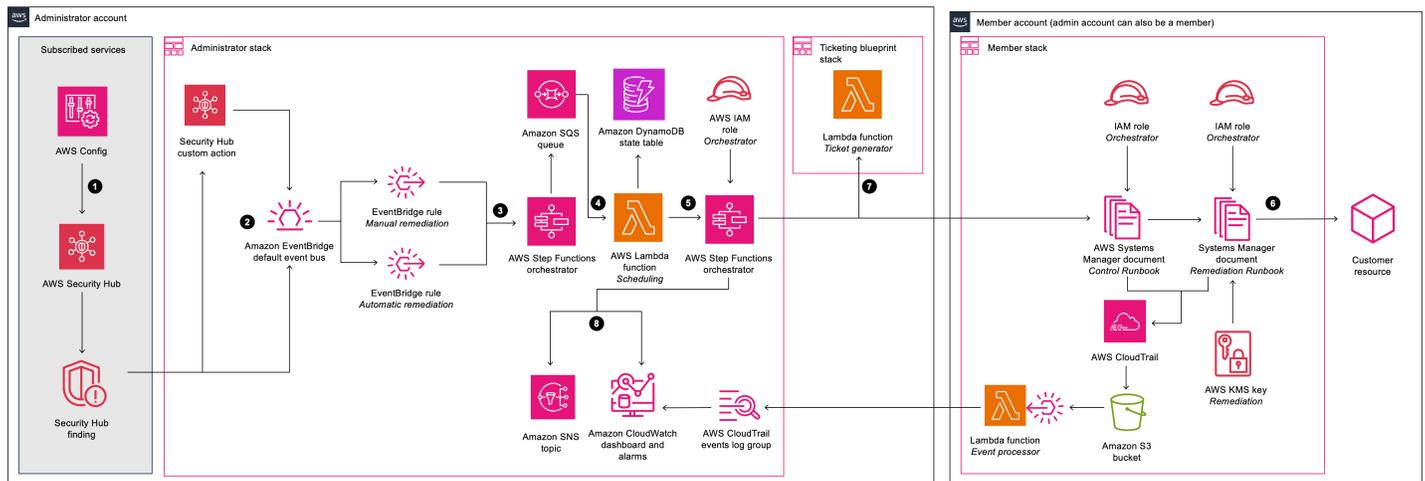
Pour une référence générale des AWS termes, reportez-vous au [AWS glossaire](#).

# Présentation de l'architecture

Cette section fournit un schéma d'architecture d'implémentation de référence pour les composants déployés avec cette solution.

## Diagramme d'architecture

Le déploiement de cette solution avec les paramètres par défaut permet de créer l'environnement suivant dans le AWS cloud.



## Réponse de sécurité automatisée sur AWS l'architecture

### Note

AWS CloudFormation les ressources sont créées à partir des constructions du AWS Cloud Development Kit (AWSCDK).

Le flux de processus de haut niveau pour les composants de solution déployés avec le AWS CloudFormation modèle est le suivant :

1. Détecter : [AWS Security Hub](#) fournit aux clients une vue complète de leur état AWS de sécurité. Cela les aide à mesurer leur environnement par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Il fonctionne en collectant des événements et des données provenant d'autres AWS services AWS Config, tels qu'Amazon Guard Duty et AWS Firewall Manager. Ces événements et données sont analysés par rapport aux normes de sécurité, telles que

CIS AWS Foundations Benchmark. Les exceptions sont indiquées sous forme de résultats dans la AWS Security Hub console. Les nouvelles découvertes sont envoyées sous forme [d'EventBridge événements Amazon](#).

2. Initier : vous pouvez lancer des événements en fonction des résultats à l'aide d'actions personnalisées, qui se traduisent par EventBridge des événements. AWS Security Hub [des actions et des EventBridge règles personnalisées](#) déclenchent une réponse de sécurité automatisée sur les AWS playbooks pour répondre aux résultats. La solution déploie :
  - a. Une EventBridge règle correspondant à l'événement d'action personnalisé
  - b. Une règle EventBridge d'événement pour chaque contrôle pris en charge (désactivée par défaut) correspondant à l'événement de recherche en temps réel

Vous pouvez utiliser le menu Actions personnalisées de la console Security Hub pour lancer une correction automatique. Après des tests approfondis dans un environnement hors production, vous pouvez également activer les corrections automatisées. Vous pouvez activer les automatisations pour des corrections individuelles. Il n'est pas nécessaire d'activer les initiations automatiques pour toutes les corrections.

3. Pré-correction : dans le compte administrateur, [AWS Step Function](#) traite l'événement de correction et le prépare à être planifié.
4. Planification : La solution invoque la [AWS Lambda](#) fonction de planification pour placer l'événement de correction dans la table d'état d'[Amazon DynamoDB](#).
5. Orchestrate : dans le compte administrateur, Step Functions utilise des rôles inter-comptes [AWS Identity and Access Management](#) (IAM). Step Functions invoque la correction dans le compte membre contenant la ressource à l'origine de la constatation de sécurité.
6. Corriger : un [document d'AWS Systems Manager automatisation](#) du compte membre exécute l'action requise pour corriger la découverte sur la ressource cible, telle que la désactivation de l'accès public à Lambda.

Vous pouvez éventuellement activer la fonctionnalité Action Log dans les piles de membres à l'aide du `EnableCloudTrailForASRActionLog` paramètre. Cette fonctionnalité capture les actions entreprises par la solution dans vos comptes de membres et les affiche dans le tableau de CloudWatch bord [Amazon](#) de la solution.

7. (Facultatif) Créez un ticket : si vous utilisez le `TicketGenFunctionName` paramètre pour activer la billetterie dans la pile d'administration, la solution invoque la fonction Lambda du générateur de tickets fournie. Cette fonction Lambda crée un ticket dans votre service de billetterie une fois que la correction a été exécutée avec succès dans le compte du membre. Nous fournissons des [piles pour l'intégration avec Jira](#) et ServiceNow

8. Notifier et consigner : le playbook enregistre les résultats dans un CloudWatch [groupe de journaux](#), envoie une notification à une rubrique [Amazon Simple Notification Service](#) (AmazonSNS) et met à jour la découverte du Security Hub. La solution conserve une piste d'audit des actions figurant dans les [notes de constatation](#).

## AWSConsidérations relatives à la conception de Well-Architected

Cette solution a été conçue selon les meilleures pratiques du AWS Well-Architected Framework, qui aide les clients à concevoir et à exploiter des charges de travail fiables, sécurisées, efficaces et rentables dans le cloud. Cette section décrit comment les principes de conception et les meilleures pratiques du Well-Architected Framework ont été appliqués lors de la création de cette solution.

### Excellence opérationnelle

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de l'excellence opérationnelle](#).

- Ressources définies comme utilisant IaC CloudFormation.
- Mesures correctives mises en œuvre avec les caractéristiques suivantes, dans la mesure du possible :
  - Idempotence
  - Gestion des erreurs et signalement
  - Journalisation
  - Restaurer les ressources à un état connu en cas de défaillance

### Sécurité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de sécurité](#).

- IAM utilisé pour l'authentification et l'autorisation.
- Les autorisations de rôle ont été définies de manière à être aussi limitées que possible, bien que dans de nombreux cas, cette solution nécessite des autorisations génériques pour pouvoir agir sur toutes les ressources.

## Fiabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de fiabilité](#).

- Security Hub continue de créer des résultats si la cause sous-jacente du résultat n'est pas résolue par la correction.
- Les services sans serveur permettent à la solution d'évoluer selon les besoins.

## Efficacité des performances

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier de l'efficacité des performances](#).

- Cette solution a été conçue pour être une plate-forme que vous pouvez étendre sans avoir à implémenter vous-même l'orchestration et les autorisations.

## Optimisation des coûts

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier d'optimisation des coûts](#).

- Les services sans serveur vous permettent de payer uniquement pour ce que vous utilisez.
- Utilisez le niveau gratuit pour SSM automatiser chaque compte

## Durabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du [pilier du développement durable](#).

- Les services sans serveur vous permettent d'augmenter ou de diminuer selon vos besoins.

## Détails de l'architecture

Cette section décrit les composants et les AWS services qui constituent cette solution ainsi que les détails de l'architecture sur la manière dont ces composants fonctionnent ensemble.

### AWS Security Hub intégration

Le déploiement de la `aws-sharr-deploy` pile crée une intégration avec AWS la fonctionnalité d'action personnalisée de Security Hub. Lorsque les utilisateurs de AWS Security Hub la console sélectionnent Résultats pour la correction, la solution achemine l'enregistrement des résultats à des fins de correction à l'aide d'un. AWS Step Functions

Les autorisations entre comptes et les AWS Systems Manager runbooks doivent être déployés sur tous les AWS Security Hub comptes (administrateur et membre) à l'aide des modèles `aws-sharr-member.template` et `aws-sharr-member-roles.template` CloudFormation. Pour plus d'informations, reportez-vous à [Playbooks](#). Ce modèle permet une correction automatique dans le compte cible.

Les utilisateurs peuvent lancer automatiquement des mesures correctives automatisées au cas par cas en utilisant les règles d'Amazon CloudWatch Events. Cette option active la correction entièrement automatique des résultats dès qu'ils sont signalés. AWS Security Hub Par défaut, les initiations automatiques sont désactivées. Cette option peut être modifiée à tout moment pendant ou après l'installation du playbook en activant les règles relatives aux CloudWatch événements dans le compte AWS Security Hub administrateur.

### Assainissement entre comptes

Automated Security Response on AWS utilise des rôles entre comptes pour travailler sur des comptes principaux et secondaires à l'aide de rôles entre comptes. Ces rôles sont déployés sur les comptes des membres lors de l'installation de la solution. Un rôle individuel est attribué à chaque correction. Le processus de correction dans le compte principal est autorisé à assumer le rôle de correction dans le compte qui nécessite une correction. La correction est effectuée par AWS les runbooks Systems Manager exécutés sur le compte qui nécessite une correction.

# Playbooks

Un ensemble de mesures correctives est regroupé dans un package appelé playbook. Les playbooks sont installés, mis à jour et supprimés à l'aide des modèles de cette solution. Pour plus d'informations sur les corrections prises en charge dans chaque playbook, reportez-vous au [Guide du développeur - > Playbooks](#). Cette solution prend actuellement en charge les playbooks suivants :

- Security Control, un manuel aligné sur la fonctionnalité Consolidated Control findings de AWS Security Hub, publié le 23 février 2023.

## Important

Lorsque [les résultats de contrôle consolidés](#) sont activés dans Security Hub, il s'agit du seul playbook qui doit être activé dans la solution.

- [Center for Internet Security \(CIS\) Benchmarks d'Amazon Web Services Foundations, version 1.2.0](#), publiés le 18 mai 2018.
- [Center for Internet Security \(CIS\) Benchmarks d'Amazon Web Services Foundations, version 1.4.0](#), publiés le 9 novembre 2022.
- [Center for Internet Security \(CIS\) Benchmarks d'Amazon Web Services Foundations, version 3.0.0](#), publiés le 13 mai 2024.
- [AWS Foundational Security Best Practices \(FSBP\) version 1.0.0](#), publiée en mars 2021.
- [Normes de sécurité des données de l'industrie des cartes de paiement \(PCI-DSS\) version 3.2.1](#), publiées en mai 2018.
- [National Institute of Standards and Technology \(NIST\) version 5.0.0](#), publiée en novembre 2023.

## Journalisation centralisée

Réponse de sécurité automatisée sur AWS les journaux à un seul groupe de CloudWatch journaux, SO0111-. SHARR Ces journaux contiennent une journalisation détaillée de la solution pour le dépannage et la gestion de la solution.

## Notifications

Cette solution utilise une rubrique Amazon Simple Notification Service (AmazonSNS) pour publier les résultats des mesures correctives. Vous pouvez utiliser les abonnements à cette rubrique pour

étendre les fonctionnalités de la solution. Par exemple, vous pouvez envoyer des notifications par e-mail et mettre à jour les tickets d'incident.

## AWSservices inclus dans cette solution

La solution utilise les services suivants. Les services de base sont nécessaires pour utiliser la solution, et les services de support connectent les services principaux.

AWS service	Description
<a href="#">Amazon EventBridge</a>	Noyau. Déploie des événements qui lanceront la fonction d'étape d'orchestration lors de la correction d'un résultat.
<a href="#">AWS IAM</a>	Noyau. Déploie de nombreux rôles pour permettre des corrections sur différentes ressources.
<a href="#">AWS Lambda</a>	Noyau. Déploie plusieurs fonctions lambda qui seront utilisées par l'orchestrateur de fonctions par étapes pour résoudre les problèmes.
<a href="#">AWS Security Hub</a>	Noyau. Fournit aux clients une vue complète de leur état AWS de sécurité.
<a href="#">AWS Step Functions</a>	Noyau. Déploie un orchestrateur qui invoquera les documents de correction par le biais d'appels AWS Systems Manager. API
<a href="#">AWS Systems Manager</a>	Noyau. Déploie les documents System Manager (lien vers le document) qui contiennent la logique de correction qui sera exécutée.
<a href="#">AWS CloudTrail</a>	Soutenir. Enregistre les modifications apportées par la solution à vos AWS ressources et les affiche sur un CloudWatch tableau de bord.

AWS service	Description
<a href="#">Amazon CloudWatch</a>	Soutenir. Déploie des groupes de journaux que les différents playbooks utiliseront pour enregistrer les résultats. Collecte des métriques à afficher sur un tableau de bord personnalisé avec des alarmes.
<a href="#">AWS DynamoDB</a>	Soutenir. Stocke la dernière correction exécutée dans chaque compte et région afin d'optimiser la planification des corrections.
<a href="#">Service Catalog AppRegistry</a>	Soutenir. Déploie une application pour les piles déployées afin de suivre les coûts et l'utilisation.
<a href="#">Amazon Simple Notification Service</a>	Soutenir. Déploie SNS les sujets qui reçoivent une notification une fois qu'une correction est terminée.
<a href="#">AWS SQS</a>	Soutenir. Aide à planifier les mesures correctives afin que la solution puisse les exécuter en parallèle.

# Planifiez votre déploiement

Cette section décrit le coût, la sécurité du réseau, le support Régions AWS, les quotas et d'autres considérations avant le déploiement de la solution.

## Coût

Vous êtes responsable du coût des AWS services utilisés pour exécuter cette solution. À partir de cette révision, le coût d'exécution de cette solution avec les paramètres par défaut dans l'est des États-Unis (Virginie du Nord) Région AWS est d'environ 21,17\$ pour 300 corrections par mois, 134,86\$ pour 3 000 mesures correctives par mois et 1 281,01\$ pour 30 000 mesures correctives par mois. Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page de tarification de chaque AWS service utilisé dans cette solution.

### Note

De nombreux AWS services incluent un niveau gratuit, c'est-à-dire une quantité de base du service que les clients peuvent utiliser gratuitement. Les coûts réels peuvent être supérieurs ou inférieurs aux exemples de prix fournis.

Nous vous recommandons de créer un [budget](#) AWS Cost Explorer pour aider à gérer les coûts. Les prix sont susceptibles d'être modifiés. Pour plus de détails, consultez la page Web de tarification de chaque AWS service utilisé dans cette solution.

## Exemple de tableau des coûts

Le coût total d'exécution de cette solution dépend des facteurs suivants :

- Le nombre de comptes de AWS Security Hub membres
- Le nombre de mesures correctives actives invoquées automatiquement
- La fréquence des mesures correctives

Cette solution utilise les AWS composants suivants, dont le coût dépend de votre configuration. Des exemples de tarification sont fournis pour les petites, moyennes et grandes entreprises.

Service	Niveau gratuit	Tarification [USD]
<a href="#">AWS Systems Manager Automation - Nombre d'étapes</a>	100 000 étapes par compte et par mois	Au-delà du niveau gratuit, chaque étape de base est facturée à 0,002\$ par étape. Pour les automatisations multi-comptes, toutes les étapes, y compris celles exécutées sur les comptes enfants, sont comptabilisées uniquement dans le compte d'origine.
<a href="#">AWS Systems Manager Automation - Durée de l'étape</a>	5 000 secondes par mois	Au-delà du niveau gratuit, chaque étape executeScript d'aws : action est facturée à 0,00003\$ par seconde après un niveau gratuit de 5 000 secondes par mois.
<a href="#">AWS Systems Manager Automation - Stockage</a>	Pas de niveau gratuit	0,046\$ par Go par mois
<a href="#">AWS Systems Manager Automation - Transfert de données</a>	Pas de niveau gratuit	0,900\$ par Go transféré (pour plusieurs comptes ou) out-of-Region
<a href="#">AWS Security Hub - Contrôles de sécurité</a>	Pas de niveau gratuit	<p>checks/account/Region/month Les 100 000 premiers coûtent 0,0010\$ par chèque</p> <p>Les 400 000 dollars suivants checks/account/Region/month coûtent 0,0008\$ par chèque</p> <p>Plus de 500 000 dollars checks/account/Region/month coûtent 0,0005\$ par chèque</p>

Service	Niveau gratuit	Tarification [USD]
<a href="#">AWS Security Hub - Détecter les événements liés à l'ingestion</a>	Les 10 000 premiers events/account/Region/month sont gratuits. Recherche d'événements d'ingestion associés aux contrôles de sécurité de Security Hub.	Plus de 10 000 dollars events/account/Region/month coûtent 0,00003\$ par événement
<a href="#">Amazon CloudWatch - Métriques</a>	Mesures de surveillance de base (à une fréquence de 5 minutes) 10 mesures de surveillance détaillées (à une fréquence d'une minute) 1 million de API demandes (non applicable à GetMetricData et GetMetricWidgetImage)	Les 10 000 premiers indicateurs coûtent 0,30\$ par mois  Les 240 000 métriques suivantes coûtent 0,10\$ métrique/mois  Les 750 000 métriques suivantes coûtent 0,05\$ par mois  Plus de 1 000 000 métriques coûtent 0,02\$ par mois  API les appels coûtent 0,01\$ pour 1 000 demandes
<a href="#">Amazon CloudWatch - Tableau de bord</a>	3 tableaux de bord pour un maximum de 50 indicateurs par mois	3,00\$ par tableau de bord par mois

Service	Niveau gratuit	Tarification [USD]
<a href="#">Amazon CloudWatch - Alarmes</a>	10 mesures d'alarme (ne s'applique pas aux alarmes haute résolution)	<p>La résolution standard (60 secondes) coûte 0,10\$ par alarme-métrique</p> <p>La haute résolution (10 secondes) coûte 0,30\$ par métrique d'alarme</p> <p>La détection des anomalies à résolution standard coûte 0,30\$ par alarme</p> <p>La détection d'anomalies à haute résolution coûte 0,90\$ par alarme</p> <p>Le composite coûte 0,50\$ par alarme</p>
<a href="#">Amazon CloudWatch - Collecte de journaux</a>	5 Go de données (ingestion, stockage d'archives et données numérisées par les requêtes Logs Insights)	0,50\$ par Go
<a href="#">Amazon CloudWatch - Stockage des journaux</a>	5 Go de données (ingestion, stockage d'archives et données numérisées par les requêtes Logs Insights)	0,005\$ par Go de données numérisées
<a href="#">Amazon CloudWatch - Événements</a>	Tous les événements, à l'exception des événements personnalisés, sont inclus	1,00\$ par million d'événements pour les événements personnalisés 1,00\$ par million d'événements pour les événements multicomptes
<a href="#">AWS Lambda - Demandes</a>	1 million de demandes gratuites par mois	0,20\$ par million de demandes

Service	Niveau gratuit	Tarifcation [USD]
<a href="#">AWS Lambda - Durée</a>	400 000 Go de temps de calcul par mois	0,0000166667\$ pour chaque Go par seconde. Le prix de Duration dépend de la quantité de mémoire que vous allouez à votre fonction. Vous pouvez allouer à votre fonction n'importe quelle quantité de mémoire comprise entre 128 Mo et 10 240 Mo, par incréments de 1 Mo.
<a href="#">AWS Step Functions - Transitions d'état</a>	4 000 transitions d'État gratuites par mois	0,025\$ par 1 000 transitions entre États par la suite
<a href="#">Amazon EventBridge</a>	Tous les événements de changement d'état publiés par les AWS services sont gratuits	<p>Les événements personnalisés coûtent 1,00 \$/million d'événements personnalisés publiés</p> <p>Les événements tiers (SaaS) coûtent 1,00 \$/million d'événements publiés</p> <p>Les événements multicomptes coûtent 1,00 \$/million de dollars. Les événements multicomptes envoyés</p>
<a href="#">Amazon SNS</a>	Les 1 premiers millions de SNS demandes Amazon par mois sont gratuites	0,50\$ par million de demandes par la suite
<a href="#">Amazon SQS</a>	Les 1 premiers millions de SQS demandes Amazon par mois sont gratuites	0,40\$ par tranche de 1 million à 100 milliards de demandes par la suite

Service	Niveau gratuit	Tarifcation [USD]
<a href="#">Amazon DynamoDB</a>	Les premiers 25 Go de stockage sont gratuits	2,00\$ par million de lectures et d'écritures cohérentes par la suite

## Exemples de prix (mensuels)

### Exemple 1 : 300 mesures correctives par mois

- 10 comptes, 1 région
- 30 mesures correctives par account/Region/month
- Coût total 21,17\$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	Étapes : ~4 étapes* 300 remédiations* 0,002\$ = 2,40\$  Durée : 10 s * 300 mesures correctives * 0,00003\$ = 0,09\$	2,49\$
AWS Security Hub	Aucun service facturable utilisé	\$0
Amazon CloudWatch Logs	300 assainissements* 0,000002\$ = 0,0006\$  0,0006\$ * 0,03 = 0,000018\$	< 0,01\$
AWS Lambda - Demandes	300 remédiations* 6 demandes = 1 800 demandes  0,20\$ * 1 000 000 demandes = 0,20\$	0,20\$

Service	Hypothèses	Charges mensuelles [USD]
AWS Lambda - Durée	256 Mo : 1,875 Go sec * 300 corrections * 0,0000167\$ = 0,009375\$	< 0,01\$
AWS Step Functions	17 transitions d'état* 300 mesures correctives = 5 100 0,025 \$* (5 100 /1 000) transitions d'état = 0,15\$	0,15\$
EventBridge Règles d'Amazon	Aucun frais pour les règles	\$0
AWS Key Management Service	1 clé * 10 comptes * 1 région * 1\$ = 10\$	10,00\$
Amazon DynamoDB	2,00 \$* 1 000 000 livres lus et écrits = 2,00\$	2,00\$
Amazon SQS	0,40\$ * 1 000 000 demandes = 0,40\$	0,40\$
Amazon SNS	0,50\$ * 1 000 000 de notifications = 0,50\$	0,50\$
Amazon CloudWatch - Métriques	0,30\$ * 7 mesures personnalisées = 2,10\$ 0,01\$ * (300* 3/1 000) API appels de mesures de vente = 0,01\$	2,11\$
Amazon CloudWatch - Tableaux de bord	3,00 \$* 1 tableau de bord = 3,00\$	3,00\$
Amazon CloudWatch — Alarmes	0,10\$ * 3 alarmes = 0,30\$	0,30\$
Total		21,17\$

## Exemple 2 : 3 000 mesures correctives par mois

- 100 comptes, 1 région
- 30 mesures correctives par account/Region/month
- Coût total 134,86\$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	<p>Étapes : ~4 étapes* 3 000 assainissements* 0,002\$ = 24,00\$</p> <p>Durée : 10 s * 3 000 mesures correctives * 0,00003\$ = 0,90\$</p>	24,90\$
AWS Security Hub	Aucun service facturable utilisé	\$0
Amazon CloudWatch Logs	<p>3 000 assainissements* 0,000002\$ = 0,006\$</p> <p>0,006 \$* 0,03 = 0,00018\$</p>	< 0,01\$
AWS Lambda - Demandes	<p>3 000 mesures correctives* 6 demandes = 18 000 demandes</p> <p>0,20\$ * 1 000 000 demandes = 0,20\$</p>	0,20\$
AWS Lambda - Durée	<p>256 Mo : 1,875 Go sec * 3 000 mesures correctives * 0,000167\$ = 0,09375\$</p>	0,09\$
AWS Step Functions	<p>17 transitions d'état* 3 000 mesures correctives = 51 000</p>	1,28\$

Service	Hypothèses	Charges mensuelles [USD]
	0,025 \$* (51 000/1 000) transitions d'état = 1,275\$	
EventBridge Règles d'Amazon	Aucun frais pour les règles	\$0
AWS Key Management Service	1 clé * 100 comptes * 1 région * 1\$ = 100\$	100 USD
Amazon DynamoDB	2,00 \$* 1 000 000 livres lus et écrits = 2,00\$	2,00\$
Amazon SQS	0,40\$ * 1 000 000 demandes = 0,40\$	0,40\$
Amazon SNS	0,50\$ * 1 000 000 de notifications = 0,50\$	0,50\$
Amazon CloudWatch - Métriques	0,30\$ * 7 mesures personnalisées = 2,10\$  0,01\$ * (3 000* 3/1 000) API appels de mesures de vente = 0,09\$	2,19\$
Amazon CloudWatch - Tableaux de bord	3,00 \$* 1 tableau de bord = 3,00\$	3,00\$
Amazon CloudWatch — Alarmes	0,10\$ * 3 alarmes = 0,30\$	0,30\$
Total		134,86\$

### Exemple 3 : 30 000 mesures correctives par mois

- 1 000 comptes, 1 région
- 30 mesures correctives par account/Region/month
- Coût total 1 281,01\$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	<p>Étapes : ~4 étapes* 30 000 assainissements* 0,002\$ = 240,00\$</p> <p>Durée : 10 s * 30 000 assainissements* 0,00003\$ = 9,00\$</p>	249,00\$
AWS Security Hub	Aucun service facturable utilisé	\$0
Amazon CloudWatch Logs	<p>30 000 assainissements* 0,000002\$ = 0,06\$</p> <p>0,06\$ * 0,03 = 0,0018\$</p>	< 0,01\$
AWS Lambda - Demandes	<p>30 000 mesures correctrices* 6 demandes = 180 000 demandes</p> <p>0,20\$ * 1 000 000 demandes = 0,20\$</p>	0,20\$
AWS Lambda - Durée	<p>256 Mo : 1,875 Go de secondes * 30 000 mesures correctives * 0,000167\$ = 0,9375\$</p>	0,94\$
AWS Step Functions	<p>17 transitions d'état* 30 000 mesures correctives = 510 000</p> <p>0,025 \$* (510 000/1 000) transitions d'état = 12,75\$</p>	12,75\$
EventBridge Règles d'Amazon	Aucun frais pour les règles	\$0

Service	Hypothèses	Charges mensuelles [USD]
AWS Key Management Service	1 clé* 1 000 comptes * 1 région * 1 dollar = 1 000 dollars	1 000\$
Amazon DynamoDB	0,000002\$ * 1 000 000 de lecture et d'écriture = 2,00\$	2,00\$
Amazon SQS	0,000004\$ * 1 000 000 demandes = 0,40\$	0,40\$
Amazon SNS	0,000005\$ * 1 000 000 de notifications = 0,50\$	0,50\$
Amazon CloudWatch - Métriques	0,30\$ * 6 mesures personnalisées = 1,80\$  0,01\$ * (30 000* 3/1 000) API appels de mesures de vente = 0,90\$	2,70\$
Amazon CloudWatch - Tableaux de bord	3,00 \$* 1 tableau de bord = 3,00\$	3,00\$
Amazon CloudWatch — Alarmes	0,10\$ * 2 alarmes = 0,20\$	0,20\$
Amazon CloudWatch — Informations sur les applications	0,10 \$* 40 alarmes (maximum) = 4,00\$  0,53 \$* 10 Go de données de journal (est.) = 5,30\$  0,00267 \$* 5 OpsItems (est.) = ~0,01 \$	9,31\$
<b>Total</b>		<b>1 281,01\$</b>

## Coût supplémentaire pour les fonctionnalités optionnelles

Cette section identifie les coûts supplémentaires associés aux fonctionnalités optionnelles de cette solution.

### CloudWatch Métriques améliorées

Si vous sélectionnez `yes` le `EnableEnhancedCloudWatchMetrics` paramètre lors du déploiement de la pile d'administration, la solution crée deux métriques personnalisées et une alarme pour chaque ID de contrôle. Le coût dépend du nombre de contrôles IDs que vous corrigez. Dans le tableau suivant, nous supposons que vous corrigez les 96 contrôles différents IDs par mois, afin de déterminer la limite supérieure des coûts.

Service	Hypothèses	Charges mensuelles [USD]
	96 IDs contrôles* 2 = 192 métriques personnalisées	
Amazon CloudWatch - Métriques	0,30\$ * 192 mesures personnalisées = 57,60\$	57,60\$
Amazon CloudWatch - Alarmes	0,10\$ * 96 alarmes = 9,60\$	9,60\$
Total		67,20\$

### CloudTrail Journal des actions

Dans chaque compte membre pour lequel vous activez la fonctionnalité Action Log, les solutions créent une CloudTrail trace pour consigner tous les événements de gestion des écritures. Une fonction Lambda filtre les événements non liés à la solution. Cela signifie que le coût est lié au nombre total d'événements de gestion de votre compte, car les événements non liés à la solution sont toujours capturés par le journal et traités par la fonction Lambda.

Pour le tableau suivant, nous supposons 150 000 événements de gestion par mois sur le compte. Le coût réel dépend de l'activité réelle des événements de gestion sur votre compte.

Service	Hypothèses	Charges mensuelles [USD]
AWS CloudTrail	$150\,000 * 2,00 \text{ \$/}100\,000\text{\$} = 3,00\text{\$}$	3,00\$
Lambda	$150\,000 * 0,2 * 0,125 = 3\,750$ Go de secondes  $3\,750\text{\$} * 0,0000166667\text{\$} =$ coût du temps de calcul de 0,0625\$  $0,15 * 0,20\text{\$} = 0,03\text{\$}$ de coût de demande  $0,0625\text{\$} + 0,03\text{\$} =$ coût Lambda total de 0,0952\$	0,0925\$
Total		3,09\$ par compte membre

## Sécurité

Lorsque vous créez des systèmes sur une AWS infrastructure, les responsabilités en matière de sécurité sont partagées entre vous et AWS. Ce [modèle partagé](#) réduit votre charge opérationnelle car il AWS exploite, gère et contrôle les composants, notamment le système d'exploitation hôte, la couche de virtualisation et la sécurité physique des installations dans lesquelles les services fonctionnent. Pour plus d'informations sur AWS la sécurité, consultez le site [AWS Cloud Security](#).

## Rôles IAM

AWS Les rôles Identity and Access Management (IAM) permettent aux clients d'attribuer des politiques d'accès et des autorisations détaillées aux services et aux utilisateurs dans le AWS cloud. Cette solution crée IAM des rôles qui accordent aux fonctions automatisées de la solution l'accès pour effectuer des actions de correction dans le cadre d'un ensemble restreint d'autorisations spécifiques à chaque correction.

La fonction Step du compte administrateur est attribuée au rôle SO0111-SHARR-Orchestrator-Admin . Seul ce rôle est autorisé à assumer le rôle de membre SO0111-Orchestrator-Member

dans chaque compte membre. Le rôle de membre est autorisé par chaque rôle de correction à le transmettre au service AWS Systems Manager pour exécuter des runbooks de correction spécifiques. Les noms des rôles de correction commencent par SO0111, suivi d'une description correspondant au nom du runbook de correction. Par exemple, SO0111-R emoveVPCDefault SecurityGroupRules est le rôle du runbook de remédiation -R. ASR emoveVPCDefault SecurityGroupRules

## Soutenu Régions AWS

Nom de la région	Code région
USA Est (Ohio)	us-east-2
USA Est (Virginie du Nord)	us-east-1
USA Ouest (Californie du Nord)	us-west-1
US West (Oregon)	us-west-2
Afrique (Le Cap)	af-south-1
Asie-Pacifique (Hong Kong)	ap-east-1
Asie-Pacifique (Hyderabad)	ap-south-2
Asie-Pacifique (Jakarta)	ap-southeast-3
Asie-Pacifique (Melbourne)	ap-southeast-4
Asie-Pacifique (Mumbai)	ap-south-1
Asie-Pacifique (Osaka)	ap-northeast-3
Asie-Pacifique (Séoul)	ap-northeast-2
Asie-Pacifique (Singapour)	ap-southeast-1
Asie-Pacifique (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1

Nom de la région	Code région
Canada (Central)	ca-central-1
Europe (Francfort)	eu-central-1
Europe (Irlande)	eu-west-1
Europe (Londres)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Espagne)	eu-south-2
Europe (Stockholm)	eu-north-1
Europe (Zurich)	eu-central-2
Moyen-Orient (Bahreïn)	me-south-1
Moyen-Orient (UAE)	me-central-1
Amérique du Sud (Sao Paulo)	sa-east-1
AWS GovCloud (USA Est)	us-gov-east-1
AWS GovCloud (US-Ouest)	us-gov-east-2
Chine (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1

## Quotas

Les quotas de service, également appelés limites, correspondent au nombre maximal de ressources ou d'opérations de service pour votre AWS compte.

## Quotas pour AWS les services dans cette solution

Assurez-vous de disposer d'un quota suffisant pour chacun des [services mis en œuvre dans cette solution](#). Pour plus d'informations, reportez-vous à la section [Quotas AWS de service](#).

Utilisez les liens suivants pour accéder à la page de ce service. Pour consulter les quotas de service pour tous les AWS services de la documentation sans changer de page, consultez PDF plutôt les informations figurant sur la page [Points de terminaison et quotas du service](#).

### AWS CloudFormation quotas

Votre AWS compte comporte AWS CloudFormation des quotas dont vous devez tenir compte lorsque vous [lancez la pile](#) dans cette solution. En comprenant ces quotas, vous pouvez éviter les erreurs de limitation qui vous empêcheraient de déployer correctement cette solution. Pour plus d'informations, consultez la section sur [AWS CloudFormation les quotas](#) dans le guide de AWS CloudFormation l'utilisateur.

### Amazon EventBridge réglemente les quotas

Votre AWS compte est soumis EventBridge aux règles Amazon et aux quotas que vous devez connaître lorsque vous sélectionnez les playbooks à déployer avec la solution. Chaque playbook créera une EventBridge règle pour chaque contrôle qu'il pourra corriger. Lors du déploiement de plusieurs playbooks, il est possible d'atteindre le quota de règles. Pour plus d'informations, consultez les [EventBridge quotas Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.

### AWS Déploiement du Security Hub

AWS Le déploiement et la configuration du Security Hub sont une condition préalable à cette solution. Pour plus d'informations sur AWS la configuration de Security Hub, reportez-vous à la section [Configuration AWS de Security Hub](#) du Guide AWS de l'utilisateur de Security Hub.

Au minimum, un Security Hub fonctionnel doit être configuré sur votre compte principal. Vous pouvez déployer cette solution dans le même compte (et dans la même AWS région) que le compte principal du Security Hub. Dans chaque compte principal et secondaire Security Hub, vous devez également déployer le modèle de membre qui autorise AssumeRole les AWS Step Functions de la solution à exécuter des runbooks de correction dans le compte.

## Stack ou StackSets déploiement

Un ensemble de piles vous permet de créer des piles dans AWS des comptes de différentes AWS régions à l'aide d'un AWS CloudFormation modèle unique. À partir de la version 1.4, cette solution prend en charge le déploiement d'ensembles de piles en répartissant les ressources en fonction de l'endroit et de la manière dont elles sont déployées. Les clients disposant de plusieurs comptes, en particulier ceux qui l'utilisent AWS Organizations, peuvent tirer parti de l'utilisation d'ensembles de piles pour le déploiement sur de nombreux comptes. Cela réduit les efforts nécessaires à l'installation et à la maintenance de la solution. Pour plus d'informations StackSets, reportez-vous à la section [Utilisation AWS CloudFormation StackSets](#).

# Déployez la solution

## Important

Si la fonctionnalité de [consolidation des résultats de contrôle](#) est activée dans Security Hub (c'est le cas par défaut dans les nouveaux déploiements), activez le playbook Security Control (CS) uniquement lors du déploiement de cette solution. Si la fonctionnalité n'est pas activée, activez uniquement les playbooks conformément aux normes de sécurité activées dans Security Hub. L'activation de playbooks supplémentaires peut permettre d'atteindre le [quota de EventBridge règles](#).

Cette solution utilise des [AWS CloudFormation modèles et des piles](#) pour automatiser son déploiement. Les CloudFormation modèles spécifient les AWS ressources incluses dans cette solution et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans les modèles.

Pour que la solution fonctionne, trois modèles doivent être déployés. Décidez d'abord où déployer les modèles, puis comment les déployer.

Cette présentation décrit les modèles et explique comment décider où et comment les déployer. Les sections suivantes contiendront des instructions plus détaillées pour déployer chaque pile en tant que Stack ou StackSet.

## Décider où déployer chaque stack

Les trois modèles seront désignés par les noms suivants et contiendront les ressources suivantes :

- Stack d'administration : fonction d'étape de l'orchestrateur, règles relatives aux événements et action personnalisée du Security Hub.
- Pile de membres : documents d'SSMautomatisation de la remédiation.
- Les rôles des membres se cumulent : IAM rôles pour les mesures correctives.

La pile d'administrateurs doit être déployée une seule fois, dans un seul compte et dans une seule région. Il doit être déployé dans le compte et dans la région que vous avez configurés comme destination d'agrégation pour les résultats du Security Hub relatifs à votre organisation.

La solution fonctionne sur la base des résultats du Security Hub. Elle ne sera donc pas en mesure de fonctionner sur les résultats d'un compte ou d'une région en particulier si ce compte ou cette région n'a pas été configuré pour agréger les résultats dans le compte administrateur du Security Hub et dans la région.

Par exemple, une organisation possède des comptes opérant dans des régions `us-east-1` et dont `us-west-2` le compte est `111111111111` celui d'administrateur délégué du Security Hub dans la région `us-east-1`. Les comptes `222222222222` et les comptes `333333333333` doivent être des comptes membres du Security Hub pour le compte d'administrateur délégué `111111111111`. Les trois comptes doivent être configurés pour agréger les résultats de `us-west-2` à `us-east-1`. La pile d'administrateurs doit être déployée pour être prise `111111111111` en compte `us-east-1`.

Pour plus de détails sur la recherche de l'agrégation, consultez la documentation relative aux [comptes d'administrateur délégué](#) de Security Hub et à l'[agrégation entre régions](#).

La pile d'administrateurs doit d'abord terminer le déploiement avant de déployer les piles de membres afin qu'une relation de confiance puisse être créée entre les comptes des membres et le compte du hub.

La pile de membres doit être déployée dans chaque compte et région dans lesquels vous souhaitez corriger les résultats. Cela peut inclure le compte d'administrateur délégué de Security Hub sur lequel vous avez précédemment déployé la pile ASR d'administrateurs. Les documents d'automatisation doivent être exécutés dans les comptes des membres afin d'utiliser le niveau gratuit d'automatisation. SSM

Dans l'exemple précédent, si vous souhaitez corriger les résultats de tous les comptes et régions, la pile de membres doit être déployée sur les trois comptes (`111111111111222222222222`, `et333333333333`) et sur les deux régions (`us-east-1` et `us-west-2`).

La pile de rôles des membres doit être déployée sur chaque compte, mais elle contient des ressources globales (IAM rôles) qui ne peuvent être déployées qu'une seule fois par compte. Peu importe la région dans laquelle vous déployez la pile de rôles des membres, par souci de simplicité, nous vous suggérons de déployer le déploiement dans la même région que celle dans laquelle la pile d'administrateurs est déployée.

À l'aide de l'exemple précédent, nous vous suggérons de déployer la pile de rôles des membres sur les trois comptes (`111111111111222222222222`, `et333333333333`) `us-east-1`.

## Décider de la manière de déployer chaque stack

Les options de déploiement d'une pile sont les suivantes :

- CloudFormation StackSet (autorisations autogérées)
- CloudFormation StackSet (autorisations gérées par le service)
- CloudFormation Empilez

StackSets avec des autorisations gérées par les services sont les plus pratiques car elles ne nécessitent pas le déploiement de vos propres rôles et peuvent être automatiquement déployées sur de nouveaux comptes au sein de l'organisation. Malheureusement, cette méthode ne prend pas en charge les piles imbriquées, que nous utilisons à la fois dans la pile d'administration et dans la pile de membres. La seule pile qui peut être déployée de cette façon est la pile des rôles des membres.

Sachez que lors du déploiement dans l'ensemble de l'organisation, le compte de gestion de l'organisation n'est pas inclus. Par conséquent, si vous souhaitez corriger les résultats du compte de gestion de l'organisation, vous devez effectuer le déploiement sur ce compte séparément.

La pile de membres doit être déployée sur tous les comptes et régions, mais elle ne peut pas être déployée StackSets avec des autorisations gérées par le service car elle contient des piles imbriquées. Nous vous suggérons donc de déployer cette pile StackSets avec des autorisations autogérées.

La pile d'administration n'est déployée qu'une seule fois, elle peut donc être déployée en tant que CloudFormation pile simple ou en tant que pile StackSet avec des autorisations autogérées dans un seul compte et une seule région.

## Conclusions de contrôle consolidées

Les comptes de votre organisation peuvent être configurés en activant ou en désactivant la fonction de consolidation des résultats de contrôle de Security Hub. Consultez les [résultats des contrôles consolidés](#) dans le Guide de l'utilisateur de AWS Security Hub.

### Important

Si cette option est activée, vous devez utiliser la version 2.0.0 ou ultérieure de la solution. En outre, vous devez déployer les piles imbriquées Admin et Member pour les normes « SC » ou « contrôle de sécurité ». Cela déploie les documents et EventBridge règles d'automatisation à utiliser avec le contrôle consolidé IDs généré lorsque cette fonctionnalité est activée. Il

n'est pas nécessaire de déployer les piles imbriquées Admin ou Member pour des normes spécifiques (par exemple AWSFSBP) lors de l'utilisation de cette fonctionnalité.

## AWS CloudFormation modèles

[View template](#)

aws-

[sharr-deploy](#).template - Utilisez ce modèle pour lancer la réponse de sécurité automatisée sur la AWS solution. Le modèle installe les composants principaux de la solution, une pile imbriquée pour les AWS Step Functions journaux et une pile imbriquée pour chaque norme de sécurité que vous choisissez d'activer.

Les services utilisés incluent Amazon Simple Notification Service AWS Key Management Service AWS Identity and Access Management AWS Lambda AWS Step Functions, Amazon CloudWatch Logs, Amazon S3 et AWS Systems Manager.

### Support pour les comptes d'administrateur

Les modèles suivants sont installés dans le compte administrateur du AWS Security Hub pour activer les normes de sécurité que vous souhaitez prendre en charge. Vous pouvez choisir le modèle à installer parmi les modèles suivants lors de l'installation de `aws-sharr-deploy`.template.

`aws-sharr-orchestrator-log`.template - Crée un groupe de CloudWatch journaux pour la fonction Orchestrator Step.

`AFSBPStack`.template - Règles relatives aux meilleures pratiques AWS de sécurité de base v1.0.0.

`CIS120Stack`.template - Benchmarks d'CISSAmazon Web Services Foundations, règles de la version v1.2.0.

`CIS140Stack`.template - Benchmarks d'CISSAmazon Web Services Foundations, règles de la version v1.4.0.

`PCI321StackRègles`.template - PCI - DSS v3.2.1.

`NISTStack`.template - National Institute of Standards and Technology (NIST), règles de la version 5.0.0.

`SCStack`.template - Règles SC v2.0.0.

## Comptes membres

[View template](#)

aws-

[sharr-member](#).template - Utilisez ce modèle après avoir configuré la solution principale pour installer les runbooks d'automatisation et les autorisations de AWS Systems Manager sur chacun de vos comptes membres du AWS Security Hub (y compris le compte administrateur). Ce modèle vous permet de choisir les playbooks standard de sécurité à installer.

`aws-sharr-member.template` Installe les modèles suivants en fonction de vos sélections :

`aws-sharr-remediations.template` - Code de correction courant utilisé par une ou plusieurs normes de sécurité.

`AFSBPMemberStack.template` - Paramètres, autorisations AWS et manuels de correction des meilleures pratiques de sécurité fondamentales de la version 1.0.0.

`CIS120 MemberStack .template` - Benchmarks d' CIS Amazon Web Services Foundation, paramètres de la version 1.2.0, autorisations et manuels de correction.

`CIS140 MemberStack .template` - Benchmarks d' CIS Amazon Web Services Foundation, paramètres de la version 1.4.0, autorisations et manuels de correction.

`PCI321MemberStack.template` - PCI - Paramètres, autorisations et manuels de correction de la DSS version 3.2.1.

`NISTMemberStack.template` - National Institute of Standards and Technology (NIST), paramètres, autorisations et manuels de correction de la version 5.0.0.

`SCMemberStack.template` - Paramètres de contrôle de sécurité, autorisations et manuels de correction.

## Rôles des membres

[View template](#)

aws-

[sharr-member-roles](#).template - Définit les rôles de correction nécessaires dans chaque compte AWS Security Hub membre.

## Intégration du système de billetterie

Utilisez l'un des modèles suivants pour l'intégrer à votre système de billetterie.

**View template**

JiraBlu

- Déployez si vous utilisez Jira comme système de billetterie.

**View template**

Service

- Déployez si vous l'utilisez ServiceNow comme système de billetterie.

Si vous souhaitez intégrer un autre système de billetterie externe, vous pouvez utiliser l'une ou l'autre de ces piles comme modèle pour comprendre comment implémenter votre propre intégration personnalisée.

## Déploiement automatisé - StackSets

### Note

Nous vous recommandons de déployer avec StackSets. Toutefois, pour les déploiements à compte unique ou à des fins de test ou d'évaluation, envisagez l'option de [déploiement stacks](#).

Avant de lancer la solution, passez en revue l'architecture, les composants de la solution, la sécurité et les considérations de conception abordées dans ce guide. Suivez les step-by-step instructions de cette section pour configurer et déployer la solution dans votre AWS Organizations.

Temps de déploiement : environ 30 minutes par compte, selon StackSet les paramètres.

## Prérequis

[AWS Organizations](#) vous aide à gérer et à gouverner de manière centralisée votre AWS environnement et vos ressources multi-comptes. StackSets fonctionnent le mieux avec les AWS Organizations.

Si vous avez déjà déployé la version v1.3.x ou une version antérieure de cette solution, vous devez désinstaller la solution existante. Pour plus d'informations, reportez-vous à la section [Mettre à jour la solution](#).

Avant de déployer cette solution, passez en revue le déploiement AWS de Security Hub :

- Votre AWS organisation doit disposer d'un compte administrateur Security Hub délégué.
- Security Hub doit être configuré pour agréger les résultats entre les régions. Pour plus d'informations, reportez-vous à la section [Agrégation des résultats par région](#) dans le Guide de l'utilisateur du AWS Security Hub.
- Vous devez [activer Security Hub](#) pour votre organisation dans chaque région où vous AWS l'utilisez.

Cette procédure suppose que vous disposez de plusieurs comptes utilisant AWS Organizations et que vous avez délégué un compte AWS Organizations administrateur et un compte administrateur AWS Security Hub.

## Vue d'ensemble du déploiement

### Note

StackSets le déploiement de cette solution utilise une combinaison de gestion des services et d'autogestion. StackSets L'autogéré StackSets doit être utilisé actuellement, car ils utilisent le mode imbriqué StackSets, qui n'est pas encore pris en charge par le service géré. StackSets

Déployez le StackSets depuis un [compte d'administrateur délégué](#) dans votre AWS Organizations.

### Planification

Utilisez le formulaire suivant pour faciliter le StackSets déploiement. Préparez vos données, puis copiez-collez les valeurs pendant le déploiement.

```
AWS Organizations admin account ID: _____  
Security Hub admin account ID: _____  
CloudTrail Logs Group: _____  
Member account IDs (comma-separated list):  
_____,  
_____
```

```
_____,  
_____,  
_____  
AWS Organizations OUs (comma-separated list):  
_____,  
_____,  
_____,  
_____,  
_____
```

### (Facultatif) Étape 0 : Déployer la pile d'intégration de billetterie

- Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, déployez d'abord la pile d'intégration de billetterie dans votre compte administrateur Security Hub.
- Copiez le nom de la fonction Lambda depuis cette pile et fournissez-le comme entrée à la pile d'administration (voir Étape 1).

### Étape 1 : Lancez la pile d'administration dans le compte administrateur délégué du Security Hub

- À l'aide d'un outil autogéré StackSet, lancez le `aws-sharr-deploy.template` AWS CloudFormation modèle sur votre compte administrateur AWS Security Hub dans la même région que votre administrateur Security Hub. Ce modèle utilise des piles imbriquées.
- Choisissez les normes de sécurité à installer. Par défaut, seul SC est sélectionné (recommandé).
- Choisissez un groupe de journaux Orchestrator existant à utiliser. Sélectionnez Yes s'il existe `S00111-SHARR-Orchestrator` déjà depuis une installation précédente.

Pour plus d'informations sur l'autogestion StackSets, reportez-vous à la section [Accorder des autorisations autogérées](#) dans le guide de l'AWS CloudFormation utilisateur.

### Étape 2 : Installation des rôles de correction dans chaque compte AWS Security Hub membre

Attendez que l'étape 1 soit terminée, car le modèle de l'étape 2 fait référence aux IAM rôles créés par l'étape 1.

- À l'aide d'un service géré StackSet, lancez le `aws-sharr-member-roles.template` AWS CloudFormation modèle dans une seule région dans chaque compte de votre AWS Organizations
- Choisissez d'installer ce modèle automatiquement lorsqu'un nouveau compte rejoint l'organisation.
- Entrez le numéro de compte de votre compte AWS Security Hub administrateur.

## Étape 3 : Lancez la pile de membres dans chaque compte membre et région du AWS Security Hub

- À l'aide de l'autogestion StackSets, lancez le `aws-sharr-member.template` AWS CloudFormation modèle dans toutes les régions où vous disposez de AWS ressources dans chaque compte de votre AWS organisation géré par le même administrateur du Security Hub.

### Note

Jusqu'à ce que le StackSets support géré par les services soit intégré, vous devez effectuer cette étape pour tous les nouveaux comptes qui rejoignent l'organisation.

- Choisissez les playbooks Security Standard à installer.
- Indiquez le nom d'un groupe de CloudTrail journaux (utilisé par certaines corrections).
- Entrez le numéro de compte de votre compte AWS Security Hub administrateur.

## (Facultatif) Étape 0 : Lancer une pile d'intégration d'un système de tickets

1. Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, lancez d'abord la pile d'intégration correspondante.
2. Choisissez les piles d'intégration fournies pour Jira ou ServiceNow utilisez-les comme modèle pour implémenter votre propre intégration personnalisée.

Pour déployer la pile Jira, procédez comme suit :

- a. Entrez un nom pour votre pile.
- b. Fournissez-les URI à votre instance Jira.
- c. Fournissez la clé de projet pour le projet Jira auquel vous souhaitez envoyer des tickets.
- d. Créez un nouveau secret clé-valeur dans Secrets Manager qui contient votre `Username` Jira et `Password`

### Note

Vous pouvez choisir d'utiliser une API clé Jira à la place de votre mot de passe en indiquant votre nom d'utilisateur `Username` et votre API clé en tant que `Password`

- e. Ajoutez le ARN de ce secret comme entrée à la pile.



## Specify stack details

**Provide a stack name**

**Stack name**

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 19/128.

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**ServiceNow Project Information**

**InstanceURI**

The URI of your ServiceNow instance. For example: `https://my-servicenow-instance.service-now.com`

**ServiceNowTableName**

Enter the name of your ServiceNow Table where tickets should be created.

**ServiceNow API Credentials**

**SecretArn**

The ARN of the Secrets Manager secret where you have stored your API credentials. This must be a JSON secret with the following keys: `API_Key`.

[Cancel](#) [Previous](#) [Next](#)

Pour créer une pile d'intégration personnalisée : incluez une fonction Lambda que l'orchestrateur de solutions Step Functions peut appeler pour chaque correction. La fonction Lambda doit prendre les données fournies par Step Functions, construire une charge utile conformément aux exigences de votre système de billetterie et demander à votre système de créer le ticket.

## Étape 1 : Lancez la pile d'administration dans le compte administrateur délégué du Security Hub

1. Lancez la [pile d'aws-sharr-deploy.templateadministration](#) avec votre compte d'administrateur Security Hub. Généralement, un par organisation dans une seule région. Comme cette pile utilise des piles imbriquées, vous devez déployer ce modèle en tant que modèle autogéré. StackSet

## Configure StackSet options

### Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack.

Key	Value	Remove
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

### Permissions

Choose an IAM role to explicitly define how CloudFormation will manage your target accounts. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

**Service-managed permissions**  
 StackSets automatically configures the permissions required to deploy to target accounts managed by AWS Organizations. With this option, you can enable automatic deployment to accounts in your organization

**Self-service permissions**  
 You create the execution roles required to deploy to target accounts

**IAM admin role ARN - optional**  
 Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name	Remove
<input type="text" value="AWSCloudFormationStackSetAdministrationRole"/>	<input type="button" value="Remove"/>

**⚠ StackSets will use this role for administering your individual accounts.**

**IAM execution role name**

IAM execution role name can include letters (A-Z and a-z), numbers (0-9), and select special characters (+,=,@,-\_) characters. Maximum length is 64 characters.

### StackSet Options de configuration

2. Pour le paramètre Numéros de compte, entrez l'ID de compte du compte administrateur du AWS Security Hub.
3. Pour le paramètre Specify regions, sélectionnez uniquement la région dans laquelle l'administrateur Security Hub est activé. Attendez que cette étape soit terminée avant de passer à l'étape 2.

## Étape 2 : Installation des rôles de correction dans chaque compte membre du AWS Security Hub

Utilisez un service géré StackSets pour déployer le [modèle de rôles des membres](#), `aws-sharr-member-roles.template`. Cela StackSet doit être déployé dans une région par compte membre. Il définit les rôles globaux qui autorisent les API appels entre comptes à partir de la fonction d'étape SHARR Orchestrator.

1. Déployez dans l'ensemble de l'organisation (standard) ou dans les unités organisationnelles, conformément aux politiques de votre organisation.
2. Activez le déploiement automatique pour que les nouveaux comptes des AWS Organisations reçoivent ces autorisations.
3. Pour le paramètre Spécifier les régions, sélectionnez une seule région. IAMles rôles sont globaux. Vous pouvez passer à l'étape 3 pendant le StackSet déploiement.

### Specify StackSet details

**StackSet name**

StackSet name

Must contain only letters, numbers, and dashes. Must start with a letter.

**StackSet description**

You can use the description to identify the stack set's purpose or other important information.

StackSet description

**Parameters (1)**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**SecHubAdminAccount**  
Admin account number

Cancel Previous Next

Spécifiez StackSet les détails

## Étape 3 : Lancez la pile de membres dans chaque compte membre et région du AWS Security Hub

Comme la [pile de membres](#) utilise des piles imbriquées, vous devez effectuer le déploiement en tant que solution autogérée. StackSet Cela ne prend pas en charge le déploiement automatique vers les nouveaux comptes de l'AWSorganisation.

## Paramètres

**LogGroup Configuration** : Choisissez le groupe de journaux qui reçoit CloudTrail les journaux. S'il n'en existe aucun, ou si le groupe de journaux est différent pour chaque compte, choisissez une valeur appropriée. Les administrateurs de compte doivent mettre à jour le paramètre Systems Manager — LogGroupName Parameter Store /Solutions/SO0111/Metrics \_ après avoir créé un groupe de CloudWatch journaux pour les CloudTrail journaux. Cela est nécessaire pour les mesures correctives qui créent des alarmes métriques lors des API appels.

**Normes** : Choisissez les normes à charger dans le compte du membre. Cela installe uniquement les runbooks de AWS Systems Manager ; cela n'active pas le Security Standard.

**SecHubAdminAccount**: Entrez l'identifiant du compte administrateur du AWS Security Hub sur lequel vous avez installé le modèle d'administration de la solution.

**Accounts**  
Identify accounts or organizational units in which you want to modify stacks

**Deployment locations**  
StackSets can be deployed into accounts or an organizational unit.

Deploy stacks in accounts  Deploy stacks in organizational units

**Account numbers**  
Enter account numbers or populate from a file.

111122223333, 123456789012, 111144442222

12-Digit account numbers separated by commas.

Upload .csv file No file chosen

## Comptes

**Lieux de déploiement** : vous pouvez spécifier une liste de numéros de compte ou d'unités organisationnelles.

**Spécifiez les régions** : sélectionnez toutes les régions dans lesquelles vous souhaitez corriger les résultats. Vous pouvez ajuster les options de déploiement en fonction du nombre de comptes et de régions. La simultanéité des régions peut être parallèle.

# Déploiement automatisé - Stacks

## Note

Pour les clients ayant plusieurs comptes, nous recommandons vivement [le déploiement avec StackSets](#).

Avant de lancer la solution, passez en revue l'architecture, les composants de la solution, la sécurité et les considérations de conception abordées dans ce guide. Suivez les step-by-step instructions de cette section pour configurer et déployer la solution dans votre compte.

Temps de déploiement : environ 30 minutes

## Prérequis

Avant de déployer cette solution, assurez-vous qu'elle AWS Security Hub se trouve dans la même AWS région que vos comptes principal et secondaire. Si vous avez déjà déployé cette solution, vous devez désinstaller la solution existante. Pour plus d'informations, reportez-vous à la section [Mettre à jour la solution](#).

## Vue d'ensemble du déploiement

Suivez les étapes ci-dessous pour déployer cette solution sur AWS.

### [\(Facultatif\) Étape 0 : Lancer une pile d'intégration d'un système de tickets](#)

- Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, déployez d'abord la pile d'intégration de billetterie dans votre compte administrateur Security Hub.
- Copiez le nom de la fonction Lambda depuis cette pile et fournissez-le comme entrée à la pile d'administration (voir Étape 1).

### [Étape 1 : Lancez la pile d'administration](#)

- Lancez le `aws-sharr-deploy.template` AWS CloudFormation modèle dans votre compte AWS Security Hub administrateur.
- Choisissez les normes de sécurité à installer.

- Choisissez un groupe de journaux Orchestrator existant à utiliser (sélectionnez Yes s'il existe S00111-SHARR-Orchestrator déjà depuis une installation précédente).

### Étape 2 : Installation des rôles de correction dans chaque compte AWS Security Hub membre

- Lancez le `aws-sharr-member-roles.template` AWS CloudFormation modèle dans une région par compte membre.
- Entrez l'IG du compte à 12 chiffres pour le compte AWS Security Hub administrateur.

### Étape 3 : Lancez la pile de membres

- Spécifiez le nom du groupe de CloudWatch journaux à utiliser avec les corrections CIS 3.1-3.14. Il doit s'agir du nom du groupe de CloudWatch journaux qui reçoit CloudTrail les journaux.
- Choisissez si vous souhaitez installer les rôles de correction. Installez ces rôles une seule fois par compte.
- Sélectionnez les playbooks à installer.
- Entrez l'identifiant du compte AWS Security Hub administrateur.

### Étape 4 : (Facultatif) Ajustez les mesures correctives disponibles

- Supprimez toutes les corrections pour chaque compte membre. Cette étape est facultative.

## (Facultatif) Étape 0 : Lancer une pile d'intégration d'un système de tickets

1. Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, lancez d'abord la pile d'intégration correspondante.
2. Choisissez les piles d'intégration fournies pour Jira ou ServiceNow utilisez-les comme modèle pour implémenter votre propre intégration personnalisée.

Pour déployer la pile Jira, procédez comme suit :

- a. Entrez un nom pour votre pile.
- b. Fournissez-les URI à votre instance Jira.
- c. Fournissez la clé de projet pour le projet Jira auquel vous souhaitez envoyer des tickets.
- d. Créez un nouveau secret clé-valeur dans Secrets Manager qui contient votre Username Jira et Password

**Note**

Vous pouvez choisir d'utiliser une API clé Jira à la place de votre mot de passe en indiquant votre nom d'utilisateur `Username` et votre API clé en tant que `Password`.

- e. Ajoutez le ARN de ce secret comme entrée à la pile.

**Specify stack details****Provide a stack name****Stack name**

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 22/128.

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**Jira Project Information****InstanceURI**

The URI of your Jira instance. For example: `https://my-jira-instance.atlassian.net`

**JiraProjectKey**

The key of your Jira project where tickets will be created.

**Jira API Credentials****SecretArn**

The ARN of the Secrets Manager secret where you have stored your API credentials. This must be a JSON secret with the following keys: `Username`, `Password`.

[Cancel](#)[Previous](#)[Next](#)

Pour déployer la ServiceNow pile, procédez comme suit :

- Entrez un nom pour votre pile.
- Indiquez le URI nom de votre ServiceNow instance.
- Entrez le nom ServiceNow de votre table.
- Créez une API clé ServiceNow avec l'autorisation de modifier la table dans laquelle vous souhaitez écrire.
- Créez un secret dans Secrets Manager à l'aide de la clé `API_Key` et ARN fournissez-le comme entrée à la pile.

## Specify stack details

**Provide a stack name**

**Stack name**

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 19/128.

**Parameters**

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

**ServiceNow Project Information**

**InstanceURI**

The URI of your ServiceNow instance. For example: `https://my-servicenow-instance.service-now.com`

**ServiceNowTableName**

Enter the name of your ServiceNow Table where tickets should be created.

**ServiceNow API Credentials**

**SecretArn**

The ARN of the Secrets Manager secret where you have stored your API credentials. This must be a JSON secret with the following keys: `API_Key`.

[Cancel](#) [Previous](#) [Next](#)

Pour créer une pile d'intégration personnalisée : incluez une fonction Lambda que l'orchestrateur de solutions Step Functions peut appeler pour chaque correction. La fonction Lambda doit prendre les données fournies par Step Functions, construire une charge utile conformément aux exigences de votre système de billetterie et demander à votre système de créer le ticket.

## Étape 1 : Lancez la pile d'administration

### Important

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre comment les clients utilisent cette solution et les services et produits associés. AWS détient les données recueillies dans le cadre de cette enquête. La collecte de données est soumise à l'[avis AWS de confidentialité](#).

Pour désactiver cette fonctionnalité, téléchargez le modèle, modifiez la section de AWS CloudFormation mappage, puis utilisez la AWS CloudFormation console pour télécharger votre modèle et déployer la solution. Pour plus d'informations, reportez-vous à la section [Collecte de données anonymisée](#) de ce guide.

Ce AWS CloudFormation modèle automatisé déploie la réponse de sécurité automatisée sur AWS une solution dans le AWS cloud. Avant de lancer la pile, vous devez activer Security Hub et remplir les [conditions requises](#).

#### Note

Vous êtes responsable du coût des AWS services utilisés lors de l'exécution de cette solution. Pour plus de détails, consultez la section [Coût](#) de ce guide et consultez la page Web de tarification de chaque AWS service utilisé dans cette solution.

1. Connectez-vous au AWS Management Console depuis le compte sur lequel le AWS Security Hub est actuellement configuré et utilisez le bouton ci-dessous pour lancer le `aws-sharr-deploy.template` AWS CloudFormation modèle.

[Launch solution](#)

Vous pouvez également [télécharger le modèle](#) comme point de départ pour votre propre implémentation.

2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre AWS région, utilisez le sélecteur de région dans la barre de AWS Management Console navigation.

#### Note

Cette solution utilise AWS Systems Manager ce qui est actuellement disponible dans certaines AWS régions uniquement. La solution fonctionne dans toutes les régions qui prennent en charge ce service. Pour connaître la disponibilité la plus récente par région, consultez la [liste des services AWS régionaux](#).

3. Sur la page **Create stack**, vérifiez que le modèle correct URL se trouve dans la zone de URL texte Amazon S3, puis choisissez **Next**.
4. Sur la page **Spécifier les détails de la pile**, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives à la dénomination [IAMdes STS](#) caractères, reportez-vous au Guide de l'AWS Identity and Access Management utilisateur.
5. Sur la page **Paramètres**, choisissez **Next**.

Paramètre	Par défaut	Description
Charger SC Admin Stack	yes	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des contrôles SC.
Charger AFSBP Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des FSBP contrôles.
Charger CIS12 0 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des contrôles CIS12 0.
Charger CIS14 0 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des contrôles CIS14 0.
Charger CIS3 00 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des contrôles CIS3 00.
Charger PC1321 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration

Paramètre	Par défaut	Description
		pour la correction automatique des PC1321 contrôles.
Charger NIST Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des NIST contrôles.
Réutiliser le groupe de journaux Orchestrator	no	Choisissez de réutiliser ou non un groupe de S00111-SHARR-Orchestrator CloudWatch journaux existant. Cela simplifie la réinstallation et les mises à niveau sans perdre les données du journal d'une version précédente. Si vous effectuez une mise à niveau depuis la version 1.2 ou une version ultérieure, sélectionnez <code>no</code> .
Utiliser CloudWatch les métriques	yes	Spécifiez si vous souhaitez activer CloudWatch les métriques pour surveiller la solution. Cela créera un CloudWatch tableau de bord pour consulter les statistiques.

Paramètre	Par défaut	Description
Utiliser les alarmes CloudWatch métriques	yes	Spécifiez si vous souhaitez activer CloudWatch les alarmes métriques pour la solution. Cela créera des alarmes pour certaines métriques collectées par la solution.
RemediationFailureAlarmThreshold	5	<p>Spécifiez le seuil pour le pourcentage d'échecs de correction par ID de contrôle. Par exemple, si vous entrez 5, vous recevez une alarme si un ID de contrôle échoue dans plus de 5 % des cas de correction au cours d'une journée donnée.</p> <p>Ce paramètre ne fonctionne que si des alarmes sont créées (voir le paramètre Utiliser CloudWatch les alarmes métriques).</p>

Paramètre	Par défaut	Description
EnableEnhancedCloudWatchMetrics	no	Si yes, crée des CloudWatch métriques supplémentaires pour suivre tous les contrôles IDs individuellement sur le CloudWatch tableau de bord et sous forme d' CloudWatch alarmes.  Consultez la section <a href="#">Coût</a> pour comprendre les coûts supplémentaires que cela entraîne.
TicketGenFunctionName	(Entrée facultative)	Facultatif. Laissez ce champ vide si vous ne souhaitez pas intégrer de système de billetterie. Sinon, fournissez le nom de la fonction Lambda à partir de la sortie de la pile de l' <a href="#">étape 0</a> , par exemple : S00111-ASR-ServiceNow-TicketGenerator

6. Sur la page Configurer les options de pile, choisissez Suivant.
7. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera AWS Identity and Access Management (IAM) des ressources.
8. Sélectionnez Create stack (Créer une pile) pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le COMPLETE statut CREATE \_ dans 15 minutes environ.

## Étape 2 : Installation des rôles de correction dans chaque compte membre du AWS Security Hub

Ils ne `aws-sharr-member-roles.template` StackSet doivent être déployés que dans une seule région par compte membre. Il définit les rôles globaux qui autorisent les API appels entre comptes à partir de la fonction d'étape SHARR Orchestrator.

1. Connectez-vous à la console AWS de gestion pour chaque compte AWS Security Hub membre (y compris le compte administrateur, qui est également membre). Cliquez sur le bouton pour lancer le `aws-sharr-member-roles.template` AWS CloudFormation modèle. Vous pouvez également [télécharger le modèle](#) comme point de départ pour votre propre implémentation.



2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre AWS région, utilisez le sélecteur de région dans la barre de navigation AWS de la console de gestion.
3. Sur la page Create stack, vérifiez que le modèle correct URL se trouve dans la zone de URL texte Amazon S3, puis choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limitations relatives aux IAM caractères de dénomination, reportez-vous au guide de l'utilisateur d'AWS Identity and Access Management. STS
5. Sur la page Paramètres, spécifiez les paramètres suivants et choisissez Next.

Paramètre	Par défaut	Description
Namespace	<i>&lt;Requires input&gt;</i>	Entrez une chaîne de 9 caractères alphanumériques minuscules maximum. Cette chaîne fait partie des noms de IAM rôles. Utilisez la même valeur pour le déploiement de la pile de membres et le déploiement

Paramètre	Par défaut	Description
		nt de la pile de rôles des membres.
Administrateur du compte Sec Hub	<Requires input>	Entrez l'identifiant de compte à 12 chiffres du compte AWS Security Hub administrateur. Cette valeur accorde des autorisations au rôle de solution du compte administrateur.

- Sur la page Configurer les options de pile, choisissez Suivant.
- Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera AWS Identity and Access Management (IAM) des ressources.
- Sélectionnez Create stack (Créer une pile) pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le COMPLETE statut CREATE \_ dans environ 5 minutes. Vous pouvez passer à l'étape suivante pendant le chargement de cette pile.

## Étape 3 : Lancez la pile de membres

### Important

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre comment les clients utilisent cette solution et les services et produits associés. AWS détient les données recueillies dans le cadre de cette enquête. La collecte de données est soumise à la AWS Politique de confidentialité.

Pour désactiver cette fonctionnalité, téléchargez le modèle, modifiez la section de AWS CloudFormation mappage, puis utilisez la AWS CloudFormation console pour télécharger votre modèle et déployer la solution. Pour plus d'informations, reportez-vous à la section [Collecte de mesures opérationnelles](#) de ce guide.

La `aws-sharr-member` pile doit être installée sur chaque compte membre du Security Hub. Cette pile définit les runbooks pour la correction automatique. L'administrateur de chaque compte membre peut contrôler les mesures correctives disponibles via cette pile.

1. Connectez-vous au compte AWS Management Console de chaque AWS Security Hub membre (y compris le compte administrateur, qui est également membre). Cliquez sur le bouton pour lancer le `aws-sharr-member.template` AWS CloudFormation modèle.

[Launch solution](#)

Vous pouvez également [télécharger le modèle](#) comme point de départ pour votre propre implémentation.

2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre AWS région, utilisez le sélecteur de région dans la barre de AWS Management Console navigation.

#### Note

Cette solution utilise AWS Systems Manager, qui est actuellement disponible dans la majorité des AWS régions. La solution fonctionne dans toutes les régions qui prennent en charge ces services. Pour connaître la disponibilité la plus récente par région, consultez la [liste des services AWS régionaux](#).

3. Sur la page Create stack, vérifiez que le modèle correct URL se trouve dans la zone de URL texte Amazon S3, puis choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives à la dénomination [IAMdes STS](#) caractères, reportez-vous au Guide de l'AWS Identity and Access Management utilisateur.
5. Sur la page Paramètres, spécifiez les paramètres suivants et choisissez Next.

Paramètre	Par défaut	Description
Indiquez le nom du LogGroup à utiliser pour créer des filtres métriques et des alarmes	<i>&lt;Requires input&gt;</i>	Spécifiez le nom d'un groupe CloudWatch Logs dans lequel CloudTrail les API appels sont enregistrés. Ceci

Paramètre	Par défaut	Description
		est utilisé pour les corrections CIS 3.1-3.14.
Load SC Member Stack	yes	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles SC.
Charger la pile de AFSBP membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des FSBP contrôles.
Charger CIS12 une pile de membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles CIS12 0.
Charger CIS14 une pile de membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles CIS14 0.
Charger une pile de CIS3 100 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles CIS3 00.
Charger la pile de PC1321 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des PC1321 contrôles.
Charger la pile de NIST membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des NIST contrôles.

Paramètre	Par défaut	Description
Création d'un compartiment S3 pour la journalisation des audits Redshift	no	Indiquez yes si le compartiment S3 doit être créé pour la correction FSBP RedShift .4. Pour plus de détails sur le compartiment S3 et la correction, consultez la correction <a href="#">Redshift.4 dans le guide de l'utilisateur</a> .AWS Security Hub
Compte administrateur Sec Hub	<i>&lt;Requires input&gt;</i>	Entrez l'identifiant de compte à 12 chiffres du compte administrateur du AWS Security Hub.
Namespace	<i>&lt;Requires input&gt;</i>	Entrez une chaîne de 9 caractères alphanumériques minuscules maximum. Cette chaîne fait partie des noms de IAM rôles et du compartiment Action Log S3. Utilisez la même valeur pour le déploiement de la pile de membres et le déploiement de la pile de rôles des membres. Cette chaîne doit respecter les règles de dénomination Amazon S3 pour les compartiments S3 à usage général.

Paramètre	Par défaut	Description
EnableCloudTrailForASRActionLog	no	Indiquez yes si vous souhaitez surveiller les événements de gestion menés par la solution sur le CloudWatch tableau de bord. La solution crée une CloudTrail trace dans chaque compte membre que vous sélectionnez. Consultez la section <a href="#">Coût</a> pour comprendre les coûts supplémentaires que cela entraîne.

- Sur la page Configurer les options de pile, choisissez Suivant.
- Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera AWS Identity and Access Management (IAM) des ressources.
- Sélectionnez Create stack (Créer une pile) pour déployer la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le COMPLETE statut CREATE \_ dans 15 minutes environ.

## Étape 4 : (Facultatif) Ajustez les mesures correctives disponibles

Si vous souhaitez supprimer des corrections spécifiques d'un compte membre, vous pouvez le faire en mettant à jour la pile imbriquée pour la norme de sécurité. Pour des raisons de simplicité, les options de pile imbriquée ne sont pas propagées à la pile racine.

- Connectez-vous à la [AWS CloudFormation console](#) et sélectionnez la pile imbriquée.
- Choisissez Mettre à jour.
- Sélectionnez Mettre à jour la pile imbriquée, puis Mettre à jour la pile.

### Update sharr-v130-rc1-member-PlaybookMemberStackPCI321-LWXPIU3B3J89? ✕

**It is recommended to update through the root stack**  
Updating a nested stack may result in an unstable state where the nested stack is out-of-sync with its root stack. [Learn more](#) 

Go to root stack (recommended)

Update nested stack

Cancel Update stack

#### Mettre à jour la pile imbriquée

- Sélectionnez Utiliser le modèle actuel, puis cliquez sur Suivant.
- Ajustez les mesures correctives disponibles. Modifiez les valeurs des commandes souhaitées par Available et des commandes indésirables par. Not available

#### Note

La désactivation d'une correction supprime le manuel de correction des solutions pour la norme et le contrôle de sécurité.

- Sur la page Configurer les options de pile, choisissez Suivant.
- Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera AWS Identity and Access Management (IAM) des ressources.
- Choisissez Mettre à jour la pile.

Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le COMPLETE statut CREATE \_ dans 15 minutes environ.

# Surveillez la solution avec Service Catalog AppRegistry

Cette solution inclut une AppRegistry ressource Service Catalog pour enregistrer le CloudFormation modèle et les ressources sous-jacentes en tant qu'application dans [Service Catalog AppRegistry](#) et [AWS Systems Manager Application Manager](#).

AWS Systems Manager Application Manager vous donne une vue d'ensemble de cette solution et de ses ressources au niveau de l'application, afin que vous puissiez :

- Surveillez ses ressources, les coûts des ressources déployées sur plusieurs piles et Comptes AWS les journaux associés à cette solution à partir d'un emplacement central.
- Affichez les données opérationnelles relatives aux ressources de cette solution (telles que l'état du déploiement, les CloudWatch alarmes, les configurations des ressources et les problèmes opérationnels) dans le contexte d'une application.

La figure suivante illustre un exemple de vue d'application pour la pile de solutions dans Application Manager.

The screenshot displays the AWS Systems Manager Application Manager console. On the left, a sidebar shows a list of components under 'Components (2)', with 'AWS-Systems-Manager-Application-Manager' and 'AWS-Systems-Manager-A' listed. The main content area is titled 'AWS-Systems-Manager-Application-Manager' and includes a 'Start runbook' button. Below the title is the 'Application information' section, which contains a 'View in AppRegistry' button and details such as 'Application type: AWS-AppRegistry', 'Name: AWS-Systems-Manager-Application-Manager', and 'Application monitoring: Not enabled'. A description states: 'Service Catalog application to track and manage all your resources for the solution'. A navigation bar below this section includes tabs for Overview, Resources, Instances, Compliance, Monitoring, OpsItems, Logs, Runbooks, and Cost. At the bottom, there are two summary cards: 'Insights and Alarms' with a 'View all' button and 'Cost' with a 'View all' button. The cost card shows 'Cost (USD)' with a dash below it.

Pile de solutions dans le gestionnaire d'applications

# Utiliser CloudWatch Application Insights

Cette solution s'intègre automatiquement à CloudWatch Application Insights lors du déploiement. CloudWatch Application Insights vous aide à voir et à comprendre l'état de santé et les performances de la solution en :

- Découverte et surveillance automatiques des principales ressources des applications.
- Création d'alarmes personnalisées pour identifier de manière proactive les problèmes potentiels.
- Génération automatique de Systems Manager OpsItems lorsque des anomalies ou des défaillances sont détectées. Il OpsItems s'agit de notifications exploitables qui vous informent rapidement des problèmes affectant la solution.

Suivez ces étapes pour consulter le tableau de bord de surveillance d' CloudWatch Application Insights, où vous pouvez consulter l'état de santé de la solution et surveiller les composants clés via des tableaux de bord et des alarmes préconfigurés.

1. Accédez à la [console CloudWatch](#) .
2. Choisissez l'onglet Insights, puis sélectionnez Application Insights.
3. Choisissez l'onglet Applications, puis sélectionnez l'application associée à la solution.

Vous pouvez également importer le CloudWatch tableau de bord de la solution pour consolider votre surveillance de l'état de santé de la solution. Sur le tableau de bord des applications de la solution dans CloudWatch Application Insights, procédez comme suit :

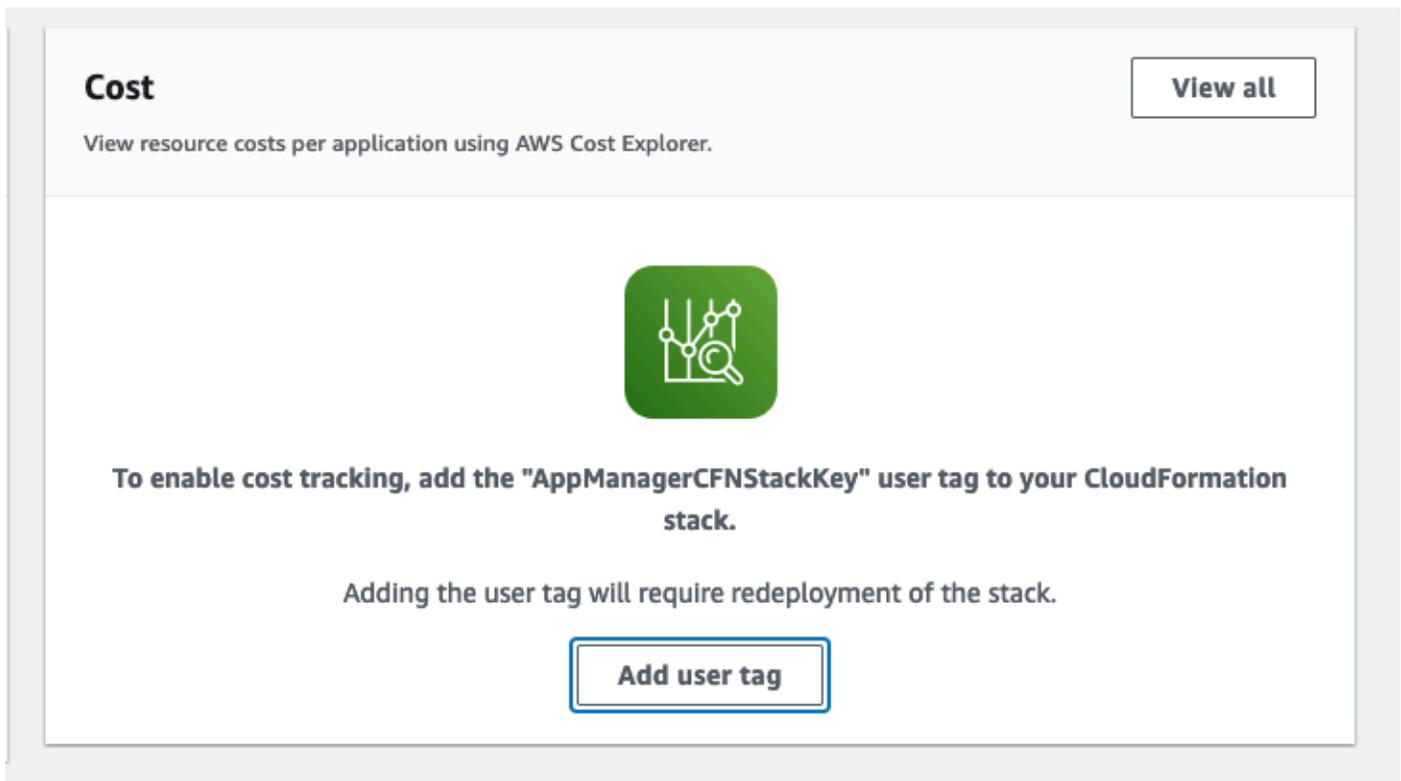
1. Choisissez l'onglet CloudWatch Tableau de bord personnalisé.
2. Choisissez Importer le CloudWatch tableau de bord.
3. Dans le champ de recherche `ASR-Remediation-Metrics-Dashboard`, entrez et sélectionnez la réponse de sécurité automatisée sur le AWS tableau de bord.
4. Choisissez Import (Importer).

Vous pouvez désormais consulter le tableau de bord CloudWatch Application Insights et le tableau de bord personnalisé de la solution dans la console CloudWatch Application Insights, sans avoir à passer d'une page à l'autre.

## Confirmez les étiquettes de coût associées à la solution

Après avoir activé les balises de répartition des coûts associées à la solution, vous devez confirmer les balises de répartition des coûts pour connaître les coûts de cette solution. Pour confirmer les balises de répartition des coûts :

1. Connectez-vous à la [console Systems Manager](#).
2. Dans le volet de navigation, choisissez Application Manager.
3. Dans Applications, choisissez le nom de l'application pour cette solution, puis sélectionnez-la.
4. Dans l'onglet Aperçu, dans Coût, sélectionnez Ajouter un tag utilisateur.



5. Sur la page Ajouter un tag utilisateur, entrez `confirm`, puis sélectionnez Ajouter un tag utilisateur.

Le processus d'activation peut prendre jusqu'à 24 heures et les données du tag peuvent apparaître.

## Activer les balises de répartition des coûts associées à la solution

Après avoir confirmé les étiquettes de coût associées à cette solution, vous devez activer les balises de répartition des coûts pour voir les coûts de cette solution. Les balises de répartition des coûts ne peuvent être activées qu'à partir du compte de gestion de l'organisation.

Pour activer les balises de répartition des coûts :

1. Connectez-vous à la [console AWS Billing and Cost Management and Cost Management](#).
2. Dans le volet de navigation, sélectionnez Balises de répartition des coûts.
3. Sur la page Balises de répartition des coûts, filtrez le AppManagerCFNStackKey tag, puis sélectionnez-le parmi les résultats affichés.
4. Choisissez Activer.

## AWS Cost Explorer

Vous pouvez consulter l'aperçu des coûts associés à l'application et aux composants de l'application dans la console Application Manager grâce à l'intégration à AWS Cost Explorer. Cost Explorer vous aide à gérer les coûts en fournissant une vue des coûts et de l'utilisation de vos AWS ressources au fil du temps.

1. Connectez-vous à la [console de gestion des AWS coûts](#).
2. Dans le menu de navigation, sélectionnez Cost Explorer pour visualiser les coûts et l'utilisation de la solution au fil du temps.

# Surveillez les opérations de la solution à l'aide d'un CloudWatch tableau de bord Amazon

Cette solution inclut des métriques personnalisées et des alarmes affichées sur un CloudWatch tableau de bord Amazon.

Le CloudWatch tableau de bord et les alarmes surveillent le fonctionnement de la solution et alertent en cas de problème potentiel.

## Activation CloudWatch des métriques, des alarmes et du tableau de bord

Il existe quatre paramètres CloudFormation de modèle pour les CloudWatch fonctionnalités.

The screenshot shows a CloudFormation console interface with four parameters for CloudWatch functionality. Each parameter has a title, a description, and a value field.

- CloudWatch Metrics**
  - UseCloudWatchMetrics**: Enable collection of operational metrics and create a CloudWatch dashboard to monitor solution operations. Value: yes.
  - UseCloudWatchMetricsAlarms**: Create CloudWatch Alarms for gathered metrics. Value: yes.
  - RemediationFailureAlarmThreshold**: Percentage of failures in one period (default period is 1 day) to trigger the remediation failures alarm for a given control ID. E.g., to specify 20% then enter the number 20. Value: 5.
  - EnableEnhancedCloudWatchMetrics**: Enable collection of metrics per Control ID in addition to standard metrics. You must also select 'yes' for UseCloudWatchMetrics to enable enhanced metric collection. The added cost of these additional custom metrics could be up to \$65/month. Value: no.

1. **UseCloudWatchMetrics**— Paramétrer cette option pour yes permettre la collecte de métriques opérationnelles et créer un CloudWatch tableau de bord pour visualiser ces métriques.
2. **UseCloudWatchAlarms**— Réglez ce paramètre pour yes activer les alarmes par défaut de la solution.
3. **RemediationFailureAlarmThreshold**— Le pourcentage de remédiations défectueuses au cours d'une période pendant laquelle une alarme a été déclenchée.
4. **EnableEnhancedCloudWatchMetrics**— Définissez ce paramètre sur yes pour collecter des métriques individuelles par ID de contrôle. Par défaut, ce paramètre est défini sur no, de sorte que

seules les mesures relatives au nombre total de mesures correctives pour l'ensemble du contrôle IDs sont collectées. Les mesures et alarmes individuelles par ID de contrôle entraînent un coût supplémentaire.

## Utilisation du CloudWatch tableau de bord

Pour consulter le tableau de bord :

1. Accédez à Amazon, CloudWatch puis à Dashboards.
2. Sélectionnez le tableau de bord nommé « ASR -Remediation-Metrics-Dashboard ».

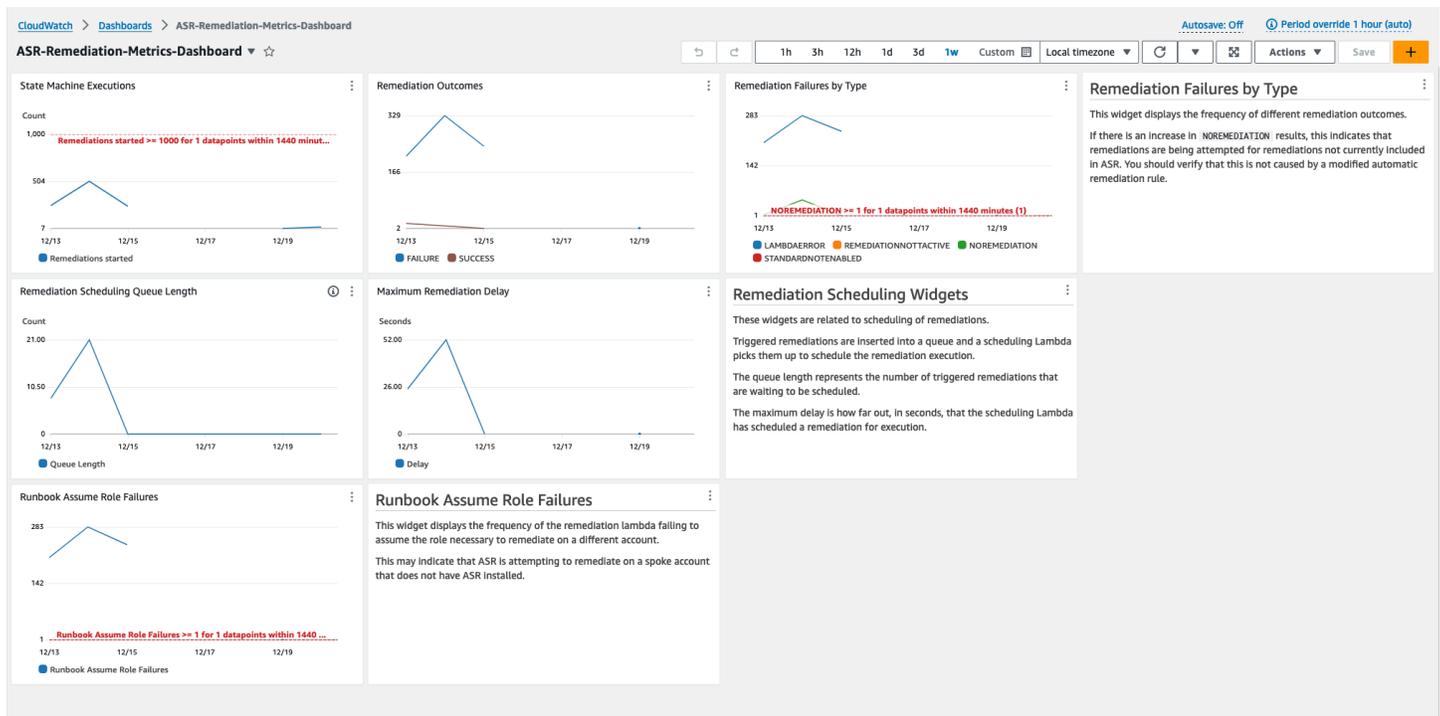
Le CloudWatch tableau de bord contient les sections suivantes :

1. Nombre total de corrections réussies : vous donne un aperçu du nombre de conclusions du Security Hub qui ont été corrigées avec succès par la solution.
2. Défaillances de correction : indique le nombre de mesures correctives qui ont échoué, au total et en pourcentage, ainsi que la cause de l'échec. Un nombre élevé de défaillances peut indiquer un problème technique lié à la solution que vous devrez peut-être étudier plus en détail.
3. Succès ou échec de la correction par ID de contrôle : si vous avez activé les métriques améliorées au moment du déploiement, cette section répertorie les résultats de la correction par ID de contrôle. Lorsque la section Défaillances de correction indique un taux d'échec élevé en général, cette section indique si les défaillances sont réparties entre de nombreux contrôles IDs ou si seuls certains contrôles IDs échouent.
4. Défaillances du rôle Runbook Assume : indique le nombre d'échecs survenus à la suite de tentatives de correction sur des comptes sur lesquels le rôle de membre de la solution n'est pas installé. Les échecs répétés dus à des tentatives de correction automatisées en raison de rôles manquants entraînent des coûts inutiles. Atténuez ce problème en installant la [pile de rôles de membre](#) dans les comptes concernés, en [désactivant toutes les EventBridge règles](#) créées par la solution ou en [dissociant le compte](#) dans Security Hub.
5. Actions de gestion de Cloud Trail par ASR : répertorie les actions de gestion effectuées par la solution sur tous les comptes membres pour lesquels vous avez activé les journaux d'actions avec le EnableCloudTrailForASRActionLogparamètre au moment du déploiement. Lorsque vous observez des modifications inattendues des ressources dans l'un de vos AWS comptes, ce widget peut vous aider à comprendre si les ressources ont été modifiées par la solution.

Le CloudWatch tableau de bord est également doté d'alarmes prédéfinies qui signalent les erreurs opérationnelles courantes.

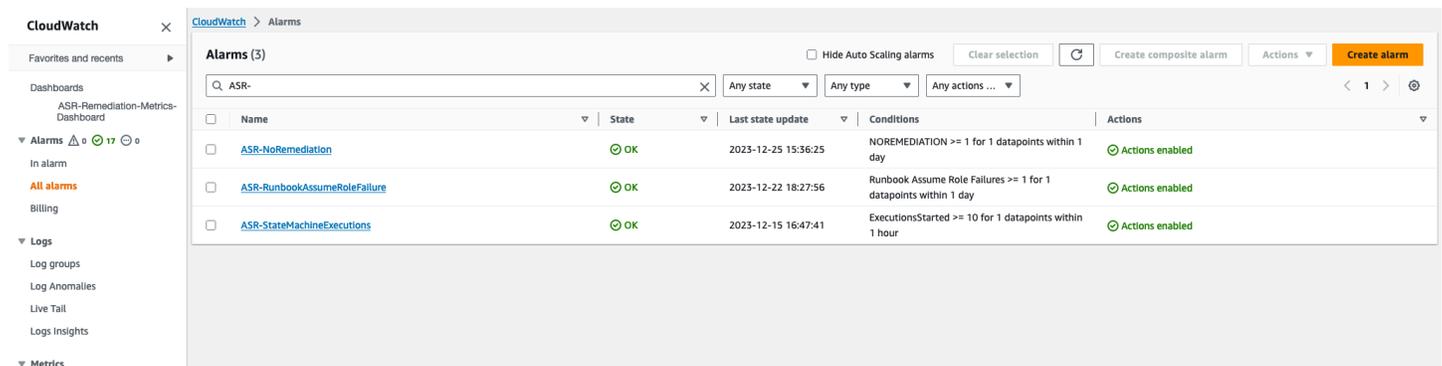
1. Exécutions par State Machine > 1 000 sur une période de 24 heures.
  - a. Une forte augmentation du nombre d'exécutions de mesures correctives peut indiquer qu'une règle événementielle est déclenchée plus souvent que prévu.
  - b. Le seuil peut être modifié à l'aide du CloudFormation paramètre.
2. Défaillances de correction par type = NOREMEDIATION > 0
  - a. Des mesures correctives sont en cours de tentative pour les mesures correctives qui ne sont pas incluses dans. ASR Cela peut indiquer qu'une règle d'événement a été modifiée pour inclure plus que les corrections prévues.
3. Défaillances du rôle Runbook Assume > 0
  - a. Des mesures correctives sont en cours de tentative sur des comptes ou des régions où la solution n'est pas correctement déployée. Cela peut indiquer qu'une règle d'événement a été modifiée pour inclure plus de comptes que prévu.

Tous les seuils d'alarme peuvent être modifiés en fonction des besoins de déploiement individuels.



## Modification des seuils d'alarme

1. Accédez à Amazon CloudWatch -> Alarmes -> Toutes les alarmes.
2. Choisissez l'alarme que vous souhaitez modifier, puis sélectionnez Actions -> Modifier.



The screenshot shows the Amazon CloudWatch Alarms console. The left sidebar contains navigation options: Dashboards, Alarms (17), In alarm, All alarms, Billing, Logs, Log groups, Log Anomalies, Live Tail, Logs Insights, and Metrics. The main content area displays a table of alarms with the following data:

Name	State	Last state update	Conditions	Actions
<a href="#">ASR-NoRemediation</a>	OK	2023-12-25 15:36:25	NOREMEDIATION >= 1 for 1 datapoints within 1 day	Actions enabled
<a href="#">ASR-RunbookAssumeRoleFailure</a>	OK	2023-12-22 18:27:56	Runbook Assume Role Failures >= 1 for 1 datapoints within 1 day	Actions enabled
<a href="#">ASR-StateMachineExecutions</a>	OK	2023-12-15 16:47:41	ExecutionsStarted >= 10 for 1 datapoints within 1 hour	Actions enabled

3. Modifiez le seuil à la valeur souhaitée et enregistrez.

CloudWatch > Alarms > ASR-StateMachineExecutions > Edit

Step 1 - optional  
Specify metric and conditions

Step 2 - optional  
[Configure actions](#)

Step 3 - optional  
[Add name and description](#)

Step 4 - optional  
[Preview and create](#)

## Specify metric and conditions - optional

### Metric

**Graph**  
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 day.

Count

1,000

501

1

01/05 01/07 01/09 01/11

ExecutionsStarted

**Namespace**  
AWS/States

**Metric name**  
ExecutionsStarted

**StateMachineArn**  
arn:aws:states:us-east-1:221128147805:stateMachine:S

**Statistic**  
Sum

**Period**  
1 day

### Conditions

**Threshold type**

**Static**  
Use a value as a threshold

**Anomaly detection**  
Use a band as a threshold

**Whenever ExecutionsStarted is...**  
Define the alarm condition.

**Greater**  
> threshold

**Greater/Equal**  
>= threshold

**Lower/Equal**  
<= threshold

**Lower**  
< threshold

**than...**  
Define the threshold value.

1000

Must be a number

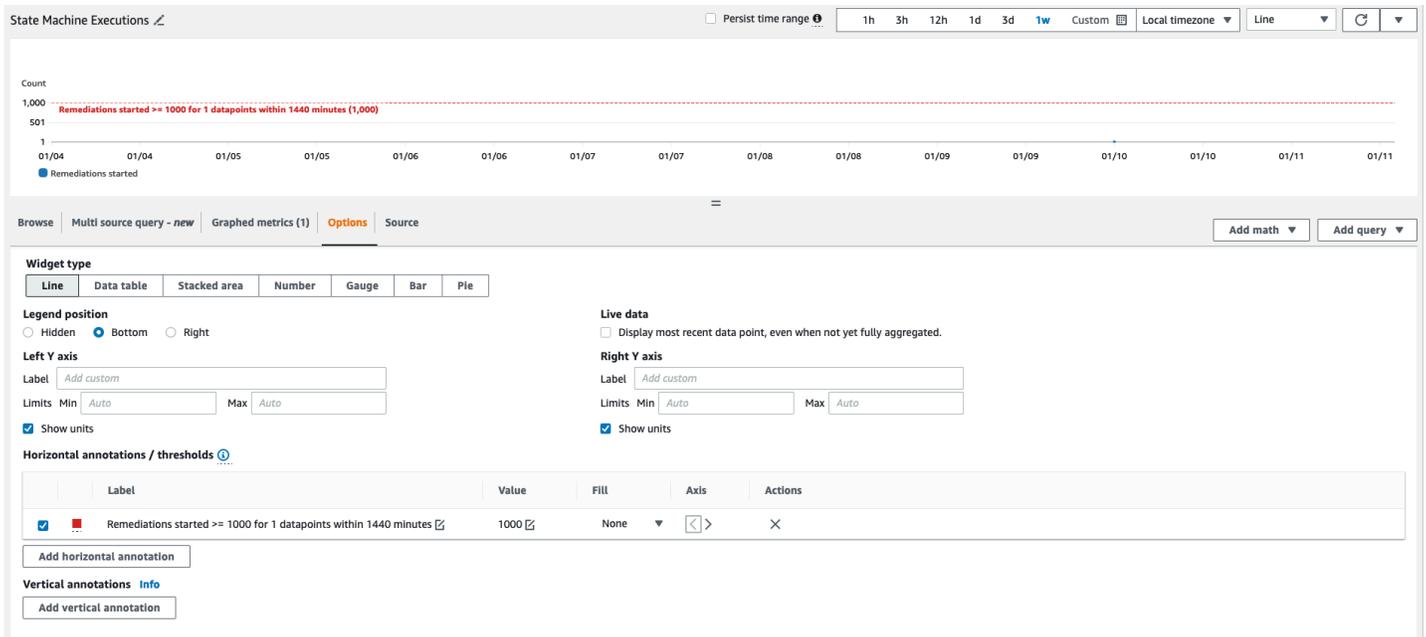
► **Additional configuration**

Cancel Skip to Preview and create **Next**

4. Accédez au CloudWatch tableau de bord pour modifier les graphiques en fonction des nouveaux paramètres.

a. Sélectionnez les points de suspension en haut à droite du widget correspondant.

- b. Tâche de sélection Modifier.
- c. Accédez à l'onglet Options.
- d. Modifiez l'annotation d'alarme pour qu'elle corresponde aux nouveaux paramètres.



## Abonnement aux notifications d'alarme

Dans le compte administrateur, abonnez-vous à la SNS rubrique Amazon créée par la pile d'administrateurs, SO0111- ASR \_Alarm\_Topic. Cela vous avertira lorsqu'une alarme entre dans l'ALARMétat.

# Mettre à jour la solution

## Mise à niveau à partir de versions antérieures à la v1.4

Si vous avez déjà déployé la solution avant la version v1.4.x, désinstallez-la, puis installez la dernière version :

1. Désinstallez la solution précédemment déployée. Reportez-vous à la section [Désinstaller la solution](#).
2. Lancez le dernier modèle. Reportez-vous à la section [Déployer la solution](#).

### Note

Si vous effectuez une mise à niveau de la version v1.2.1 ou antérieure vers la version v1.3.0 ou ultérieure, définissez Use existing Orchestrator Log Group sur. No Si vous réinstallez la version v1.3.0 ou une version ultérieure, vous pouvez sélectionner Yes cette option. Cette option vous permet de continuer à vous connecter au même groupe de journaux pour Orchestrator Step Functions.

## Mise à niveau depuis la version 1.4 et les versions ultérieures

Si vous effectuez une mise à niveau depuis la version v1.4.x, mettez à jour toutes les piles ou StackSets procédez comme suit :

1. Mettez à jour la pile du compte administrateur du Security Hub à l'aide du [dernier modèle](#).
2. Dans chaque compte membre, mettez à jour les autorisations à partir du dernier modèle.
3. Dans chaque compte membre, dans toutes les régions où il est actuellement déployé, mettez à jour la pile de membres à partir du dernier modèle.

## Mise à niveau depuis la version 2.0.x

Si vous effectuez une mise à niveau depuis la version 2.0.x, passez à la version 2.1.2 ou ultérieure. La mise à jour vers v2.1.0 - v2.1.1 échouera. CloudFormation

# Résolution des problèmes

[La résolution des problèmes connus](#) fournit des instructions pour atténuer les erreurs connues. Si ces instructions ne répondent pas à votre problème, [Contacter le AWS Support](#) fournit des instructions pour ouvrir un dossier d'AWSassistance pour cette solution.

## Journaux de solutions

Cette section contient des informations de résolution des problèmes pour cette solution, voir la navigation de gauche pour les rubriques.

Cette solution collecte les résultats des runbooks de correction, qui s'exécutent sous AWS Systems Manager, et enregistre le résultat S00111-SHARR dans le groupe CloudWatch Logs du compte AWS Security Hub administrateur. Il y a un flux par contrôle et par jour.

The Orchestrator Step Functions enregistre toutes les transitions par étapes dans le groupe S00111-SHARR-0rchestrator CloudWatch Logs du compte administrateur du AWS Security Hub. Ce journal est une piste d'audit permettant d'enregistrer les transitions d'état pour chaque instance des Step Functions. Il existe un flux de log par exécution de Step Functions.

Les deux groupes de journaux sont chiffrés à l'aide d'une clé AWS KMS Customer-Manager ( )CMK.

Les informations de dépannage suivantes utilisent le groupe de S00111-SHARR journaux. Utilisez ce journal, ainsi que la console AWS Systems Manager Automation, les journaux Automation Executions, la console Step Function et les journaux Lambda pour résoudre les problèmes.

Si une correction échoue, un message similaire au suivant sera enregistré S00111-SHARR dans le flux de journal pour la norme, le contrôle et la date. Par exemple : CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
vpc-0e92bbe911cf08acb)
```

Les messages suivants fournissent des informations supplémentaires. Ce résultat provient du SHARR manuel d'exécution relatif à la norme et au contrôle de sécurité. Par exemple : SHARR- CIS \_1.2.0\_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.
```

Ces informations vous indiquent l'échec, qui dans ce cas était dû à une automatisation secondaire exécutée sur le compte du membre. Pour résoudre ce problème, vous devez vous connecter au compte du membre ( AWS Management Console à partir du message ci-dessus) AWS Systems Manager, accéder à Automation et examiner le résultat du journal pour l'identifiant eecdef79-9111-4532-921a-e098549f525 d'exécution.

## Résolution des problèmes connus

- Problème : Le déploiement de la solution échoue avec un message d'erreur indiquant que les ressources sont déjà disponibles sur Amazon CloudWatch.

Solution : recherchez un message d'erreur dans la section CloudFormation ressources/ événements indiquant que des groupes de journaux existent déjà. Les modèles SHARR de déploiement permettent de réutiliser les groupes de journaux existants. Vérifiez que vous avez sélectionné Réutiliser.

- Problème : la solution ne parvient pas à être déployée avec une erreur dans une pile imbriquée de playbooks où une EventBridge règle ne parvient pas à être créée

Résolution : vous avez probablement atteint le [quota de EventBridge règles compte](#) tenu du nombre de playbooks déployés. Vous pouvez éviter cela en utilisant les [résultats de contrôle consolidés](#) dans Security Hub associés au playbook SC de cette solution, en déployant uniquement les playbooks correspondant aux normes utilisées ou en demandant une augmentation du quota de EventBridge règles.

- Problème : J'utilise Security Hub dans plusieurs régions avec le même compte. Je souhaite déployer cette solution dans plusieurs régions.

Solution : déployez la pile d'administrateurs dans le même compte et dans la même région que votre administrateur Security Hub. Installez le modèle de membre dans chaque compte et région dans lesquels un membre du Security Hub est configuré. Activez l'agrégation dans le Security Hub.

- Problème : Immédiatement après le déploiement, le SO0111- SHARR -Orchestrator échoue dans l'état du document Get Automation avec une erreur 502 : « Lambda n'a pas pu déchiffrer les variables d'environnement car l'accès a été refusé. KMS Vérifiez les KMS principaux paramètres de la fonction. KMS Exception : UnrecognizedClientException KMS Message : le jeton de sécurité

inclus dans la demande n'est pas valide. (Service : AWSLambda ; Code d'état : 502 ; Code d'erreur : KMSAccessDeniedException ; ID de demande :... »

Résolution : attendez environ 10 minutes pour que la solution se stabilise avant d'exécuter les corrections. Si le problème persiste, ouvrez un ticket d'assistance ou un GitHub problème.

- Problème : J'ai essayé de corriger une constatation, mais rien ne s'est passé.

Résolution : Consultez les notes relatives à la constatation pour connaître les raisons pour lesquelles elle n'a pas été corrigée. L'une des causes les plus fréquentes est qu'aucune correction automatique n'est apportée au résultat. À l'heure actuelle, il n'existe aucun moyen de fournir un feedback direct à l'utilisateur lorsqu'il n'existe aucune correction autre que par le biais des notes. Consultez les journaux des solutions. Ouvrez CloudWatch Logs dans la console. Trouvez le groupe SO0111- SHARR CloudWatch Logs. Triez la liste de manière à ce que les derniers streams mis à jour apparaissent en premier. Sélectionnez le flux de journal correspondant à la recherche que vous avez tenté d'exécuter. Vous devriez y trouver des erreurs. L'échec peut s'expliquer notamment par une inadéquation entre le contrôle des résultats et le contrôle des mesures correctives, par la correction entre comptes (non encore prise en charge) ou par le fait que le résultat a déjà été corrigé. Si vous ne parvenez pas à déterminer la raison de l'échec, collectez les journaux et ouvrez un ticket d'assistance.

- Problème : Après le lancement d'une correction, l'état de la console Security Hub n'est pas mis à jour.

Résolution : La console Security Hub ne se met pas à jour automatiquement. Rafraîchissez la vue actuelle. L'état de la découverte doit être mis à jour. Plusieurs heures peuvent être nécessaires pour que le résultat passe du statut d'échec à celui de réussite. Les résultats sont créés à partir des données d'événements envoyées par d'autres services, tels que AWS Config, à AWS Security Hub. Le délai avant la réévaluation d'une règle dépend du service sous-jacent. Si cela ne résout pas le problème, reportez-vous à la résolution précédente pour « J'ai essayé de corriger une constatation mais rien ne s'est passé ».

- Problème : La fonction d'étape de l'orchestrateur échoue dans Get Automation Document State : une erreur s'est produite (AccessDenied) lors de l'appel de l' AssumeRole opération.

Résolution : Le modèle de membre n'a pas été installé dans le compte membre où l'on SHARR tente de remédier à une constatation. Suivez les instructions de déploiement du modèle de membre.

- Problème : le runbook Config.1 échoue car l'enregistreur ou le canal de diffusion existent déjà.

Résolution : Inspectez soigneusement vos AWS Config paramètres pour vous assurer que Config est correctement configuré. La correction automatique ne permet pas de corriger les paramètres de AWS configuration existants dans certains cas.

- Problème : la correction a réussi mais renvoie le message "No output available yet because the step is not successfully executed."

Résolution : il s'agit d'un problème connu dans cette version, à savoir que certains runbooks de correction ne renvoient pas de réponse. Les runbooks de correction échoueront correctement et signaleront la solution s'ils ne fonctionnent pas.

- Problème : La résolution a échoué et a envoyé une trace de pile.

Solution : Nous manquons parfois l'occasion de gérer une condition d'erreur qui entraîne un suivi de la pile plutôt qu'un message d'erreur. Essayez de résoudre le problème à partir des données de suivi. Ouvrez un ticket d'assistance si vous avez besoin d'aide.

- Problème : la suppression de la pile v1.3.0 a échoué sur la ressource Custom Action.

Résolution : La suppression du modèle d'administration peut échouer lors de la suppression de l'action personnalisée. Il s'agit d'un problème connu qui sera résolu dans la prochaine version. Si cela se produit :

1. Connectez-vous à la [console de gestion du AWS Security Hub](#).
2. Dans le compte administrateur, allez dans Réglages.
3. Sélectionnez l'onglet Actions personnalisées
4. Supprimez manuellement l'entrée Corriger avecSHARR.
5. Supprimez à nouveau la pile.

- Problème : Après le redéploiement de la pile d'administration, la fonction step échoue. AssumeRole

Résolution : le redéploiement de la pile d'administrateurs rompt le lien de confiance entre le rôle d'administrateur dans le compte d'administrateur et le rôle de membre dans les comptes de membres. Vous devez redéployer la pile des rôles des membres dans tous les comptes membres.

- Problème : les CIS corrections 3.x ne s'affichent pas PASSED après plus de 24 heures.

Solution : Cela se produit fréquemment si vous n'êtes pas abonné au S00111-SHARR\_LocalAlarmNotification SNS sujet dans le compte membre.

## Problèmes liés à des mesures correctives spécifiques

S etSSLBucket Policy échoue avec une AccessDenied erreur

Contrôles associés : AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI .S3.5, v1.4.0 2.1.2, SC v2.0.0 S3.5 CIS

Problème : La etSSLBucket politique S échoue avec une AccessDenied erreur :

Une erreur s'est produite (AccessDenied) lors de l'appel de l' PutBucketPolicyopération : Accès refusé

Si le paramètre Bloquer l'accès public a été activé pour un bucket, les tentatives de mise en place d'une politique de bucket incluant des instructions autorisant l'accès public échoueront avec cette erreur. Cet état peut être atteint en définissant une politique de compartiment contenant de telles instructions, puis en activant le blocage de l'accès public pour ce compartiment.

La correction ConfigureS3 BucketPublicAccessBlock (commandes associées : AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI .S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) peut également placer un bucket dans cet état car elle définit le paramètre de blocage de l'accès public sans modifier la politique du bucket.

La etSSLBucket politique S ajoute une déclaration à la politique des compartiments pour refuser les demandes qui ne sont pas utiliséesSSL. Cela ne modifie pas les autres instructions de la politique. Ainsi, si certaines instructions autorisent l'accès du public, la correction échouera en tentant de mettre en place la politique de compartiment modifiée qui inclut toujours ces instructions.

Résolution : modifiez la politique du compartiment pour supprimer les instructions qui autorisent l'accès public en conflit avec le paramètre de blocage de l'accès public sur le compartiment.

## PuTS3 échoue BucketPolicyDeny

Contrôles associés : AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9 (1), .800-53.r5 CM-2 NIST

Problème : le PuTS3 BucketPolicyDeny avec l'erreur suivante :

Unable to create an explicit deny statement for {bucket\_name}.

Si les principes de toutes les politiques du compartiment cible sont « \* », la solution ne peut pas ajouter la politique de refus au compartiment cible car cela bloquerait toutes les actions du compartiment pour tous les principaux.

Solution : modifiez la politique des compartiments pour autoriser les actions sur des comptes spécifiques au lieu d'utiliser des principes « \* » et limitez les actions refusées.

## Comment désactiver la solution

En cas d'incident, il se peut que vous deviez désactiver la solution sans supprimer aucune infrastructure. Ces scénarios expliquent comment désactiver les différents composants de la solution.

Scénario 1 : désactivez la correction automatique pour un seul contrôle.

1. Accédez à EventBridge dans la [AWS CloudFormation console](#).
2. Sélectionnez Règles dans la barre latérale.
3. Sélectionnez le bus d'événements par défaut et recherchez le contrôle que vous souhaitez désactiver.
4. Sélectionnez la règle et cliquez sur le bouton Désactiver.

Scénario 2 : désactivez la correction automatique pour tous les contrôles.

1. Accédez à EventBridge dans la console.
2. Sélectionnez Règles dans la barre latérale.
3. Sélectionnez le bus d'événements « par défaut » et sélectionnez toutes les règles ci-dessous.
4. Sélectionnez le bouton « Désactiver ». Notez que vous devrez peut-être effectuer cette opération pour plusieurs pages de règles.

Scénario 3 : désactiver la correction manuelle pour un compte

1. Accédez à EventBridge dans la console.
2. Sélectionnez Règles dans la barre latérale.
3. Sélectionnez le bus d'événements « par défaut » et recherchez « SHARR Remediate\_with\_\_ » CustomAction
4. Sélectionnez la règle et cliquez sur le bouton « Désactiver ».

# Contacteur AWS Support

Si vous bénéficiez [AWSdu Support aux développeurs](#), du [Support aux AWS AWS entreprises](#) ou du [Support aux entreprises](#), vous pouvez utiliser le Centre de support pour obtenir l'assistance d'experts sur cette solution. Les sections suivantes fournissent des instructions.

## Créer un dossier

1. Connectez-vous au [Centre de Support](#).
2. Choisissez Create case (Créer une demande).

## Comment pouvons-nous vous aider ?

1. Choisissez Technique.
2. Dans le champ Service, sélectionnez Solutions.
3. Dans Catégorie, sélectionnez Autres solutions.
4. Pour Severity, sélectionnez l'option qui correspond le mieux à votre cas d'utilisation.
5. Lorsque vous entrez le service, la catégorie et la gravité, l'interface contient des liens vers des questions de dépannage courantes. Si vous ne parvenez pas à résoudre votre question à l'aide de ces liens, sélectionnez Étape suivante : Informations supplémentaires.

## Informations supplémentaires

1. Dans le champ Objet, saisissez un texte résumant votre question ou problème.
2. Dans le champ Description, décrivez le problème en détail.
3. Choisissez Joindre des fichiers.
4. Joignez les informations AWS Support nécessaires au traitement de la demande.

## Aidez-nous à résoudre votre cas plus rapidement

1. Entrez les informations demandées.
2. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).

## Résolvez maintenant ou contactez-nous

1. Passez en revue les solutions Solve now.
2. Si vous ne parvenez pas à résoudre votre problème avec ces solutions, choisissez Contactez-nous, entrez les informations demandées, puis choisissez Soumettre.

# Désinstallez la solution

Utilisez la procédure suivante pour désinstaller la solution avec le AWS Management Console.

## V1.0.0-V1.2.1

Pour les versions v1.0.0 à v1.2.1, utilisez Service Catalog pour désinstaller et/ou Playbooks. CIS FSBP Avec la version v1.3.0, Service Catalog n'est plus utilisé.

1. Connectez-vous à la [AWS CloudFormation console](#) et accédez au compte principal Security Hub.
2. Choisissez Service Catalog pour mettre fin à tous les playbooks fournis, supprimer les groupes de sécurité, les rôles ou les utilisateurs.
3. Supprimez le `CISPermissions.template` modèle Spoke des comptes membres du Security Hub.
4. Supprimez le `AFSBPMemberStack.template` modèle Spoke des comptes d'administrateur et de membre du Security Hub.
5. Accédez au compte principal Security Hub, sélectionnez la pile d'installation de la solution, puis choisissez Supprimer.

### Note

CloudWatch Les journaux des groupes de journaux sont conservés. Nous vous recommandons de conserver ces journaux conformément à la politique de conservation des journaux de votre organisation.

## V1.3.x

1. `aws-sharr-member.template` Supprimez-le de chaque compte membre.
2. `aws-sharr-admin.template` Supprimez-le du compte administrateur.

**Note**

La suppression du modèle d'administration dans la version v1.3.0 échouera probablement lors de la suppression de l'action personnalisée. Il s'agit d'un problème connu qui sera résolu dans la prochaine version. Suivez les instructions suivantes pour résoudre ce problème :

1. Connectez-vous à la [console de gestion du AWS Security Hub](#).
2. Dans le compte administrateur, allez dans Paramètres.
3. Sélectionnez l'onglet Actions personnalisées.
4. Supprimez manuellement l'entrée Corriger avec SHARR.
5. Supprimez à nouveau la pile.

## V1.4.0 et versions ultérieures

### Déploiement en pile

1. `aws-sharr-member.template` Supprimez-le de chaque compte membre.
2. `aws-sharr-admin.template` Supprimez-le du compte administrateur.

### StackSet déploiement

Pour chacun StackSet, supprimez les piles, puis retirez-les StackSet dans l'ordre inverse du déploiement.

Notez que IAM les rôles du `aws-sharr-member-roles.template` sont conservés même si le modèle est supprimé. Cela permet aux correctifs utilisant ces rôles de continuer à fonctionner. Ces rôles SO0111-\* peuvent être supprimés manuellement après avoir vérifié qu'ils ne sont plus utilisés par des mesures correctives actives, telles que la CloudWatch journalisation ou la surveillance CloudTrail améliorée. RDS

# Guide de l'administrateur

## Activation et désactivation de certaines parties de la solution

En tant qu'administrateur de solution, vous pouvez contrôler les fonctionnalités de la solution activées comme suit.

Où les piles de rôles des membres et des membres sont déployées :

- La pile d'administrateurs ne pourra initier des corrections (par le biais d'actions personnalisées ou de EventBridge règles entièrement automatisées) que dans les comptes dans lesquels les piles de membres et de rôles de membre ont été déployées avec le numéro de compte administrateur indiqué comme valeur de paramètre.
- Pour exempter complètement les comptes ou les régions du contrôle de la solution, ne déployez pas les piles de rôles des membres ou des membres sur ces comptes ou régions.

Configuration de l'agrégation de recherche de comptes et de régions dans Security Hub :

- La pile d'administrateurs ne pourra initier des corrections (par le biais d'actions personnalisées ou de EventBridge règles entièrement automatisées) que pour les résultats qui arrivent dans le compte administrateur et dans la région.
- Pour exempter complètement les comptes ou les régions du contrôle de la solution, n'incluez pas ces comptes ou régions pour envoyer les résultats au même compte administrateur et à la même région dans lesquels la pile d'administrateurs est déployée.

Quelles piles imbriquées standard sont déployées :

- La pile d'administrateurs ne pourra initier des corrections (par le biais d'actions personnalisées ou de EventBridge règles entièrement automatisées) que pour les contrôles dotés d'un manuel de contrôle déployé dans le compte membre et la région cibles. Ils sont déployés par la pile de membres pour chaque norme.
- La pile d'administration ne pourra lancer des corrections entièrement automatisées qu'à l'aide de EventBridge règles pour les contrôles dont les règles sont déployées par la pile d'administration pour cette norme. Ils sont déployés sur le compte administrateur.
- Pour des raisons de simplicité, nous vous recommandons de déployer les normes de manière cohérente sur vos comptes d'administrateur et de membre. Si la CIS v1.2.0 vous AWS FSBP

intéresse, déployez ces deux piles d'administration imbriquées sur le compte administrateur, et déployez ces deux piles de membres imbriquées sur chaque compte membre et région.

Quels runbooks Control sont déployés dans chaque pile de membres imbriquée :

- La pile d'administrateurs ne sera en mesure de lancer des corrections (par le biais d'actions personnalisées ou de EventBridge règles entièrement automatisées) que pour les contrôles dotés d'un manuel de contrôle déployé dans le compte membre cible et dans la région par la pile de membres pour chaque norme.
- Pour exercer un contrôle plus précis sur les contrôles activés pour une norme donnée, chaque pile imbriquée d'une norme possède des paramètres pour lesquels les runbooks de contrôle sont déployés. Définissez le paramètre d'un contrôle sur la valeur « NOT Disponible » pour annuler le déploiement de ce runbook de contrôle.

SSMParamètres d'activation et de désactivation des normes :

- La pile d'administration ne pourra initier des corrections (par le biais d'actions personnalisées ou de EventBridge règles entièrement automatisées) que pour les normes activées via le SSM paramètre déployé par la pile d'administration standard.
- Pour désactiver une norme, définissez la valeur du SSM paramètre avec le chemin « /Solutions/SO0111/<standard\_name>/<standard\_version>/status » sur « Non ».

## Exemples de SNS notifications

Lorsqu'une correction est initiée

```
{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control RDS.13 in account 111111111111",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
```

```

    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/finding/22222222-2222-2222-2222-222222222222"
  }
}

```

### En cas de réussite d'une correction

```

{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC control RDS.13 in account 111111111111: See Automation Execution output for details (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/finding/22222222-2222-2222-2222-222222222222"
  }
}

```

### En cas d'échec d'une correction

```

{
  "severity": "ERROR",
  "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC control RDS.13 in account 111111111111: See Automation Execution output for details (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {

```

```
"finding_id": "22222222-2222-2222-2222-222222222222",
"finding_description": "This control checks if automatic minor version upgrades are
enabled for the Amazon RDS database instance.",
"standard_name": "security-control",
"standard_version": "2.0.0",
"standard_control": "RDS.13",
"title": "RDS automatic minor version upgrades should be enabled",
"region": "us-east-1",
"account": "111111111111",
"finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
}
}
```

## Utilisez la solution

Il s'agit d'un didacticiel qui vous guidera lors de votre premier déploiement de ASR. Cela commencera par les conditions préalables au déploiement de la solution et se terminera par la correction des exemples trouvés dans un compte membre.

## Tutoriel : Démarrage avec Automated Security Response sur AWS

Il s'agit d'un didacticiel qui vous guidera tout au long de votre premier déploiement. Cela commencera par les conditions préalables au déploiement de la solution et se terminera par la correction des exemples trouvés dans un compte membre.

### Préparez les comptes

Afin de démontrer les capacités de correction entre comptes et entre régions de la solution, ce didacticiel utilisera deux comptes. Vous pouvez également déployer la solution sur un seul compte.

Les exemples suivants utilisent 11111111111 des comptes 22222222222 pour démontrer la solution. 11111111111 sera le compte administrateur et 22222222222 sera le compte membre. Nous mettrons en place la solution pour remédier aux problèmes liés aux ressources dans les régions us-east-1 et us-west-2.

Le tableau ci-dessous est un exemple illustrant les actions que nous entreprendrons pour chaque étape dans chaque compte et région.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
11111111111	Administrateur	Aucun	Aucun
22222222222	Membre	Aucun	Aucun

Le compte administrateur est le compte qui exécutera les actions d'administration de la solution, notamment le lancement manuel des corrections ou l'activation d'une correction entièrement automatisée avec EventBridge des règles. Ce compte doit également être le compte d'administrateur délégué de Security Hub pour tous les comptes dans lesquels vous souhaitez corriger les résultats, mais il n'est pas nécessaire et il ne doit pas être le compte administrateur AWS des Organisations de l'AWS organisation à laquelle appartiennent vos comptes.

## Activer AWS Config

Consultez la documentation suivante :

- [AWS Documentation de configuration](#)
- [AWS Tarification de Config](#)
- [Activation de AWS Config](#)

Activez AWS Config dans les deux comptes et dans les deux régions. Cela entraînera des frais.

### Important

Assurez-vous de sélectionner l'option « Inclure les ressources globales (par exemple, AWS IAM les ressources) ». Si vous ne sélectionnez pas cette option lors de l'activation de AWS Config, vous ne verrez pas les résultats relatifs aux ressources globales (par exemple AWS IAM les ressources)

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Activer AWS Config	Activer AWS Config
222222222222	Membre	Activer AWS Config	Activer AWS Config

## Activer le hub AWS de sécurité

Consultez la documentation suivante :

- [AWS Documentation du Security Hub](#)
- [AWS Tarification du Security Hub](#)
- [Activation AWS de Security Hub](#)

Activez AWS Security Hub dans les deux comptes et dans les deux régions. Cela entraînera des frais.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Activer AWS Security Hub	Activer AWS Security Hub
222222222222	Membre	Activer AWS Security Hub	Activer AWS Security Hub

## Permettre des résultats de contrôle consolidés

Consultez la documentation suivante :

- [Génération et mise à jour des résultats de contrôle](#)

Dans le cadre de ce didacticiel, nous allons démontrer l'utilisation de la solution en activant la fonction de résultats de contrôle consolidés de AWS Security Hub, qui est la configuration recommandée. Dans les partitions qui ne prennent pas en charge cette fonctionnalité au moment de la rédaction, vous devrez déployer les playbooks spécifiques au standard plutôt que le SC (Security Control).

Activez les résultats de contrôle consolidés dans les deux comptes et dans les deux régions.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Permettre des résultats de contrôle consolidés	Permettre des résultats de contrôle consolidés
222222222222	Membre	Permettre des résultats de contrôle consolidés	Permettre des résultats de contrôle consolidés

La génération des résultats avec la nouvelle fonctionnalité peut prendre un certain temps. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger les résultats générés sans la nouvelle fonctionnalité. Les résultats générés avec la nouvelle fonctionnalité peuvent être identifiés par la valeur du GeneratorId champ `security-control/<control_id>`.

## Configuration de l'agrégation de recherche entre régions

Consultez la documentation suivante :

- [Agrégation entre régions](#)
- [Activation de l'agrégation entre régions](#)

Configurez l'agrégation de recherche entre us-west-2 et us-east-1 dans les deux comptes.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Configurer l'agrégation depuis us-west-2	Aucun
222222222222	Membre	Configurer l'agrégation depuis us-west-2	Aucun

La propagation des résultats dans la région d'agrégation peut prendre un certain temps. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger les résultats provenant d'autres régions tant qu'ils ne commenceront pas à apparaître dans la région d'agrégation.

## Désignez un compte administrateur Security Hub

Consultez la documentation suivante :

- [Gestion des comptes dans AWS Security Hub](#)
- [Gestion des comptes des membres de l'organisation](#)
- [Gérer les comptes des membres sur invitation](#)

Dans l'exemple suivant, nous utiliserons la méthode d'invitation manuelle. Pour un ensemble de comptes de production, nous vous recommandons de gérer l'administration déléguée de Security Hub via Organizations. AWS

Depuis la console AWS Security Hub du compte administrateur (111111111111), invitez le compte membre (222222222222) à accepter le compte administrateur en tant qu'administrateur délégué du Security Hub. Depuis le compte membre, acceptez l'invitation.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Inviter le compte membre	Aucun
222222222222	Membre	Acceptez l'invitation	Aucun

La propagation des résultats vers le compte administrateur peut prendre un certain temps. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger les résultats des comptes des membres tant qu'ils ne commenceront pas à apparaître dans le compte administrateur.

## Création des rôles pour les autorisations autogérées StackSets

Consultez la documentation suivante :

- [AWS CloudFormation StackSets](#)
- [Accorder des autorisations autogérées](#)

Nous allons déployer des CloudFormation stacks sur plusieurs comptes, nous allons donc utiliser StackSets. Nous ne pouvons pas utiliser les autorisations gérées par le service car la pile d'administrateurs et la pile de membres ont des piles imbriquées, qui ne sont pas prises en charge par le service. Nous devons donc utiliser des autorisations autogérées.

Déployez les piles pour obtenir des autorisations de base pour les StackSet opérations. Pour les comptes de production, vous souhaitez peut-être restreindre les autorisations conformément à la documentation sur les « options d'autorisations avancées ».

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Déployer la pile de rôles d' StackSet administrateur  Déployer la pile de rôles StackSet d'exécution	Aucun

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
222222222222	Membre	Déployer la pile de rôles StackSet d'exécution	Aucun

## Créez les ressources non sécurisées qui généreront des exemples de résultats

Consultez la documentation suivante :

- [Référence des contrôles Security Hub](#)
- [AWSContrôles Lambda](#)

L'exemple de ressource suivant avec une configuration non sécurisée afin de démontrer une correction. L'exemple de contrôle est Lambda.1 : les politiques relatives aux fonctions Lambda doivent interdire l'accès public.

### Important

Nous allons créer intentionnellement une ressource avec une configuration non sécurisée. Passez en revue la nature du contrôle et évaluez le risque lié à la création d'une telle ressource dans votre environnement pour vous-même. Renseignez-vous sur les outils dont dispose votre organisation pour détecter et signaler de telles ressources et demandez une exception le cas échéant. Si l'exemple de contrôle que nous avons sélectionné ne vous convient pas, sélectionnez un autre contrôle pris en charge par la solution.

Dans la deuxième région du compte membre, accédez à la console AWS Lambda et créez une fonction dans le dernier environnement d'exécution Python. Sous Configuration -> Autorisations, ajoutez une déclaration de politique pour autoriser l'appel de la fonction URL sans authentification.

Vérifiez sur la page de console que la fonction autorise l'accès public. Une fois que la solution a résolu ce problème, comparez les autorisations pour confirmer que l'accès public a été révoqué.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Aucun	Aucun
222222222222	Membre	Aucun	Création d'une fonction Lambda avec une configuration non sécurisée

AWSSConfig peut mettre un certain temps à détecter la configuration non sécurisée. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger le résultat tant que Config ne l'aura pas détecté.

## Création de groupes de CloudWatch journaux pour les contrôles associés

Consultez la documentation suivante :

- [Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs](#)
- [CloudTrail commandes](#)

CloudTrail Les différents contrôles pris en charge par la solution nécessitent qu'un groupe de CloudWatch journaux soit la destination d'une multirégion. CloudTrail Dans l'exemple suivant, nous allons créer un groupe de journaux à espace réservé. Pour les comptes de production, vous devez configurer correctement CloudTrail l'intégration avec CloudWatch Logs.

Créez un groupe de journaux dans chaque compte et région avec le même nom, par exemple :`asx-log-group`.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Création d'un groupe de journaux	Création d'un groupe de journaux
222222222222	Membre	Création d'un groupe de journaux	Création d'un groupe de journaux

## Déployer la solution sur des comptes de didacticiel

Rassemblez les trois Amazon S3 URLs pour la pile des rôles d'administrateur, de membre et de membre.

### Déployer la pile d'administration

[View template](#)

aws-

[sharr-deploy](#).modèle

Dans le compte administrateur, accédez à la CloudFormation console et déployez la pile d'administrateurs dans la région d'agrégation de recherche du Security Hub.

Choisissez No la valeur de tous les paramètres de chargement des piles d'administration imbriquées, à l'exception de la pile « SC » ou « Security Control ». Cette pile contient les ressources nécessaires aux résultats de contrôle consolidés que nous avons configurés dans nos comptes.

Choisissez No de réutiliser le groupe de journaux de l'orchestrateur, sauf si vous avez déjà déployé cette solution dans ce compte et cette région.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Déployer la pile d'administration	Aucun
222222222222	Membre	Aucun	Aucun

Attendez que la pile d'administrateurs ait terminé le déploiement avant de continuer afin qu'une relation de confiance puisse être créée entre les comptes membres et le compte administrateur.

### Déployer la pile de membres

[View template](#)

aws-

[sharr-member](#).modèle

Dans le compte administrateur, accédez à la CloudFormation StackSets console et déployez la pile de membres sur chaque compte et région. Utilisez les rôles StackSets d'administration et d'exécution créés dans ce didacticiel.

Entrez le nom du groupe de journaux que vous avez créé comme valeur du paramètre pour le nom du groupe de journaux.

Choisissez No la valeur de tous les paramètres de chargement des piles de membres imbriquées, à l'exception de la pile « SC » ou « Security Control ». Cette pile contient les ressources nécessaires aux résultats de contrôle consolidés que nous avons configurés dans nos comptes.

Entrez l'ID du compte administrateur comme valeur du paramètre du numéro de compte administrateur. Dans notre exemple, c'est le cas111111111111.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Déployer le StackSet membre/Confirmer le déploiement de la pile de membres	Confirmer le déploiement de la pile de membres
222222222222	Membre	Confirmer le déploiement de la pile de membres	Confirmer le déploiement de la pile de membres

## Déployer la pile de rôles des membres

[View template](#)

aws-

[sharr-member-roles](#).modèle

Dans le compte administrateur, accédez à la CloudFormation StackSets console et déployez la pile de membres sur chaque compte. Utilisez les rôles StackSets d'administration et d'exécution créés dans ce didacticiel. Entrez l'ID du compte administrateur comme valeur du paramètre du numéro de compte administrateur. Dans notre exemple, c'est le cas111111111111.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Déployer le StackSet membre/Confirmer le déploiement de la pile de membres	Aucun
222222222222	Membre	Confirmer le déploiement de la pile de membres	Aucun

Vous pouvez continuer, mais vous ne pourrez pas corriger les résultats tant que le déploiement n'aura pas CloudFormation StackSets été terminé.

## Abonnez-vous au SNS sujet

Mises à jour des mesures correctives

Sujet - [SO0111](#) - \_Topic SHARR

Dans le compte administrateur, abonnez-vous à la SNS rubrique Amazon créée par la pile d'administrateurs. Cela vous avertira lorsque les mesures correctives seront initiées et en cas de réussite ou d'échec.

Alarmes

Sujet - [SO0111](#) - \_Alarm\_Topic ASR

Dans le compte administrateur, abonnez-vous à la SNS rubrique Amazon créée par la pile d'administrateurs. Cela vous avertira lorsque des alarmes métriques se déclenchent.

## Corriger les résultats des exemples

Dans le compte administrateur, accédez à la console Security Hub et recherchez la ressource dont la configuration n'est pas sécurisée que vous avez créée dans le cadre de ce didacticiel.

Cela peut se faire de plusieurs manières :

1. Dans les partitions qui prennent en charge la fonctionnalité des résultats de contrôle consolidés, une page intitulée « Contrôles » vous permet de localiser le résultat à l'aide de l'ID de contrôle consolidé.
2. Dans la page « Normes de sécurité », vous pouvez localiser le contrôle en fonction de la norme à laquelle il appartient.
3. Vous pouvez consulter tous les résultats sur la page « Résultats » et effectuer une recherche par attribut.

L'ID de contrôle consolidé pour la fonction Lambda publique que nous avons créée est Lambda.1.

## Lancer la correction

Cochez la case située à gauche de la constatation relative à la ressource que nous avons créée. Dans le menu déroulant « Actions », sélectionnez « Corriger avec ASR ». Vous verrez une notification indiquant que le résultat a été envoyé à Amazon EventBridge.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Lancer la correction	Aucun
222222222222	Membre	Aucun	Aucun

## Confirmez que la correction a résolu le problème

Vous devriez recevoir deux SNS notifications. Le premier indiquera qu'une correction a été initiée, et le second indiquera que la correction a réussi. Après avoir reçu la deuxième notification, accédez à la console Lambda dans le compte membre et confirmez que l'accès public a été révoqué.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Aucun	Aucun
222222222222	Membre	Aucun	Confirmez que la correction a réussi

## Suivez l'exécution de la remédiation

Pour mieux comprendre le fonctionnement de la solution, vous pouvez suivre l'exécution de la correction.

### EventBridge règle

Dans le compte administrateur, recherchez une EventBridge règle nommée SHARRRemediate\_with\_... CustomAction Cette règle correspond au résultat que vous avez envoyé depuis Security Hub et l'envoi à Orchestrator Step Functions.

### Step Functions : exécution

Dans le compte administrateur, recherchez les AWS Step Functions nommées « SO0111- SHARR - Orchestrator ». Cette fonction d'étape appelle le document SSM d'automatisation dans le compte et la région cibles. Vous pouvez suivre l'exécution de la correction dans l'historique d'exécution de ce AWS Step Functions.

### SSM Automation

Dans le compte membre, accédez à la console SSM Automation. Vous trouverez deux exécutions d'un document nommé « ASR -SC\_2.0.0\_Lambda.1 » et une exécution d'un document nommé « - ». ASR RemoveLambdaPublicAccess

La première exécution provient de la fonction d'étape de l'orchestrateur dans le compte cible. La deuxième exécution a lieu dans la région cible, qui peut ne pas être la région d'où provient la découverte. L'exécution finale est la correction qui révoque la politique d'accès public de la fonction Lambda.

### CloudWatch Groupe de journaux

Dans le compte administrateur, accédez à la console CloudWatch Logs et recherchez un groupe de journaux nommé « SO0111- SHARR ». Ce groupe de journaux est la destination des journaux de haut niveau provenant d'Orchestrator Step Functions.

## Activez des mesures correctives entièrement automatisées

L'autre mode de fonctionnement de la solution consiste à corriger automatiquement les résultats dès leur arrivée dans Security Hub.

## Vérifiez que vous ne disposez d'aucune ressource à laquelle cette constatation peut s'appliquer accidentellement

L'activation des corrections automatiques initiera des corrections sur toutes les ressources correspondant au contrôle que vous activez (Lambda.1).

### Important

Confirmez que vous souhaitez que cette autorisation soit révoquée pour toutes les fonctions Lambda publiques incluses dans le cadre de la solution. La portée des corrections entièrement automatisées ne sera pas limitée à la fonction que vous avez créée. La solution corrigera ce contrôle s'il est détecté dans l'un des comptes ou régions dans lesquels il est installé.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Confirmez qu'aucune fonction publique n'est souhaitée	Confirmez qu'aucune fonction publique n'est souhaitée
222222222222	Membre	Confirmez qu'aucune fonction publique n'est souhaitée	Confirmez qu'aucune fonction publique n'est souhaitée

## Activer la règle

Dans le compte Admin, recherchez une EventBridge règle nommée AutoTriggerSC\_2.0.0\_Lambda.1\_ et activez-la.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Activez les règles de correction automatisées	Aucun

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
222222222222	Membre	Aucun	Aucun

## Configuration de la ressource

Dans le compte membre, reconfigurez la fonction Lambda pour autoriser l'accès public.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Aucun	Aucun
222222222222	Membre	Aucun	Configurer la fonction Lambda pour autoriser l'accès public

## Confirmez que la correction a résolu le problème

Config peut mettre un certain temps à détecter à nouveau la configuration non sécurisée. Vous devriez recevoir deux SNS notifications. Le premier indiquera qu'une correction a été initiée. Le second indiquera que la correction a réussi. Après avoir reçu la deuxième notification, accédez à la console Lambda dans le compte membre et confirmez que l'accès public a été révoqué.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Activez les règles de correction automatisées	Aucun
222222222222	Membre	Aucun	Confirmez que la correction a réussi

## Nettoyage

### Supprimer les exemples de ressources

Dans le compte membre, supprimez l'exemple de fonction Lambda que vous avez créé.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Aucun	Aucun
222222222222	Membre	Aucun	Supprimer l'exemple de fonction Lambda

### Supprimer la pile d'administrateurs

Dans le compte administrateur, supprimez la pile d'administrateurs.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Supprimer la pile d'administrateurs	Aucun
222222222222	Membre	Aucun	Aucun

### Supprimer la pile de membres

Dans le compte Admin, supprimez le membre StackSet.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Supprimer le membre StackSet  Confirmer la suppression de la pile de membres	Confirmer la suppression de la pile de membres

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
222222222222	Membre	Confirmer la suppression de la pile de membres	Confirmer la suppression de la pile de membres

## Supprimer la pile de rôles des membres

Dans le compte administrateur, supprimez les rôles des membres StackSet.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Supprimer les rôles des membres StackSet  Confirmez que la pile de rôles des membres a été supprimée	Aucun
222222222222	Membre	Confirmer la suppression de la pile des rôles des membres	Aucun

## Supprimer les rôles conservés

Dans chaque compte, supprimez les IAM rôles conservés.

Important : Ces rôles sont conservés pour les corrections qui nécessitent un rôle pour que la correction continue de fonctionner (par exemple, l'enregistrement des VPC flux). Vérifiez que vous n'avez pas besoin du fonctionnement continu d'aucun de ces rôles avant de les supprimer.

Supprimez tous les rôles préfixés par SO0111-.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Supprimer les rôles conservés	Aucun
222222222222	Membre	Supprimer les rôles conservés	Aucun

## Planifier la suppression KMS des clés conservées

Les piles d'administrateurs et de membres créent et conservent une KMS clé. Des frais vous seront facturés si vous conservez ces clés.

Ces clés sont conservées afin de vous donner accès à toutes les ressources cryptées par la solution. Vérifiez que vous n'en avez pas besoin avant de planifier leur suppression.

Identifiez les clés déployées par la solution à l'aide des alias créés par la solution ou à partir de l'CloudFormation historique. Programmez-les pour leur suppression.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Identifier et planifier la suppression de la clé d'administration  Identifier et planifier la suppression de la clé de membre	Identifier et planifier la suppression de la clé de membre
222222222222	Membre	Identifier et planifier la suppression de la clé de membre	Identifier et planifier la suppression de la clé de membre

## Supprimer les piles pour les autorisations autogérées StackSets

Supprimer les piles créées pour autoriser les autorisations autogérées StackSets

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Administrateur	Supprimer la pile de rôles d' StackSet administrateur	Aucun
222222222222	Membre	Supprimer la pile de rôles StackSet d'exécution	Aucun

# Manuel du développeur

Cette section fournit le code source de la solution ainsi que des personnalisations supplémentaires.

## Code source

Consultez notre [GitHub référentiel](#) pour télécharger les modèles et les scripts de cette solution et pour partager vos personnalisations avec d'autres utilisateurs.

## Playbooks

[Cette solution inclut les correctifs relatifs aux normes de sécurité définies dans le cadre du Center for Internet Security \(CIS\) AWS Foundations Benchmark v1.2.0, Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmarkv3.0.0, CIS AWS AWS FoundationalSecurity Best Practices \(FSBP\) v.1.0.0, Payment Card Industry Data Security Standard \(PCI-\) v3.2.1 et National Institute of Standards DSS et technologie \(NIST\).](#)

Si vous avez activé les résultats des contrôles consolidés, ces contrôles sont pris en charge dans toutes les normes. Si cette fonctionnalité est activée, seul le playbook SC doit être déployé. Si ce n'est pas le cas, les playbooks sont compatibles avec les normes répertoriées précédemment.

### Important

Déployez uniquement les playbooks correspondant aux normes activées afin d'éviter d'atteindre les quotas de service.

Pour plus de détails sur une correction spécifique, reportez-vous au document d'automatisation de Systems Manager portant le nom déployé par la solution dans votre compte. Accédez à la [console AWS Systems Manager](#), puis dans le volet de navigation, sélectionnez Documents.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
Nombre total de mesures correctives	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroupELBHealthCheck  Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser des contrôles de santé de l'équilibreur de charge	Mise à l'échelle automatique.1		Mise à l'échelle automatique.1		Mise à l'échelle automatique.1		Mise à l'échelle automatique.1

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Creat eMultiReg ionTrail  CloudTrai l doit être activé et configuré avec au moins un parcours multirégi onal	CloudTrai l1.	2.1	CloudTrai l2.	3.1	CloudTrai l1.	3.1	CloudTrai l1.
ASR-Enabl eEncrypti on  CloudTrai l le chiffreme nt au repos doit être activé	CloudTrai l2.	2.7	CloudTrai l1.	3.7	CloudTrai l2.	3,5	CloudTrai l2.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EnableLogFileValidation  Assurez-vous que la validation du fichier CloudTrail journal est activée	CloudTrail 14.	2.2	CloudTrail 13.	3.2	CloudTrail 14.		CloudTrail 14.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR-EnableCloudTrailToCloudWatchLogging</p> <p>Assurez-vous que les CloudTrail sentiers sont intégrés à Amazon CloudWatch Logs</p>	CloudTrail5.	2,4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Configure S3 BucketLogging		2.6		3.6		3.4	CloudTrail 17.
Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Repla ceCodeBui ldClearTe xtCredent ials  CodeBuild les variables d'environ nement du projet ne doivent pas contenir d'informa tions d'identif ication en texte clair	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-E nableAWS onfig  Assurez- vous que AWS Config c'est activé	Config.1	2,5	Config.1	3,5	Config.1	3.3	Config.1
ASR- M Privé akeEBSSna pshots  EBSLes instantan és Amazon ne doivent pas être restaurab les publiquem ent	EC21.		EC21.		EC21.		EC21.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-R removeVPC default SecurityG roupRules  VPCle groupe de sécurité par défaut doit interdire le trafic entrant et sortant	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.
ASR- E Logs nableVPCF low  VPCla journalis ation des flux doit être activée dans tous VPCs	EC26.	2.9	EC26.	3.9	EC26.	3.7	EC26.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EnableEbsEncryptionByDefault  EBSLe chiffrement par défaut doit être activé	EC27.	2.2.1			EC27.	2.2.1	EC27.
ASR-RotateKeys  Les clés d'accès des utilisateurs doivent être renouvelées tous les 90 jours ou moins	IAM3.	1.4		1.14	IAM3.	1.14	IAM3.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR Politique - SetIAM Password  IAM politique de mot de passe par défaut	IAM7.	1,5-1,11	IAM8.	1.8	IAM7.	1.8	IAM7.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR- RevokeUnusedIAMUserCredentials</p> <p>Les informations d'identification de l'utilisateur doivent être désactivées si elles ne sont pas utilisées dans les 90 jours</p>	IAM8.	1.3	IAM7.		IAM8.		IAM8.

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Revok eUnusedIA MUserCred entials  Les informati ons d'identif ication de l'utilisa teur doivent être désactivé es si elles ne sont pas utilisées dans les 45 jours.				1.12		1.12	IAM2.2

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-RemoveLambdaPublicAccess  Les fonctions Lambda devraient interdire l'accès public	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakeRDSSnapshot  RDSles instances doivent interdire l'accès public	RDS1.		RDS1.		RDS1.		RDS1.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-DisablePublicAccessToRDSInstance  RDS Les instances de base de données doivent interdire l'accès public	RDS2.		RDS2.		RDS2.	2.3.3	RDS2.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EncryptRDS Snapshot RDS les instantanés de cluster et les instantanés de base de données doivent être chiffrés au repos	RDS4.				RDS4.		RDS4.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- EnableMultiAZOnRDSInstance  RDSLes instances de base de données doivent être configurées avec plusieurs zones de disponibilité	RDS5.				RDS5.		RDS5.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR-EnableEnhancedMonitoringOnRDSInstance</p> <p>Une surveillance améliorée doit être configurée pour les RDS instances de base de données et les clusters</p>	RDS6.				RDS6.		RDS6.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Enable RDS Cluster Deletion Protection  RDS la protection contre la suppression des clusters doit être activée	RDS7.				RDS7.		RDS7.

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-E nableRDSI nstance DeletionP rotection  RDSL a protectio n contre la suppressi on des instances de base de données doit être activée	RDS8.				RDS8.		RDS8.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR-EnableMinorVersionUpgradeOnRDSEInstance</p> <p>RDSLes mises à niveau automatiques des versions mineures doivent être activées</p>	RDS.13				RDS.13	2.3.2	RDS.13

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EnableCopyTagsToSnapshotOnRDSCluster  RDSLes clusters de base de données doivent être configurés pour copier des balises dans des instantanés	RDS.16				RDS.16		RDS.16

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-DisablePublicAccessToRedshiftCluster  Les clusters Amazon Redshift devraient interdire l'accès public	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Enabl eAutomati cSnapshot sOnRedshi ftCluster  Les snapshots automatiq ues doivent être activés sur les clusters Amazon Redshift	Redshift. 3				Redshift. 3		Redshift. 3

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- EnableRedshift ClusterAuditLogging  La journalisation des audits doit être activée sur les clusters Amazon Redshift	Redshift. 4				Redshift. 4		Redshift. 4

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Enabl eAutomati cVersionU pgradeOnR edshiftCl uster  Amazon Redshift devrait activer les mises à niveau automatiq ues vers les versions majeures	Redshift. 6				Redshift. 6		Redshift. 6

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Configure S3 PublicAccessBlock  Le paramètre S3 Block Public Access doit être activé	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-Configure S3 BucketPublicAccessBlock  Les compartiments S3 devraient interdire l'accès public à la lecture	S3.2		S3.2	2.1.5.2	S3.2		S3.2

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR-Configure S3 BucketPublicAccessBlock</p> <p>Les compartiments S3 devraient interdire l'accès public en écriture</p>		S3.3					S3.3
<p>ASR-EnableDefaultEncryption S3</p> <p>Le chiffrement côté serveur doit être activé dans les compartiments S3</p>	S3.4		S3.4	2.1.1	S3.4		S3.4

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR Politique - S et SSL Bucket  Les compartiments S3 doivent nécessiter des demandes d'utilisation SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-S3 BlockDeny list  Les autorisations Amazon S3 accordées à d'autres politiques internes Comptes A au compartiment doivent être limitées	S3.6				S3.6		S3.6
Le paramètre S3 Block Public Access doit être activé au niveau du bucket	S3.8				S3.8		S3.8

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Configure S3 BucketPublicAccess Block Assurez-vous que les CloudTrail logs du compartiment S3 ne sont pas accessibles au public		2.3					CloudTrail6.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateAccessLoggingBucket  Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3		2.6					CloudTrail7.

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Enabl eKeyRotat ion  Assurez- vous que la rotation pour les applicati ons créées par le client CMKs est activée		2,8	KMS1.	3.8	KMS4.	3.6	KMS4.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm  Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les API appels non autorisés		3.1		4.1			Cloudwatch 1

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm		3.2		4.2			Cloudwatch 2
Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour AWS Management Console vous connecter sans MFA							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm  Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour l'utilisation de l'utilisateur « root »		3.3	CW.1	4.3			Cloudwatch 3

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm		3.4		4,4			Cloudwatch 4
Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modifications IAM de politique							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm		3,5		4,5			Cloudwatch 5
Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modifications CloudTrail de configuration							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm		3.6		4.6			Cloudwatch 6
Assurez-vous qu'un journal, un filtre métrique et une alarme existent en cas d'échec d'authentification							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR-CreateLogMetricFilterAndAlarm</p> <p>Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour désactiver ou planifier la suppression des fichiers créés par le client CMKs</p>		3.7		4,7			Cloudwatch.7

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm  Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique de compartiment S3		3.8		4.8			Cloudwatch.8

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm		3.9		4,9			Cloudwatch.9
Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modifications AWS Config de configuration							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm  Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des groupes de sécurité		3,10		4,10			Cloudwatch.10

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Creat eLogMetri cFilterAn dAlarm  Assurez- vous qu'un journal, un filtre métrique et une alarme existent pour les modificat ions apportées aux listes de contrôle d'accès au réseau (NACL)		3,11		4,11			Cloudwatc h.11

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm  Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des passerelles réseau		3,12		4,12			Cloudwatch.h.12

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm  Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des tables de routage		3.13		4,13			Cloudwatch.13

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-CreateLogMetricFilterAndAlarm		3,14		4,14			Cloudwatch.14
Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les VPC modifications.							

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
AWS- Disab lePublicA ccessForS ecurityGr oup  Assurez- vous qu'aucun groupe de sécurité n'autoris e l'entrée entre 0.0.0.0/0 et le port 22		4.1	EC25.		EC2.13		EC2.13

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>AWS-DisablePublicAccessForSecurityGroup</p> <p>Assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée entre 0.0.0.0/0 et le port 3389</p>		4.2			EC2.14		EC2.14
ASR-ConfigureSNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
ASR-CreateIAMSupportRole		1,20		1,17		1,17	IAM.18

Descripti on	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Disab lePublicl PAutoAssi gn  EC2Les sous- réseaux Amazon ne doivent pas attribuer automatiq ument d'adresse s IP publiques	EC2.15				EC2.15		EC2.15
ASR- Enabl eCloudTra ilLogFile Validatio n	CloudTrai I4.	2.2	CloudTrai I3.	3.2			CloudTrai I4.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EnableEncryptionForSNSNotification	SNS1.				SNS1.		SNS1.
ASR-EnableDeliveryStatusLoggingForSNSNotification  L'enregistrement de l'état de livraison doit être activé pour les messages de notification envoyés à un sujet	SNS2.				SNS2.		SNS2.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- EnableEncryptionForSQSQueue	SQS1.				SQS1.		SQS1.
ASR- MakeRDSSnapshot RDS'instance must be private	RDS1.		RDS1.				RDS1.
ASR-B LockSSMDocument PublicAccess SSM Documents must not be public	SSM4.				SSM4.		SSM4.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EnableCloudFrontDefaultRootObject	CloudFront1.				CloudFront1.		CloudFront1.
CloudFront les distributions doivent avoir un objet racine par défaut configuré							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-SetCloudFrontOriginDomainCloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes	CloudFront.12				CloudFront.12		CloudFront.12

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Remov eCodeBuildPrivilegedMode  CodeBuild les environne ments de projet doivent avoir une durée de AWS Config journalis ation	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Terminer EC2Instance  EC2Les instances arrêtées doivent être supprimées après une période spécifiée	EC24.				EC24.		EC24.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Activer IMDSV2On nstance  EC2les instances doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)	EC28.				EC28.	5.6	EC28.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- RevokeUnauthorizedInboundRules  Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés	EC2.18				EC2.18		EC2.18

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-DisableUnrestrictedAccessToHighRiskPorts  Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé	EC2.19				EC2.19		EC2.19

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-D isableTGW Auto AcceptShareAttachments  Amazon EC2 Transit Gateways ne doit pas accepter automatiquement les demandes de VPC pièces jointes	EC2.23				EC2.23		EC2.23

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- EnablePrivateRepositoryScanning  ECR la numérisation des images doit être configurée dans les référentiels privés	ECR1.				ECR1.		ECR1.
ASR- EnableGuardDuty  GuardDuty doit être activé	GuardDuty1.		GuardDuty1.		GuardDuty1.		GuardDuty1.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR- Configure S3 BucketLogging  La journalisation des accès au serveur de compartiments S3 doit être activée	S3.9				S3.9		S3.9

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EnableBucketEventNotifications  Les notifications d'événements doivent être activées dans les compartiments S3	S3.11				S3.11		S3.11

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-3 Lifecycle Policy  Les politiques de cycle de vie des compartiments S3 doivent être configurées	S3.13				S3.13		S3.13

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR-EnableAutoSecretRotation</p> <p>La rotation automatique des secrets des secrets du Gestionnaire de secrets doit être activée</p>	SecretsManager1.				SecretsManager1.		SecretsManager1.
<p>ASR-RemoveUnusedSecret</p> <p>Supprimer les secrets inutilisés de Secrets Manager</p>	SecretsManager3.				SecretsManager3.		SecretsManager3.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-UpdateSecretRotationPeriod  Les secrets de Secrets Manager doivent faire l'objet d'une rotation dans un délai spécifié	SecretsManager4.				SecretsManager4.		SecretsManager4.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Enable API Gateway CacheData Encryption					API Gateway 5.		API Gateway 5.
API Les données REST API du cache de la passerelle doivent être chiffrées au repos							

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-SetLoggingGroupRetentionDays  CloudWatch les groupes de journaux doivent être conservés pendant une période spécifiée					CloudWatch h.16		CloudWatch h.16

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-Attac hServiceV PCEndpoin t  Amazon EC2 doit être configuré pour utiliser les VPC points de terminais on créés pour le service Amazon EC2	EC2.10				EC2.10		EC2.10
ASR- TagGu ardDutyRe source  GuardDuty les filtres doivent être étiquetés							GuardDuty 2.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
<p>ASR-TagGuardDutyResource</p> <p>GuardDuty les détecteurs doivent être étiquetés</p>							GuardDuty4.
<p>ASR-AttachSSMPermissionsToEC2</p> <p>EC2 Les instances Amazon doivent être gérées par Systems Manager</p>	SSM1.		SSM3.				SSM1.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-ConfigureLaunchConfigurationPublicIPdocument					Autoscaling.5		Autoscaling.5
EC2Les instances Amazon lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresse IP publique							
ASR-EnableAPIGatewayExecutionLogs	APIGateway1.						APIGateway1.

Description	AWS FSBP	CISv1.2.0	PCIv3.2.1	CISv1.4.0	NIST	CISv3.0.0	<a href="#">ID de contrôle de sécurité</a>
ASR-EnableMacie  Amazon Macie devrait être activé	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging  La journalisation des groupes de travail Athena doit être activée	Athéna.4						Athéna.4

## Ajouter de nouvelles mesures correctives

L'ajout d'une nouvelle correction à un playbook existant ne nécessite pas de modification de la solution elle-même.

**Note**

Les instructions qui suivent utilisent les ressources installées par la solution comme point de départ. Par convention, la plupart des noms de ressources de solutions contiennent SHARRet/ou SO0111 pour faciliter leur localisation et leur identification.

## Présentation

La réponse de sécurité automatisée sur AWS les runbooks doit suivre la dénomination standard suivante :

ASR-*<standard>*-*<version>*-*<control>*

Standard : Abréviation de la norme de sécurité. Cela doit correspondre aux normes prises en charge par SHARR. Il doit s'agir de l'un des types « AFSBP », « PCI », « », NIST « » ou « SC ». CIS

Version : version de la norme. Encore une fois, cela doit correspondre à la version prise en charge par SHARR et à la version figurant dans les données de recherche.

Contrôle : ID du contrôle à corriger. Cela doit correspondre aux données de recherche.

1. Créez un runbook sur le (s) compte (s) membre (s).
2. Créez un IAM rôle dans le (s) compte (s) membre (s).
3. (Facultatif) Créez une règle de correction automatique dans le compte administrateur.

### Étape 1. Créez un runbook sur le (s) compte (s) membre (s)

1. Connectez-vous à la [AWS Systems Manager console](#) et obtenez un exemple du résultatJSON.
2. Créez un runbook d'automatisation qui corrige le résultat. Dans l'onglet Owned by me, utilisez l'un des ASR- documents de l'onglet Documents comme point de départ.
3. Le AWS Step Functions compte administrateur exécutera votre runbook. Votre runbook doit spécifier le rôle de correction afin d'être transmis lors de l'appel du runbook.

### Étape 2. Créez un IAM rôle dans le (s) compte (s) membre (s)

1. Connectez-vous à la [console AWS Identity and Access Management](#).

2. Obtenez un exemple à partir des rôles IAM S00111 et créez un nouveau rôle. Le nom du rôle doit commencer par S00111-Remediate-*<standard>*-*<version>*-*<control>*. Par exemple, si vous ajoutez le contrôle CIS v1.2.0 5.6, le rôle doit être S00111-Remediate-CIS-1.2.0-5.6.
3. À l'aide de cet exemple, créez un rôle correctement défini qui autorise uniquement les API appels nécessaires pour effectuer la correction.

À ce stade, votre correction est active et disponible pour une correction automatique à partir de l'action SHARR personnalisée dans AWS Security Hub.

## Étape 3 : (Facultatif) Créez une règle de correction automatique dans le compte administrateur

La correction automatique (et non « automatisée ») est l'exécution immédiate de la correction dès que le résultat est reçu par AWS Security Hub. Examinez attentivement les risques avant d'utiliser cette option.

1. Consultez un exemple de règle pour la même norme de sécurité dans CloudWatch Events. La norme de dénomination pour les règles est `standard_control_AutoTrigger`.
2. Copiez le modèle d'événement de l'exemple à utiliser.
3. Modifiez la `GeneratorId` valeur pour qu'elle corresponde `GeneratorId` à celle de votre rechercheJSON.
4. Enregistrez et activez la règle.

## Ajouter un nouveau playbook

Téléchargez la réponse de sécurité automatisée sur les playbooks des AWS solutions et le code source de déploiement depuis le [GitHub référentiel](#).

Les AWS CloudFormation ressources sont créées à partir de [AWS CDK](#) composants, et les ressources contiennent le code du modèle de playbook que vous pouvez utiliser pour créer et configurer de nouveaux playbooks. Pour plus d'informations sur la configuration de votre projet et la personnalisation de vos playbooks, consultez le [README](#) fichier `.md` dans [GitHub](#)

## AWS Systems Manager Magasin de paramètres

Automated Security Response on AWS utilise le magasin de paramètres de AWS Systems Manager pour le stockage des données opérationnelles. Les paramètres suivants sont enregistrés dans Parameter Store :

Nom	Valeur	Utilisez
/Solutions/S00111/ CMK_REMEDIATION_ARN	AWS KMS clé qui chiffrera les données pour les corrections FSBP	Chiffrement des données clients, telles que CloudTrail les journaux, dans le cadre des mesures correctives
/Solutions/S00111/ CMK_ARN	AWS KMS clé qui SHARR sera utilisée pour chiffrer les données	Chiffrement des données de solution
/Solutions/S00111/ SNS_Topic_ARN	ARN de la SNS rubrique Amazon consacrée à la solution	Notification des événements de remédiation
/Solutions/S00111/ SNS_Topic_Config.1	SNS sujet pour les AWS Config mises à jour	Correction de la configuration 1
/Solutions/S00111/ sendAnonymousMetrics	Yes	Collecte de métriques anonymisée
/Solutions/S00111/ version	Version de la solution	
/Solutions/S00111/ <i>&lt;security standard long name&gt;/&lt;version&gt;</i> / status	enabled	Indique si le standard est actif dans la solution. Une norme peut être désactivée pour une correction automatique en la remplaçant par disabled

Nom	Valeur	Utilisez
/Solutions/S00111/ <security standard long name>/shortname	String	Nom abrégé de la norme de sécurité. Par exemple : « CIS », « AFSBP », « PCI »
/Solutions/S00111/ <security standard long name>/<version> /<control> /remap	String	Lorsqu'un contrôle utilise la même correction qu'un autre, ces paramètres exécutent le remappage

## SNSRubrique Amazon : Progression de la correction

Réponse de sécurité automatisée sur la AWS création d'une SNS rubrique Amazon, SO0111-SHARR\_Topic. Cette rubrique est utilisée pour publier des mises à jour sur la progression de la correction. Voici les trois notifications possibles envoyées à ce sujet.

```
Remediation queued for <standard> control <control_ID> in account <account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account <account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems Manager in  
account <account_ID>
```

Il s'agit du message d'achèvement. Cela indique que la correction s'est terminée sans erreur ; toutefois, le test définitif pour une correction réussie est la vérification de la AWS configuration et/ou la validation manuelle.

## Filtrage et abonnement à un SNS sujet

[Politiques de filtrage des SNS abonnements Amazon](#) :

1. Accédez à l'abonnement du SNS sujet.
2. Sous Politique de filtrage des abonnements, sélectionnez « Modifier ».
3. Développez « Politique de filtrage des abonnements » et activez l'option « Politique de filtrage des abonnements » pour activer les filtres.

4. Sélectionnez le champ « Corps du message ».
5. Ajoutez votre politique à l'JSONéditeur.
6. Enregistrez les modifications.

Exemples de politiques :

#### Filtrer par compte

```
{
  "finding": {
    "account": [
      "111111111111",
      "222222222222"
    ]
  }
}
```

#### Filtrer les erreurs

```
{
  "severity": ["ERROR"]
}
```

#### Filtrer par commandes

```
{
  "finding": {
    "standard_control": ["S3.9", "S3.6"]
  }
}
```

## SNSRubrique Amazon — CloudWatch Alarmes

Cette solution crée un SNS sujet Amazon, `S00111-ASR_Alarm_Topic`. Cette rubrique est utilisée pour publier des alertes d'alarme.

Les détails de toutes les alarmes qui entrent dans l'ALARMétat seront envoyés à cette rubrique.

## Lancer Runbook sur la base des résultats de configuration

Cette solution peut lancer des runbooks en fonction de AWS Config résultats personnalisés. Pour ce faire, vous devez :

1. Trouvez le nom de la AWS Config règle à laquelle vous souhaitez remédier. Cela se trouve dans l'une AWS Config ou l'autre des conclusions générées par Security Hub pour cette règle.
2. Accédez à AWS Systems Manager Parameter Store et sélectionnez Create Parameter.
3. Le nom de votre règle doit être `/Solutions/S00111/Rule name from Step 1`
4. La valeur doit être formatée comme suit :

```
{  
  
"RunbookName": "Name of SSM runbook",  
  
"RunbookRole": "Role that Orchestrator will assume"  
  
}
```

5. RunbookName est un champ obligatoire et sera le runbook qui sera exécuté lorsque vous corrigerez cette règle de Config. RunbookRole est le rôle que l'orchestrateur assumera lors de l'exécution de ce rôle. Ce champ n'est pas obligatoire, et s'il est omis, l'orchestrateur utilisera par défaut le rôle de membre du compte.
6. Une fois que cela est en place, vous pouvez corriger votre règle Config à l'aide de l'action personnalisée « ASR Corriger avec » disponible sur le Security Hub.

# Référence

Cette section inclut des informations sur une fonctionnalité facultative permettant de collecter des métriques uniques pour cette solution, des pointeurs vers des ressources connexes et une liste des créateurs qui ont contribué à cette solution.

## Collecte de données anonymisée

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles anonymisées à AWS. Nous utilisons ces données pour mieux comprendre la façon dont les clients utilisent cette solution et les services et produits associés. Lorsque cette option est activée, les informations suivantes sont collectées et envoyées à AWS :

- ID de solution : identifiant de AWS solution
- ID unique (UUID) : identifiant unique généré de manière aléatoire pour chaque déploiement de AWS Security Hub réponse et de correction
- Horodatage - Horodatage de la collecte de données
- Données d'instance : informations sur le déploiement de cette pile
- CloudWatchMetricsDashboardEnabled- "Yes" si CloudWatch les métriques et le tableau de bord sont activés pendant le déploiement
- État : état du déploiement (solution réussie ou défectueuse) ou (résolution réussie ou échec)
- Message d'erreur : message d'erreur générique dans le champ d'état
- Generator\_ID - Informations sur les règles du Security Hub
- Type : type et nom de la correction
- productArn- La région dans laquelle Security Hub est déployé
- finding\_triggered\_by : type de correction effectué (action personnalisée ou déclencheur automatique)

AWS détient les données recueillies dans le cadre de cette enquête. La collecte de données est soumise à l'[avis AWS de confidentialité](#). Pour désactiver cette fonctionnalité, suivez les étapes ci-dessous avant de lancer le AWS CloudFormation modèle.

1. Téléchargez le [AWS CloudFormation modèle](#) sur votre disque dur local.
2. Ouvrez le AWS CloudFormation modèle dans un éditeur de texte.

### 3. Modifiez la section de mappage du AWS CloudFormation modèle à partir de :

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'Yes'
```

par :

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'No'
```

4. Connectez-vous à la [console AWS CloudFormation](#) .
5. Sélectionnez Créer une pile.
6. Sur la page Créer une pile, section Spécifier le modèle, sélectionnez Télécharger un fichier modèle.
7. Sous Télécharger un fichier modèle, choisissez Choisir un fichier et sélectionnez le modèle modifié sur votre disque local.
8. Choisissez Next et suivez les étapes décrites dans [Lancer la pile](#) dans la section Déploiement automatisé de ce guide.

## Ressources connexes

- [Réponse et correction automatisées avec AWS Security Hub](#)
- [CISBenchmarks d'Amazon Web Services Foundations, version 1.2.0](#)
- [Norme concernant les bonnes pratiques de sécurité de base AWS](#)
- [Norme de sécurité des données du secteur des cartes de paiement \(PCIDSS\)](#)
- [Institut national des normes et de la technologie \(NIST\) SP 800-53 Rev. 5](#)

# Collaborateurs

Les personnes suivantes ont contribué à ce document :

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schütter
- Andrew Yankowski
- Joshua Moss
- Ryan Garay
- Thiemo Belméga

# Révisions

Date	Modification
août 2020	Première version
octobre 2020	Ajout d'informations de dépannage supplémentaires à l'annexe C.
Novembre 2020	Ajout d'instructions de déploiement pour les régions de Chine ; instructions de déploiement de solutions mises à jour pour le compte administrateur du Security Hub ; pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
avril 2021	Version v1.2.0 : ajout d'une nouvelle architecture de playbook et de nouvelles FSBP corrections. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
mai 2021	Version v1.2.1 : correction d'un bogue pour un problème affectant les versions EC2 2.2 et EC2 2.7. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
août 2021	Version v1.3.0 : Ajout du Playbook PCI DSS v3.2.1. 17 nouvelles corrections ont été ajoutées à la CIS version v1.2.0. Quatre nouvelles corrections ont été ajoutées à FSBP Converti CIS pour utiliser la nouvelle architecture de playbook basée sur les SSM runbooks. Ajout d'instructions pour étendre les Playbooks existants avec des correctifs définis par le client. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.

Date	Modification
septembre 2021	Version v1.3.1 : <code>CreateLogMetricFilterAndAlarm.py</code> modifiée pour activer les actions, ajouter SNS une notification à <code>S00111-SHARR-LocalAlarmNotification</code> . Modification de la correction de la version CIS 2.8 pour correspondre au nouveau format des données de recherche. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
novembre 2021	Version v1.3.2 : corrections de bogues pour les contrôles CIS v1.2.0 3.1 - 3.14. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Décembre 2021	Version v1.4.0 : La solution peut désormais être déployée à l'aide StackSets de. La correction entre régions est désormais prise en charge en plus de la correction entre comptes. Les IAM rôles des comptes membres sont désormais conservés lorsque la pile est supprimée. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Janvier 2022	Version v1.4.1 : corrections de bugs. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Janvier 2022	Version v1.4.2 : corrections de bugs. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
juin 2022	Version v1.5.0 : corrections supplémentaires. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.

Date	Modification
Décembre 2022	Version 1.5.1 Modifications pour passer de la création de SSM documents de Custom Resource CfnDocument Lambda à. Le préfixe des noms de SSM documents est mis à jour pour commencer ASR par. SHARR Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Mars 2023	Version 2.0.0 : ajout de la prise en charge des contrôles de sécurité et des normes CIS v1.4.0, cinq nouvelles corrections aux FSBP normes, une nouvelle correction aux normes CIS v1.2.0, AppRegistry intégration du catalogue de services et protections supplémentaires pour éviter les échecs de déploiement dus à la limitation des documents. SSM Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Avril 2023	Version 2.0.1 : impact atténué causé par les nouveaux paramètres par défaut pour la propriété des objets S3 (ACLsdésactivés) pour tous les nouveaux compartiments S3. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Mai 2023	Mise à jour de la documentation : mises à jour des définitions de Well-Architected, ajout de conseils sur l'endroit où déployer chaque stack, édition supplémentaire de résolution des problèmes liés à des mesures correctives spécifiques et exemples de code mis à jour dans les notifications. SNS

Date	Modification
Juillet 2023	Mise à jour de la documentation : mise à jour du schéma d'architecture et des composants de la solution dans le flux de travail.
Octobre 2023	Version 2.0.2 : versions des packages mises à jour pour résoudre les failles de sécurité. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Novembre 2023	Mise à jour de la documentation : ajout des <a href="#">balises de coût de confirmation associées à la solution</a> dans la AppRegistry section Surveillance de la solution avec AWS Service Catalog.
Mars 2024	Version 2.1.0 : ajout de la prise en charge de la NIST norme, ajout de 17 nouvelles corrections aux FSBP normes, ajout d'un tableau de CloudWatch bord pour la solution de surveillance, ajout d'un gestionnaire de régulation à l'architecture, prise en charge des paramètres d'entrée personnalisables de Security Hub et prise en charge supplémentaire de la correction des résultats de Config. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Avril 2024	Version 2.1.1 : mise à jour de l'ordre des CloudFormation paramètres et des valeurs par défaut Mise à jour de la documentation. Ajout de références à la NIST norme. Ajout d'informations concernant les quotas de service des EventBridge règles. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.

Date	Modification
Juin 2024	Version 2.1.2 : désactivée AppRegistry pour certains playbooks afin d'éviter les erreurs lors de la mise à jour de la solution. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Septembre 2024	Version 2.1.3 : résolution d'un problème dans les scripts de correction pour EC2 .18 et EC2 .19 en raison duquel les règles de groupe de sécurité IpProtocol définies sur -1 étaient ignorées à tort. Mise à niveau de tous les environnements d'exécution Python dans SSM les documents de correction de Python 3.8 à Python 3.11. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
Novembre 2024	Version 2.1.4 : amélioration des environnements d'exécution Python dans tous les runbooks de contrôle, de Python 3.8 à Python 3.11. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.
décembre 2024	Version 2.2.0 : intégration du système de billetterie, CloudTrail Action Log et Playbook CIS 3.0.0 ajoutés. Tableau de bord et notifications améliorés. Pour plus d'informations, reportez-vous au fichier <a href="#">CHANGELOG.md</a> du GitHub référentiel.

## Avis

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de produits et les pratiques AWS actuelles, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune assurance de la part de AWS ses filiales, fournisseurs ou concédants de licence. AWS les produits ou services sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. AWS les responsabilités et les obligations envers ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne le modifie pas.

Automated Security AWS Response on est licencié selon les termes de la licence Apache version 2.0 disponible auprès de [l'Apache Software Foundation](#).

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.