AWS Architecture de référence en matière de confidentialité (AWS PRA)

AWS Conseils prescriptifs

AWS Conseils prescriptifs: AWS Architecture de référence en matière de confidentialité (AWS PRA)

Table of Contents

AWS Architecture de référence en matière de confidentialité (AWS PRA)

Amazon Web Services (contributeurs)

Mars 2024 (historique du document)

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Avis

Ce guide est fourni à titre informatif uniquement. Il ne s'agit pas d'un avis juridique et ne doit pas être considéré comme un avis juridique. AWS encourage ses clients à obtenir des conseils appropriés sur la mise en œuvre d'environnements de confidentialité et de protection des données, et plus généralement sur les lois applicables applicables à leur activité.

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 AWS produits et les pratiques 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 garantie, représentation ou condition d'aucune sorte, expresse ou implicite.

Les responsabilités et obligations AWS de ses clients sont régies par AWS des accords, et ce document ne fait partie d'aucun accord entre AWS et ses clients et ne le modifie pas.

Introduction

L'architecture de référence de AWS confidentialité (PRA) fournit un ensemble de directives spécifiques à la conception et à la configuration des contrôles garantissant la confidentialité dans. Services AWS Ce guide peut vous aider à prendre des décisions concernant les personnes, les processus et les technologies qui contribuent à protéger la confidentialité dans le AWS Cloud.

Le modèle de responsabilité AWS partagée et la confidentialité

Dans le AWS Cloud, vous partagez la responsabilité de la sécurité et de la conformité avec AWS. AWS est responsable de la sécurité du cloud, ce qui signifie qu'il AWS est responsable de la protection de l'infrastructure qui exécute tous les services proposés dans le AWS Cloud. Vous êtes responsable de la sécurité dans le cloud, ce qui signifie que vous êtes responsable de la configuration et de la gestion Services AWS conformément aux exigences de sécurité et de confidentialité. Pour plus d'informations, consultez le modèle de responsabilitéAWS partagée.

Services AWS fournissent des fonctionnalités qui vous permettent de mettre en œuvre vos propres contrôles de confidentialité dans le cloud afin de répondre à vos exigences en matière de confidentialité. Votre responsabilité en matière de confidentialité varie en fonction de nombreux facteurs, notamment de Régions AWS votre choix, de l'intégration de ces services dans votre environnement informatique, ainsi que des lois et réglementations applicables à votre organisation et à votre charge de travail. Services AWS

Lors de l'utilisation Services AWS, vous gardez le contrôle de votre contenu. Plus précisément, le contenu est défini comme un logiciel (y compris des images de machine), des données, du texte, du son, de la vidéo ou des images que vous ou un utilisateur final nous transférez à des fins de traitement, de stockage ou d'hébergement Services AWS en relation avec votre compte. Cela inclut également tous les résultats de calcul que vous ou un utilisateur final obtenez en utilisant Services AWS. Vous êtes responsable de la gestion des décisions suivantes, qui sont sous votre contrôle :

- Les données que vous choisissez de collecter, de stocker ou de traiter sur AWS
- Le Services AWS que vous utilisez avec les données
- L' Région AWS endroit où vous collectez, stockez ou traitez les données
- Le format et la structure de vos données et leur masquage, leur anonymisation ou leur cryptage
- Comment définir, stocker, faire pivoter et utiliser vos clés cryptographiques pour le chiffrement
- Qui a accès à vos données et à quel moment, et comment ces droits d'accès sont accordés, gérés et révoqués

Une fois que vous avez compris le modèle de responsabilité AWS partagée et comment il s'applique généralement au fonctionnement dans le cloud, vous devez déterminer comment il s'applique à votre cas d'utilisation. Les paramètres Services AWS que vous choisissez d'utiliser déterminent le niveau de configuration que vous devez effectuer dans le cadre des responsabilités de confidentialité de votre entreprise. Par exemple, un service tel qu'Amazon Elastic Compute Cloud (Amazon

EC2) est classé dans la catégorie infrastructure en tant que service (IaaS). Ainsi, si vous utilisez Amazon EC2, vous devez effectuer toutes les configurations de confidentialité nécessaires pour les systèmes d'exploitation clients et pour les logiciels ou utilitaires d'application que vous installez sur vos instances EC2. Lorsque vous utilisez un service abstrait, tel qu'Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB, vous êtes responsable de la couche d'infrastructure AWS , du système d'exploitation et des plateformes. Votre responsabilité est de gérer et de classer les données et de configurer les politiques utilisées pour accéder aux points de terminaison afin de stocker et de récupérer les données. Pour plus d'informations sur la manière dont AWS vous pouvez protéger les données et la confidentialité, consultez la section Protection des données et confidentialité sur AWS.

Comprendre le AWS PRA

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

La section décrit la relation entre l'architecture de référence de AWS confidentialité (AWS PRA) et les autres AWS directives. Cette section passe également en revue la disposition générale et la structure de l'exemple d'environnement AWS multi-comptes dans le AWS PRA.

Cette section contient les rubriques suivantes :

- Utilisation du AWS PRA et du AWS SRA
- AWS Organizations et la structure de compte dédiée
- Opérationnalisation des services AWS de confidentialité

Utilisation du AWS PRA et du AWS SRA

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Le AWS PRA fournit des modèles que les clients ont trouvés utiles pour planifier des contrôles de confidentialité fondamentaux et au niveau des applications pour leur infrastructure et leurs charges de travail. AWS L'architecture AWS de référence de sécurité (AWS SRA) fournit un ensemble de directives pour créer une architecture qui implémente et prend en charge le bon ensemble de contrôles de sécurité dans votre zone AWS d'atterrissage et dans vos applications. Afin d'établir les contrôles de confidentialité détaillés dans ce guide, la AWS PRA part de nombreuses directives fondamentales et de la même structure de compte que celles décrites dans la AWS SRA. Le AWS PRA et le AWS SRA détaillent plusieurs des mêmes clés Services AWS. Ce guide ne contient que de brèves descriptions de ces services. Vous pouvez en savoir plus sur ces services et sur la manière dont ils sont utilisés dans un contexte de sécurité dans la AWS SRA.

La AWS SRA peut vous aider à concevoir, mettre en œuvre et gérer les services AWS de sécurité afin qu'ils soient conformes aux pratiques AWS recommandées. Vous pouvez utiliser le AWS SRA

comme guide autonome, ou vous pouvez utiliser le AWS SRA et le AWS PRA comme guides accompagnateurs. La plupart des directives de sécurité détaillées dans la AWS SRA peuvent être suivies en parallèle avec les contrôles de confidentialité détaillés dans la AWS PRA. À l'instar de la sécurité, il peut être utile de prendre en compte certaines considérations fondamentales en matière de confidentialité dès le début de votre AWS Cloud parcours, car ces décisions peuvent avoir une incidence sur la conception de la structure des comptes de l'organisation. Par exemple, vous pourriez envisager de vous poser les questions suivantes :

- Comment mon organisation définit-elle les données personnelles ?
- Mon organisation prend-elle en charge les applications qui traitent des données personnelles ?
- Qu'en est-il des applications qui traitent d'autres types de données réglementées ?
- Quels contrôles au niveau de l'organisation puis-je mettre en œuvre pour éloigner autant que possible mes développeurs et ingénieurs cloud des données personnelles ?
- Comment séparer les données personnelles des autres types de données ?
- Quelles sont les exigences de mon organisation en matière de transfert de données transfrontalier ?

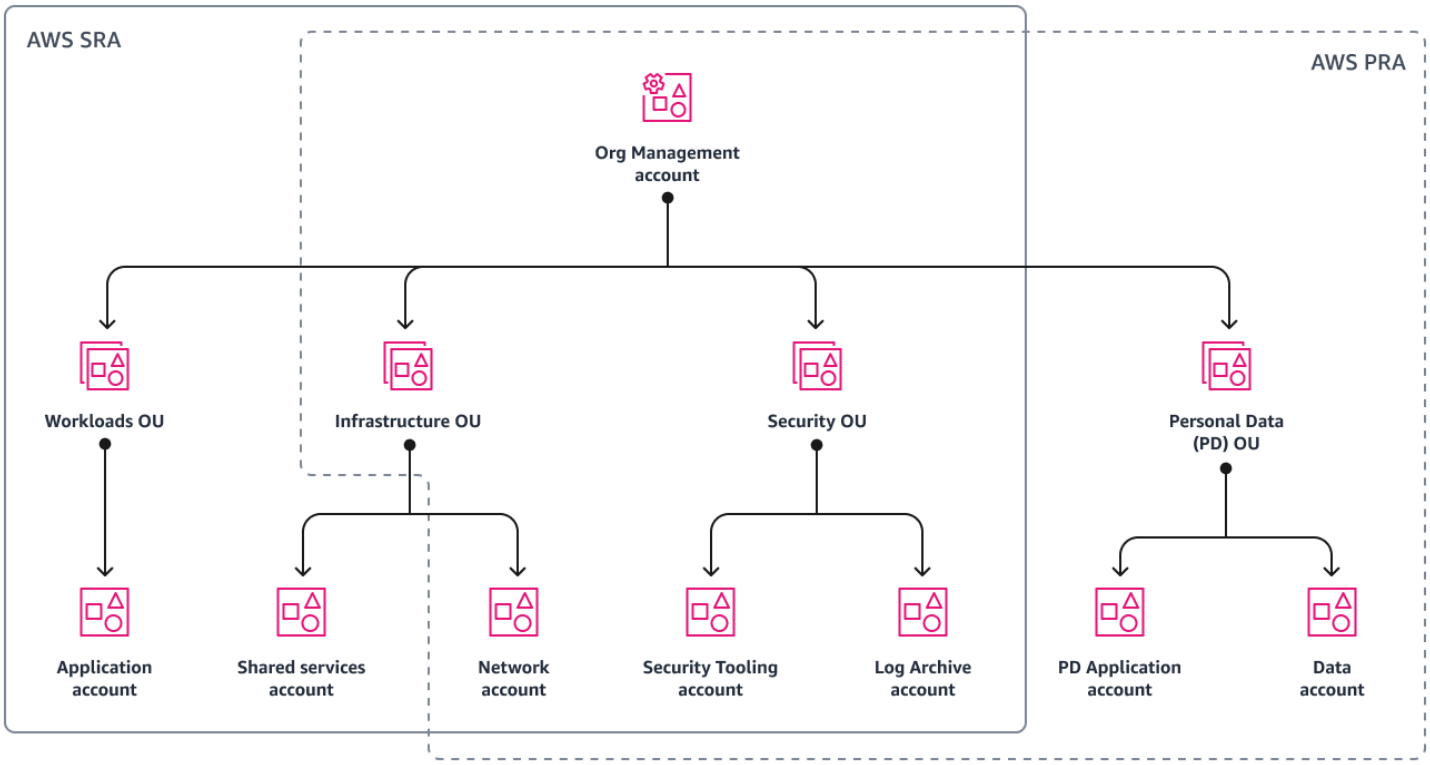
Les réponses à bon nombre de ces questions peuvent avoir des répercussions sur la conception de votre environnement cloud, notamment sur votre Compte AWS structure, vos politiques de contrôle des services et vos rôles AWS Identity and Access Management (IAM).

AWS Organizations et la structure de compte dédiée

> Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

AWS Organizationsest un service de gestion de comptes qui vous permet de gérer et de gouverner plusieurs comptes de manière centralisée Comptes AWS. L'utilisation de AWS Organizations est la base d'un environnement AWS multi-comptes bien conçu. Pour plus d'informations, consultez la section Création de votre AWS environnement de bonnes pratiques.

Le schéma suivant montre la structure de haut niveau des comptes et des unités organisationnelles (OU) du AWS PRA. Dans l'ensemble, la structure organisationnelle de la AWS PRA correspond à celle de la AWS SRA.



Les écarts par rapport à l'organisation AWS SRA incluent :

- La AWS PRA ajoute l'UO de données personnelles (DP), qui est dédiée à la collecte, au stockage et au traitement des données personnelles. Cette séparation structurelle offre de la flexibilité qui vous permet de définir des contrôles spécifiques et précis pour protéger les données personnelles contre toute divulgation involontaire.
- Dans l'UO d'infrastructure, le AWS PRA n'inclut actuellement pas de directives supplémentaires pour le compte Shared Services décrites dans le AWS SRA.
- La AWS PRA ne contient actuellement pas de directives supplémentaires pour l'unité d'organisation des charges de travail décrites dans la AWS SRA. Les applications qui collectent ou traitent des données personnelles se trouvent dans des comptes dédiés au sein de l'UO DP.

Vous pouvez l'utiliser AWS Control Towerpour une gouvernance de base globale et pour le déploiement automatisé des contrôles de sécurité et de confidentialité au sein de votre organisation. S'il AWS Control Tower n'est pas utilisé aujourd'hui dans votre organisation, vous pouvez toujours déployer de nombreux contrôles de sécurité et de confidentialité AWS Control Tower, tels que les politiques et AWS Config règles de contrôle des services, dans leurs services respectifs.

Vous trouverez peut-être utile de prendre en compte le traitement des données personnelles lorsque vous planifiez la structure de votre compte et de votre unité d'organisation, y compris une stratégie de segmentation des comptes. Vous devrez peut-être tenir compte des types de données que vous traitez en fonction de leurs cas d'utilisation uniques et des lois et réglementations applicables. Par exemple, les données des titulaires de cartes sont protégées par la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), et les informations médicales protégées peuvent être soumises à la loi HIPAA (Health Insurance Portability and Accountability Act). Vous souhaiterez peut-être examiner quels environnements contiennent des données personnelles et planifier votre stratégie de segmentation en fonction de cela. Une stratégie de segmentation des comptes typique peut inclure des comptes dédiés Comptes AWS adaptés au cycle de vie du développement logiciel (SDLC), tels que des comptes dédiés au développement, à la mise en scène ou à l'assurance qualité (QA) et à la production. Une telle stratégie de segmentation peut être un élément essentiel de la discussion globale sur la conception, et vos unités d'organisation devront peut-être s'aligner sur vos exigences réglementaires spécifiques.

Opérationnalisation des services AWS de confidentialité

> Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Pour de nombreuses personnes, la protection de la vie privée est transversale. De nombreuses équipes ont un rôle à jouer, notamment les équipes chargées de la réglementation, de la conformité et de l'ingénierie. Lorsque votre organisation a commencé à définir les personnes clés et les éléments politiques de votre programme de confidentialité, vous pouvez associer les contrôles à un cadre de conformité en matière de confidentialité pour des opérations cohérentes. Un framework peut servir de rubrique pour la mise en œuvre de contrôles de confidentialité fondamentaux et spécifiques à l'application pour les données personnelles de votre environnement. AWS

Quel que soit le cadre utilisé par les clients pour classer leurs exigences en matière de confidentialité, les équipes chargées de la conformité en matière de confidentialité, de l'ingénierie de la confidentialité et des applications doivent souvent travailler ensemble pour atteindre les objectifs de mise en œuvre. Par exemple, les équipes chargées de la réglementation et de la conformité peuvent fournir les exigences de haut niveau, tandis que les équipes d'ingénierie et d'application configurent Services AWS et proposent les fonctionnalités nécessaires pour répondre à ces exigences.

Commencer par un cadre de contrôle peut vous aider à définir des contrôles organisationnels et techniques plus prescriptifs.

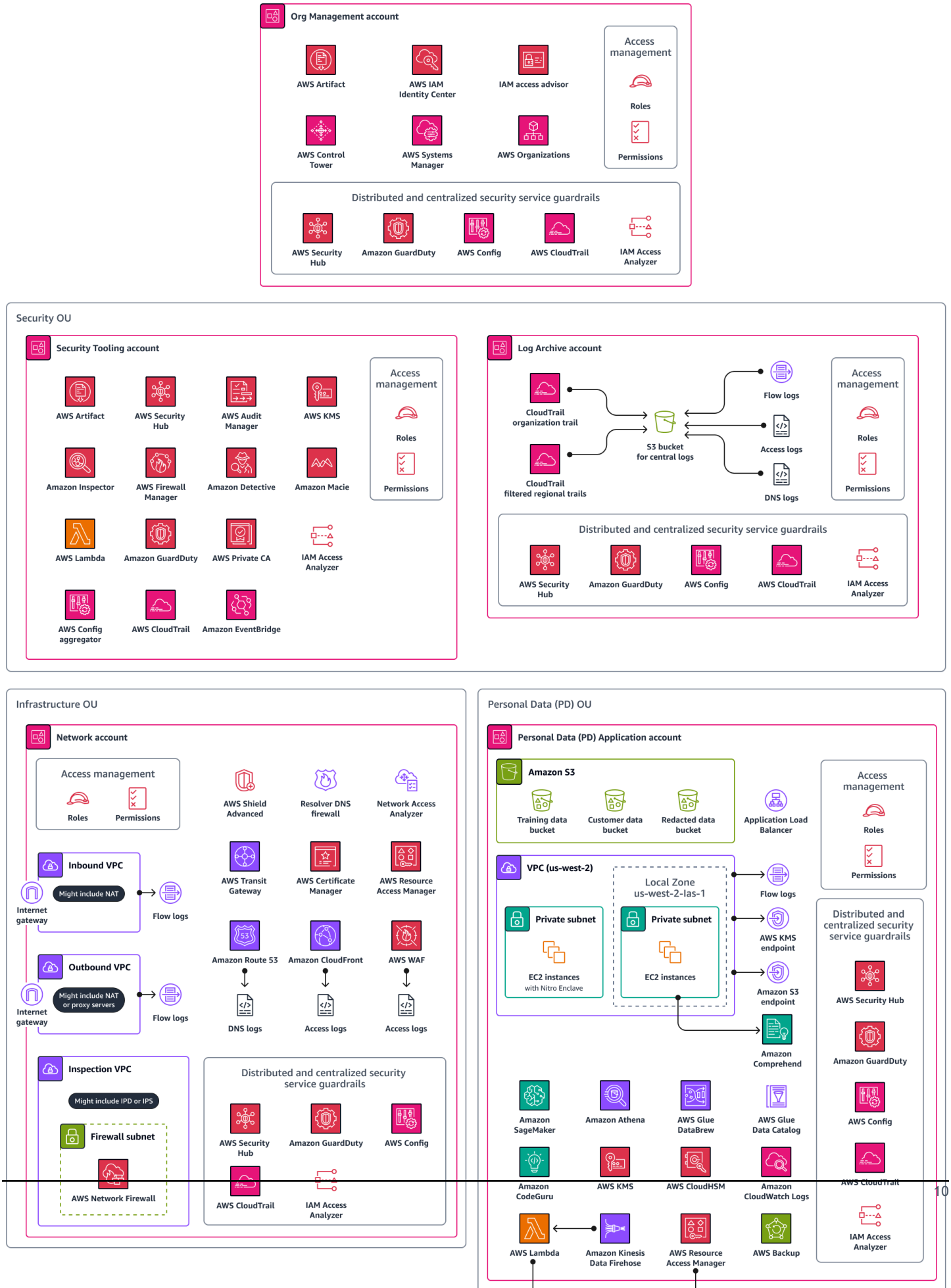
Lors de la définition des contrôles techniques Services AWS et des fonctionnalités, une autre décision clé est de savoir si un contrôle doit s'appliquer à l'ensemble de l'organisation, à une unité d'organisation, à un compte ou à une ressource spécifique. Certains services et fonctionnalités conviennent parfaitement à la mise en œuvre de contrôles dans l'ensemble de votre AWS organisation. Par exemple, le blocage de l'accès public aux compartiments Amazon S3 est un contrôle spécifique qui est de préférence configuré à la racine de l'organisation plutôt qu'individuellement pour chaque compte. Toutefois, vos politiques de rétention peuvent varier d'une application à l'autre, ce qui signifie que vous pouvez appliquer le contrôle au niveau des ressources.

Pour vous aider à accélérer la mise en œuvre de la confidentialité dans votre organisation, AWS propose des services d'audit et de conseil en conformité pour vos charges AWS de travail. Pour plus d'informations, contactez AWS SAS.

Architecture de référence en AWS matière de confidentialité

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Le schéma suivant illustre l'architecture de référence de AWS confidentialité (AWS PRA). Il s'agit d'un exemple d'architecture qui relie de nombreuses fonctionnalités liées à la confidentialité Services AWS . Cette architecture repose sur une zone d'atterrissage régie par AWS Control Tower.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup

Le AWS PRA inclut une architecture Web sans serveur hébergée dans le compte de l'application de données personnelles (DP). L'architecture de ce compte est un exemple de charge de travail qui collecte des données personnelles directement auprès des consommateurs. Dans cette charge de travail, les utilisateurs se connectent via un niveau Web. Le niveau Web interagit avec le niveau application. Ce niveau reçoit les entrées du niveau Web, traite et stocke les données, permet aux équipes internes autorisées et à des tiers d'accéder aux données, puis archive et supprime les données lorsqu'elles ne sont plus nécessaires. L'architecture est délibérément modulaire et axée sur les événements afin de démontrer de nombreuses techniques fondamentales d'ingénierie de confidentialité sans entrer dans des cas d'utilisation spécifiques, tels que les lacs de données, les conteneurs, le calcul ou l'Internet des objets (IoT).

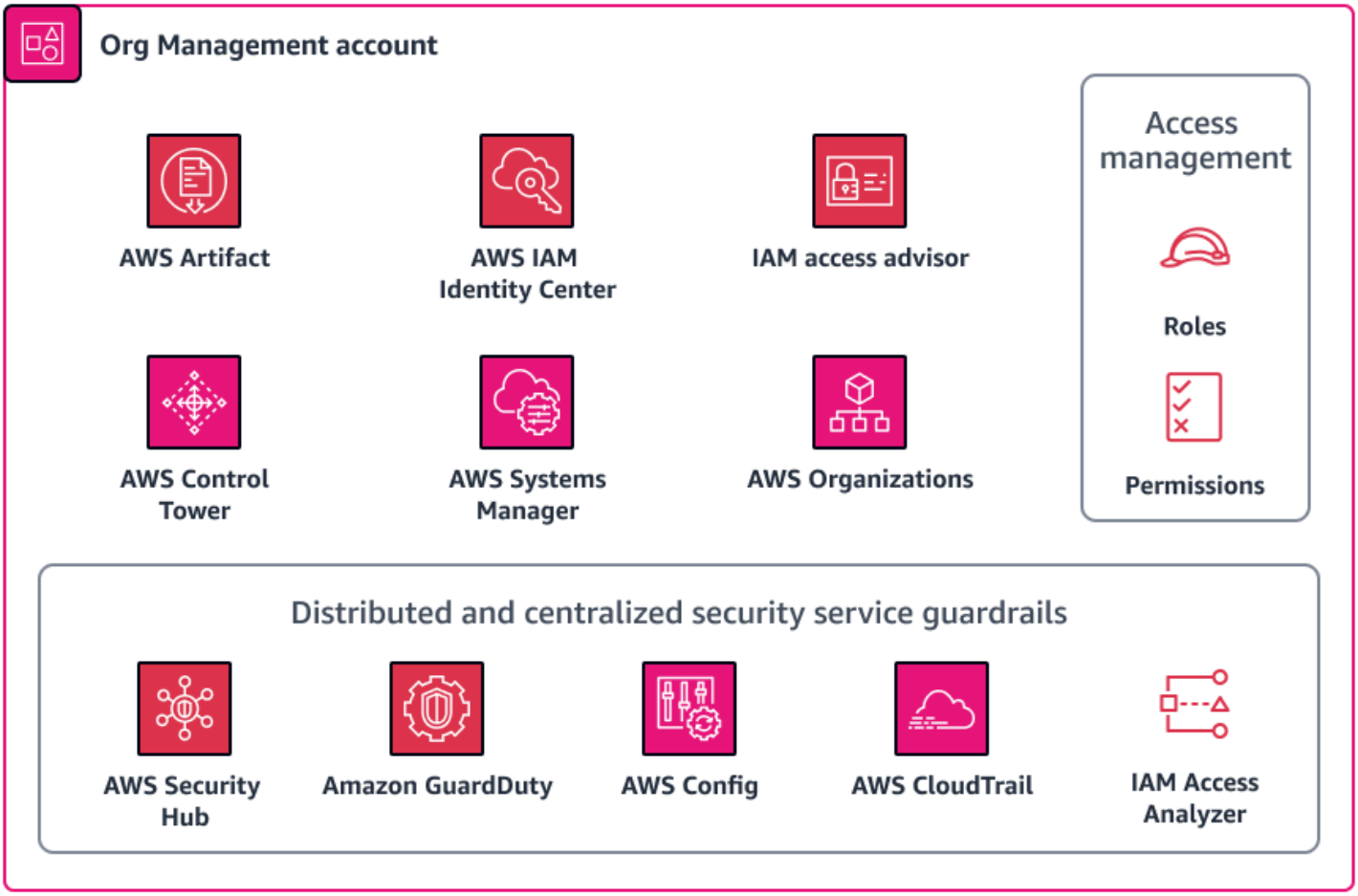
Ensuite, ce guide décrit en détail chaque compte de l'organisation. Il décrit les services et fonctionnalités liés à la confidentialité, les considérations et les recommandations, ainsi que des diagrammes pour chacun des comptes suivants :

- Compte de gestion de l'organisation
- Security OU — Compte Security Tooling
- Security OU — Compte Log Archive
- Infrastructure UO – Compte réseau
- Données personnelles OU — Compte d'application PDF

Compte de gestion de l'organisation

> Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Le compte Org Management est principalement utilisé pour gérer la dérive de la configuration des ressources pour les contrôles de confidentialité fondamentaux sur tous les comptes de votre organisation, qui est gérée par AWS Organizations. Ce compte est également l'endroit où vous pouvez déployer de nouveaux comptes membres de manière cohérente, avec les mêmes contrôles de sécurité et de confidentialité. Pour plus d'informations sur ce compte, consultez l'architecture AWS de référence de sécurité (AWS SRA). Le schéma suivant illustre les services AWS de sécurité et de confidentialité configurés dans le compte Org Management.



Cette section fournit des informations plus détaillées sur Services AWS les éléments suivants utilisés dans ce compte :

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifactpeut vous aider dans vos audits en proposant des téléchargements à la demande de documents de AWS sécurité et de conformité. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

Cela vous Service AWS permet de comprendre les contrôles dont vous héritez AWS et de déterminer ceux qu'il vous reste à implémenter dans votre environnement. AWS Artifact donne accès aux

rapports AWS de sécurité et de conformité, tels que les rapports sur les contrôles du système et de l'organisation (SOC) et les rapports du secteur des cartes de paiement (PCI). Il donne également accès aux certifications des organismes d'accréditation de toutes les zones géographiques et de tous les secteurs de conformité qui valident la mise en œuvre et l'efficacité opérationnelle des AWS contrôles. En utilisant AWS Artifact, vous pouvez fournir les artefacts AWS d'audit à vos auditeurs ou régulateurs comme preuve des contrôles de AWS sécurité. Les rapports suivants peuvent être utiles pour démontrer l'efficacité des contrôles de AWS confidentialité :

- Rapport de confidentialité SOC 2 Type 2 — Ce rapport démontre l'efficacité des AWS contrôles relatifs à la manière dont les données personnelles sont collectées, utilisées, conservées, divulguées et éliminées. Pour plus d'informations, consultez la FAQ du SOC.
- Rapport de confidentialité SOC 3 — Le rapport de confidentialité SOC 3 est une description moins détaillée des contrôles de confidentialité du SOC, destiné à une diffusion générale.
- Rapport de certification ISO/IEC 27701:2019 — L'ISO/IEC 27701:2019 décrit les exigences et les directives pour établir et améliorer continuellement un système de gestion des informations de confidentialité (PIMS). Ce rapport détaille l'étendue de cette certification et peut servir de preuve de AWS certification. Pour plus d'informations sur cette norme, consultez la norme ISO/IEC 27701:2019 (site Web de l'ISO).

AWS Control Tower

AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes conforme aux meilleures pratiques de sécurité prescriptives. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

Dans AWS Control Tower, vous pouvez également automatiser le déploiement d'un certain nombre de contrôles proactifs, préventifs et de détection, également appelés garde-fous, qui répondent à vos exigences en matière de résidence et de protection des données. Par exemple, vous pouvez définir des barrières de sécurité qui limitent le transfert de données aux données approuvées uniquement. Régions AWS Pour un contrôle encore plus précis, vous pouvez choisir parmi plus de 17 barrières conçues pour contrôler la résidence des données, telles que Interdire les connexions au réseau privé virtuel (VPN) Amazon, interdire l'accès à Internet pour une instance Amazon VPC et refuser l'accès en fonction de la demande. AWS Région AWS Ces garde-fous se composent d'un certain nombre de AWS CloudFormation crochets, de politiques de contrôle des services et de AWS Config règles qui peuvent être déployés de manière uniforme au sein de votre organisation. Pour plus d'informations,

consultez la section Contrôles qui améliorent la protection de résidence des données dans la AWS Control Tower documentation.

Si vous devez déployer des mesures de protection de la vie privée au-delà des contrôles de résidence des données, cela AWS Control Tower inclut un certain nombre de contrôles obligatoires. Ces contrôles sont déployés par défaut sur chaque unité organisationnelle lorsque vous configurez votre zone d'atterrissage. La plupart de ces contrôles sont préventifs conçus pour protéger les journaux, tels que l'interdiction de la suppression des archives de journaux et l'activation de la validation de l'intégrité du fichier CloudTrail journal.

AWS Control Tower est également intégré AWS Security Hub pour fournir des commandes de détection. Ces contrôles sont connus sous le nom de Service-Managed Standard :. AWS Control Tower Vous pouvez utiliser ces contrôles pour surveiller toute dérive de configuration des contrôles garantissant la confidentialité, tels que le chiffrement au repos pour les instances de base de données Amazon Relational Database Service (Amazon RDS).

AWS Organizations

Le AWS PRA permet AWS Organizations de gérer de manière centralisée tous les comptes au sein de l'architecture. Pour plus d'informations, consultez AWS Organizations et la structure de compte dédiée dans ce guide. Dans AWS Organizations, vous pouvez utiliser les politiques de contrôle des services (SCP) et les politiques de gestion pour protéger les données personnelles et la confidentialité.

Politiques de contrôle de service (SCP)

Les politiques de contrôle des services (SCP) sont un type de politique d'organisation que vous pouvez utiliser pour gérer les autorisations au sein de votre organisation. Ils fournissent un contrôle centralisé des autorisations maximales disponibles pour les rôles AWS Identity and Access Management (IAM) et les utilisateurs du compte cible, de l'unité organisationnelle (UO) ou de l'ensemble de l'organisation. Vous pouvez créer et appliquer des SCP à partir du compte Org Management.

Vous pouvez l'utiliser AWS Control Tower pour déployer les SCP de manière uniforme sur tous vos comptes. Pour plus d'informations sur les contrôles de résidence des données que vous pouvez appliquer AWS Control Tower, consultez AWS Control Tower ce guide. AWS Control Tower inclut une gamme complète de SCP préventifs. S' AWS Control Tower ils ne sont pas utilisés actuellement dans votre organisation, vous pouvez également déployer ces contrôles manuellement.

Utilisation des SCP pour répondre aux exigences de résidence des données

Il est courant de gérer les exigences de résidence des données personnelles en stockant et en traitant les données dans une région géographique spécifique. Afin de vérifier que les exigences uniques en matière de résidence des données d'une juridiction sont respectées, nous vous recommandons de travailler en étroite collaboration avec votre équipe réglementaire pour confirmer vos exigences. Une fois ces exigences déterminées, il existe un certain nombre de contrôles de confidentialité AWS fondamentaux qui peuvent vous aider. Par exemple, vous pouvez utiliser les SCP pour limiter ce qui Régions AWS peut être utilisé pour traiter et stocker des données. Pour un exemple de politique, consultez Limitez les transferts de données entre Régions AWS ce guide.

Utilisation de SCP pour limiter les appels d'API à haut risque

Il est important de comprendre quels sont les contrôles AWS de sécurité et de confidentialité qui sont responsables et ceux dont vous êtes responsable. Par exemple, vous êtes responsable des résultats des appels d'API qui pourraient être effectués contre l'API Services AWS que vous utilisez. Il vous incombe également de comprendre lesquels de ces appels peuvent entraîner des modifications de votre posture en matière de sécurité ou de confidentialité. Si vous êtes préoccupé par le maintien d'une certaine posture de sécurité et de confidentialité, vous pouvez activer les SCP qui refusent certains appels d'API. Ces appels d'API peuvent avoir des implications, telles que la divulgation involontaire de données personnelles ou des violations de transferts de données transfrontaliers spécifiques. Par exemple, vous souhaiterez peut-être interdire les appels d'API suivants :

- Permettre l'accès public aux compartiments Amazon Simple Storage Service (Amazon S3)
- Désactiver Amazon GuardDuty ou créer des règles de suppression pour les résultats d'exfiltration de données, tels que le test Trojan:EC2/DNS DataExfiltration
- Supprimer les règles d'exfiltration de AWS WAF données
- Partage public d'instantanés Amazon Elastic Block Store (Amazon EBS)
- Supprimer un compte membre de l'organisation
- Dissociation d'Amazon CodeGuru Reviewer d'un référentiel

Politiques de gestion

Les politiques de gestion AWS Organizations intégrées peuvent vous aider à configurer et à gérer Services AWS leurs fonctionnalités de manière centralisée. Les types de stratégie de gestion que vous choisissez déterminent la manière dont les politiques affectent les unités d'organisation et les

comptes qui en héritent. Les politiques relatives aux balises sont un exemple de politique de AWS Organizations gestion directement liée à la confidentialité.

Utilisation des politiques relatives aux balises

Les balises sont des paires clé-valeur qui vous aident à gérer, identifier, organiser, rechercher et filtrer AWS les ressources. Il peut être utile d'appliquer des balises qui distinguent les ressources de votre organisation qui traitent des données personnelles. L'utilisation de balises est compatible avec de nombreuses solutions de confidentialité présentées dans ce guide. Par exemple, vous pouvez appliquer une balise indiquant la classification générale des données traitées ou stockées dans la ressource. Vous pouvez écrire des politiques de contrôle d'accès basé sur les attributs (ABAC) qui limitent l'accès aux ressources dotées d'une balise ou d'un ensemble de balises en particulier. Par exemple, votre politique peut spécifier que le `SysAdmin` rôle ne peut pas accéder aux ressources dotées de cette `dataclassification:4` balise. Pour plus d'informations et un didacticiel, voir Définir les autorisations d'accès aux AWS ressources en fonction des balises dans la documentation IAM. En outre, si votre entreprise applique des politiques de conservation des données de manière générale AWS Backupà l'ensemble de vos sauvegardes dans de nombreux comptes, vous pouvez appliquer une balise qui place cette ressource dans le champ d'application de cette politique de sauvegarde.

Les politiques relatives aux balises vous aident à maintenir la cohérence des balises dans l'ensemble de votre organisation. Dans une politique de balises, vous spécifiez les règles qui s'appliquent aux ressources lorsqu'elles sont étiquetées. Par exemple, vous pouvez exiger que les ressources soient étiquetées avec des clés spécifiques, telles que `DataClassification` ou`DataSteward`, et vous pouvez spécifier des traitements de cas ou des valeurs valides pour les clés. Vous pouvez également recourir à l'application pour empêcher le traitement des demandes de balisage non conformes.

Lorsque vous utilisez des balises comme élément essentiel de votre stratégie de contrôle de confidentialité, tenez compte des points suivants :

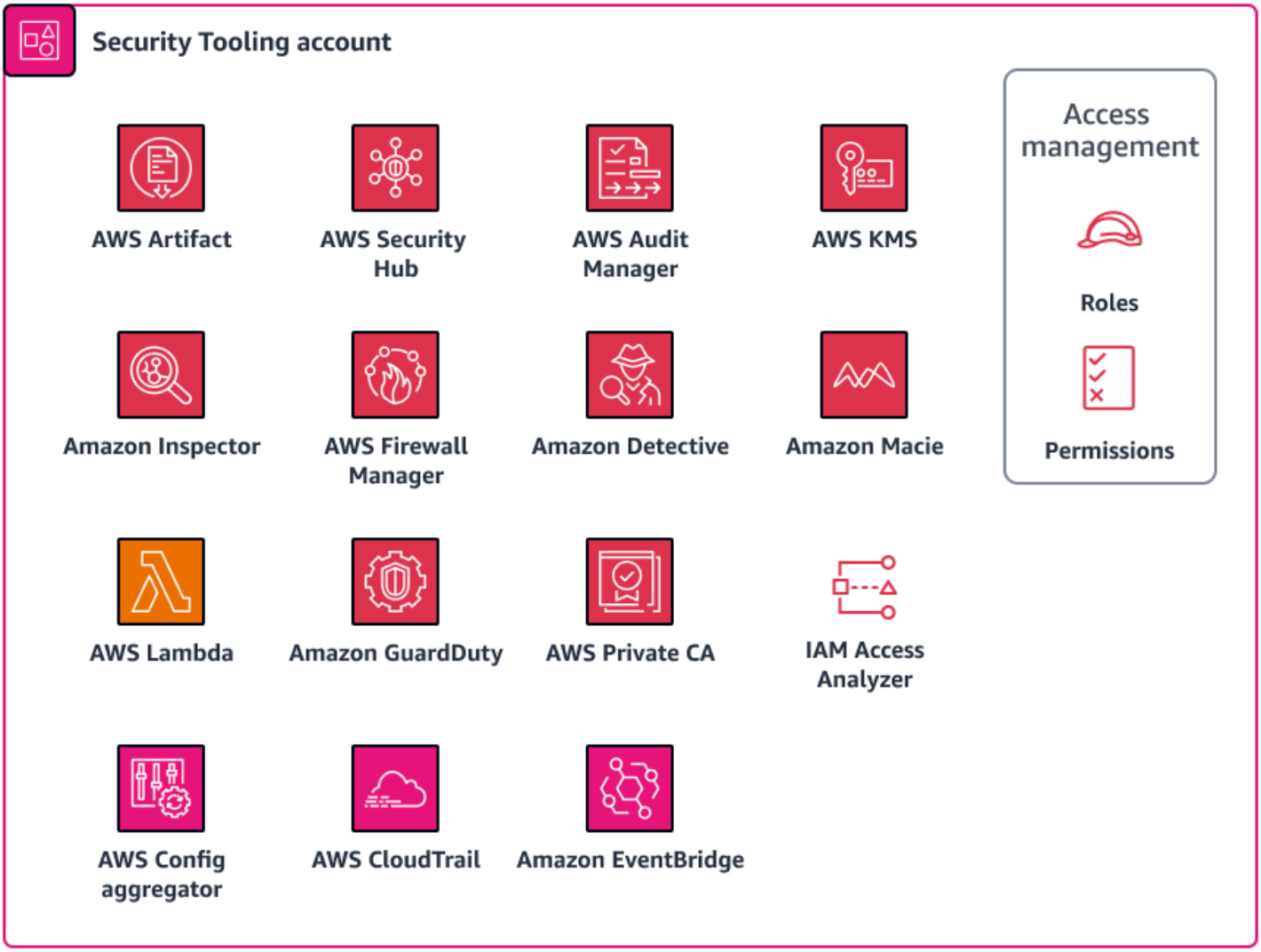
- Réfléchissez aux implications du placement de données personnelles ou d'autres types de données sensibles dans des clés ou des valeurs de balise. Lorsque vous contactez AWS une assistance technique, AWS il est possible que vous analysiez les balises et autres identifiants de ressources pour résoudre le problème. Dans ce cas, vous souhaiterez peut-être dépersonnaliser les valeurs des balises, puis les réidentifier à l'aide d'un système contrôlé par le client, tel qu'un système de gestion des services informatiques (ITSM). AWS recommande de ne pas inclure d'informations personnelles identifiables dans les balises.

- N'oubliez pas que certaines valeurs de balises doivent être rendues immuables (non modifiables) pour empêcher le contournement des contrôles techniques, telles que les conditions ABAC qui reposent sur des balises.

Security OU — Compte Security Tooling

> Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Le compte Security Tooling est dédié à l'exploitation des services fondamentaux de sécurité et de confidentialité, à la surveillance Comptes AWS et à l'automatisation des alertes et réponses en matière de sécurité et de confidentialité. Pour plus d'informations sur ce compte, consultez l'architecture AWS de référence de sécurité (AWS SRA). Le schéma suivant illustre les services AWS de sécurité et de confidentialité configurés dans le compte Security Tooling.



Cette section fournit des informations plus détaillées sur les éléments suivants de ce compte :

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- IAM Access Analyzer
- Amazon Macie

AWS CloudTrail

AWS CloudTrailvous aide à auditer l'activité globale des API dans votre Compte AWS. L'activation CloudTrail de tous Comptes AWS ceux Régions AWS qui stockent, traitent ou transmettent des

données personnelles peut vous aider à suivre l'utilisation et la divulgation de ces données. L'architecture AWS de référence de sécurité recommande d'activer un suivi organisationnel, qui est un suivi unique qui enregistre tous les événements pour tous les comptes de l'organisation. Cependant, l'activation de ce suivi organisationnel permet d'agréger les données du journal multirégional dans un seul compartiment Amazon Simple Storage Service (Amazon S3) dans le compte Log Archive. Pour les comptes qui traitent des données personnelles, cela peut entraîner des considérations de conception supplémentaires. Les enregistrements du journal peuvent contenir des références à des données personnelles. Pour répondre à vos exigences en matière de résidence et de transfert des données, vous devrez peut-être reconsidérer l'agrégation des données des journaux interrégionaux dans une seule région où se trouve le compartiment S3. Votre organisation peut se demander quelles charges de travail régionales devraient être incluses ou exclues du parcours organisationnel. Pour les charges de travail que vous décidez d'exclure du suivi de l'organisation, vous pouvez envisager de configurer un suivi spécifique à la région qui masque les données personnelles. Pour plus d'informations sur le masquage des données personnelles, consultez la Amazon Data Firehose section de ce guide. En fin de compte, votre organisation peut avoir à la fois des traces organisationnelles et des pistes régionales agrégées dans le compte Log Archive centralisé.

Pour plus d'informations sur la configuration d'un suivi à région unique, consultez les instructions d'utilisation du AWS Command Line Interface (AWS CLI) ou de la console. Lorsque vous créez le journal de l'organisation, vous pouvez utiliser un paramètre d'inscription ou vous pouvez créer le journal directement dans la CloudTrail console. AWS Control Tower

Pour plus d'informations sur l'approche globale et sur la manière de gérer la centralisation des journaux et les exigences en matière de transfert de données, consultez la Stockage centralisé des journaux section de ce guide. Quelle que soit la configuration choisie, vous souhaiterez peut-être séparer la gestion des traces dans le compte Security Tooling du stockage des journaux dans le compte Log Archive, selon la AWS SRA. Cette conception vous permet de créer des politiques d'accès avec le moindre privilège pour ceux qui ont besoin de gérer les journaux et ceux qui ont besoin d'utiliser les données des journaux.

AWS Config

AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier les liens entre les ressources et l'évolution de leurs configurations au fil du temps. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

Dans AWS Config, vous pouvez déployer des packs de conformité, qui sont des ensembles de AWS Config règles et d'actions correctives. Les packs de conformité fournissent un cadre général conçu pour permettre des contrôles de gouvernance en matière de confidentialité, de sécurité, d'exploitation et d'optimisation des coûts à l'aide de règles gérées ou personnalisées. AWS Config Vous pouvez utiliser cet outil dans le cadre d'un ensemble plus large d'outils d'automatisation pour vérifier si les configurations de vos AWS ressources sont conformes aux exigences de votre propre cadre de contrôle.

Le pack de conformité Operational Best Practices for NIST Privacy Framework v1.0 est aligné sur un certain nombre de contrôles liés à la confidentialité du NIST Privacy Framework. Chaque AWS Config règle s'applique à un type de AWS ressource spécifique et concerne un ou plusieurs contrôles du NIST Privacy Framework. Vous pouvez utiliser ce pack de conformité pour suivre la conformité continue en matière de confidentialité entre les ressources de vos comptes. Voici certaines des règles incluses dans ce pack de conformité :

- `no-unrestricted-route-to-igw`— Cette règle permet d'empêcher l'exfiltration de données sur le plan de données en surveillant en permanence les tables de routage VPC pour détecter les itinéraires `0.0.0.0/0` par défaut `::/0` ou de sortie vers une passerelle Internet. Cela vous permet de limiter les endroits où le trafic lié à Internet peut être envoyé, en particulier si certaines plages d'adresses CIDR sont connues pour être malveillantes.
- `encrypted-volumes`— Cette règle vérifie si les volumes Amazon Elastic Block Store (Amazon EBS) attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont chiffrés. Si votre organisation a des exigences de contrôle spécifiques relatives à l'utilisation des clés AWS Key Management Service (AWS KMS) pour la protection des données personnelles, vous pouvez spécifier des identifiants de clé spécifiques dans le cadre de la règle afin de vérifier que les volumes sont chiffrés avec une AWS KMS clé spécifique.
- `restricted-common-ports`— Cette règle vérifie si les groupes de sécurité Amazon EC2 autorisent un trafic TCP illimité vers des ports spécifiques. Les groupes de sécurité peuvent vous aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Le blocage du trafic entrant `0.0.0.0/0` vers les ports courants, tels que TCP 3389 et TCP 21, sur vos ressources vous permet de restreindre l'accès à distance.

AWS Config peut être utilisé pour des contrôles de conformité proactifs et réactifs de vos AWS ressources. En plus de prendre en compte les règles contenues dans les packs de conformité, vous pouvez intégrer ces règles dans les modes d'évaluation détective et proactive. Cela permet de mettre en œuvre des contrôles de confidentialité plus tôt dans le cycle de développement de votre

logiciel, car les développeurs d'applications peuvent commencer à intégrer des contrôles avant le déploiement. Par exemple, ils peuvent inclure des hooks dans leurs AWS CloudFormation modèles qui vérifient que la ressource déclarée dans le modèle est conforme à toutes les AWS Config règles relatives à la confidentialité pour lesquelles le mode proactif est activé. Pour plus d'informations, consultez AWS Config Rules Now Support Proactive Compliance (billet de AWS blog).

Amazon GuardDuty

AWS propose plusieurs services qui peuvent être utilisés pour stocker ou traiter des données personnelles, tels qu'Amazon S3, Amazon Relational Database Service (Amazon RDS) ou Amazon EC2 avec Kubernetes. Amazon GuardDuty associe une visibilité intelligente à une surveillance continue pour détecter les indicateurs susceptibles d'être liés à la divulgation involontaire de données personnelles. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

Vous pouvez GuardDuty ainsi identifier les activités potentiellement malveillantes liées à la confidentialité tout au long du cycle de vie d'une attaque. Par exemple, GuardDuty peut vous avertir en cas de connexions à des sites sur liste noire, de trafic ou de volumes de trafic inhabituels sur les ports réseau, d'exfiltration DNS, de lancements inattendus d'instances EC2 et d'appels inhabituels d'un fournisseur de services Internet. Vous pouvez également configurer pour arrêter GuardDuty les alertes relatives aux adresses IP fiables provenant de vos propres listes d'adresses IP fiables et pour émettre des alertes sur les adresses IP malveillantes connues provenant de vos propres listes de menaces.

Comme le recommande la AWS SRA, vous pouvez activer le compte Security Tooling GuardDuty pour tous Comptes AWS les membres de votre organisation et configurer le compte Security Tooling en tant qu'administrateur GuardDuty délégué. GuardDutyregroupe les résultats de l'ensemble de l'organisation dans ce compte unique. Pour plus d'informations, consultez la section Gestion GuardDuty des comptes avec AWS Organizations. Vous pouvez également envisager d'identifier toutes les parties prenantes liées à la confidentialité dans le processus de réponse aux incidents, de la détection et de l'analyse au confinement et à l'éradication, et de les impliquer dans tout incident susceptible d'impliquer une exfiltration de données.

IAM Access Analyzer

De nombreux clients veulent avoir l'assurance permanente que les données personnelles sont partagées de manière appropriée avec des sous-traitants tiers préapprouvés et prévus, et aucune autre entité. Un périmètre de données est un ensemble de barrières préventives conçues pour

permettre uniquement aux identités fiables issues des réseaux attendus d'accéder aux ressources fiables de votre AWS environnement. Lorsque vous définissez des contrôles pour la divulgation involontaire et intentionnelle de données personnelles, vous pouvez définir des identités fiables, des ressources fiables et des réseaux attendus.

Avec AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), les organisations peuvent définir une Compte AWS zone de confiance et configurer des alertes en cas de violation de cette zone de confiance. IAM Access Analyzer analyse les politiques IAM pour aider à identifier et à résoudre les accès publics ou intercomptes involontaires à des ressources potentiellement sensibles. IAM Access Analyzer utilise la logique mathématique et l'inférence pour générer des résultats complets pour les ressources accessibles depuis l'extérieur d'un. Compte AWS Enfin, pour répondre aux politiques IAM trop permissives et y remédier, vous pouvez utiliser IAM Access Analyzer pour valider les politiques existantes par rapport aux meilleures pratiques IAM et fournir des suggestions. IAM Access Analyzer peut générer une politique IAM de moindre privilège basée sur l'activité d'accès antérieure d'un principal IAM. Il analyse CloudTrail les journaux et génère une politique qui n'accorde que les autorisations nécessaires pour continuer à effectuer ces tâches.

Pour plus d'informations sur la manière dont IAM Access Analyzer est utilisé dans un contexte de sécurité, consultez l'architecture de référence AWS de sécurité.

Amazon Macie

Amazon Macie est un service qui utilise l'apprentissage automatique et la correspondance de modèles pour découvrir les données sensibles, fournit une visibilité sur les risques liés à la sécurité des données et vous aide à automatiser les protections contre ces risques. Macie génère des résultats lorsqu'il détecte des violations potentielles des politiques ou des problèmes liés à la sécurité ou à la confidentialité de vos compartiments Amazon S3. Macie est un autre outil que les entreprises peuvent utiliser pour mettre en œuvre l'automatisation afin de soutenir les efforts de conformité. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

Macie peut détecter une liste importante et croissante de types de données sensibles, y compris des informations personnelles identifiables (PII), telles que des noms, des adresses et d'autres attributs identifiables. Vous pouvez même créer des identifiants de données personnalisés afin de définir des critères de détection qui reflètent la définition des données personnelles de votre organisation.

Lorsque votre entreprise définit des contrôles préventifs pour vos compartiments Amazon S3 contenant des données personnelles, vous pouvez utiliser Macie comme mécanisme de validation

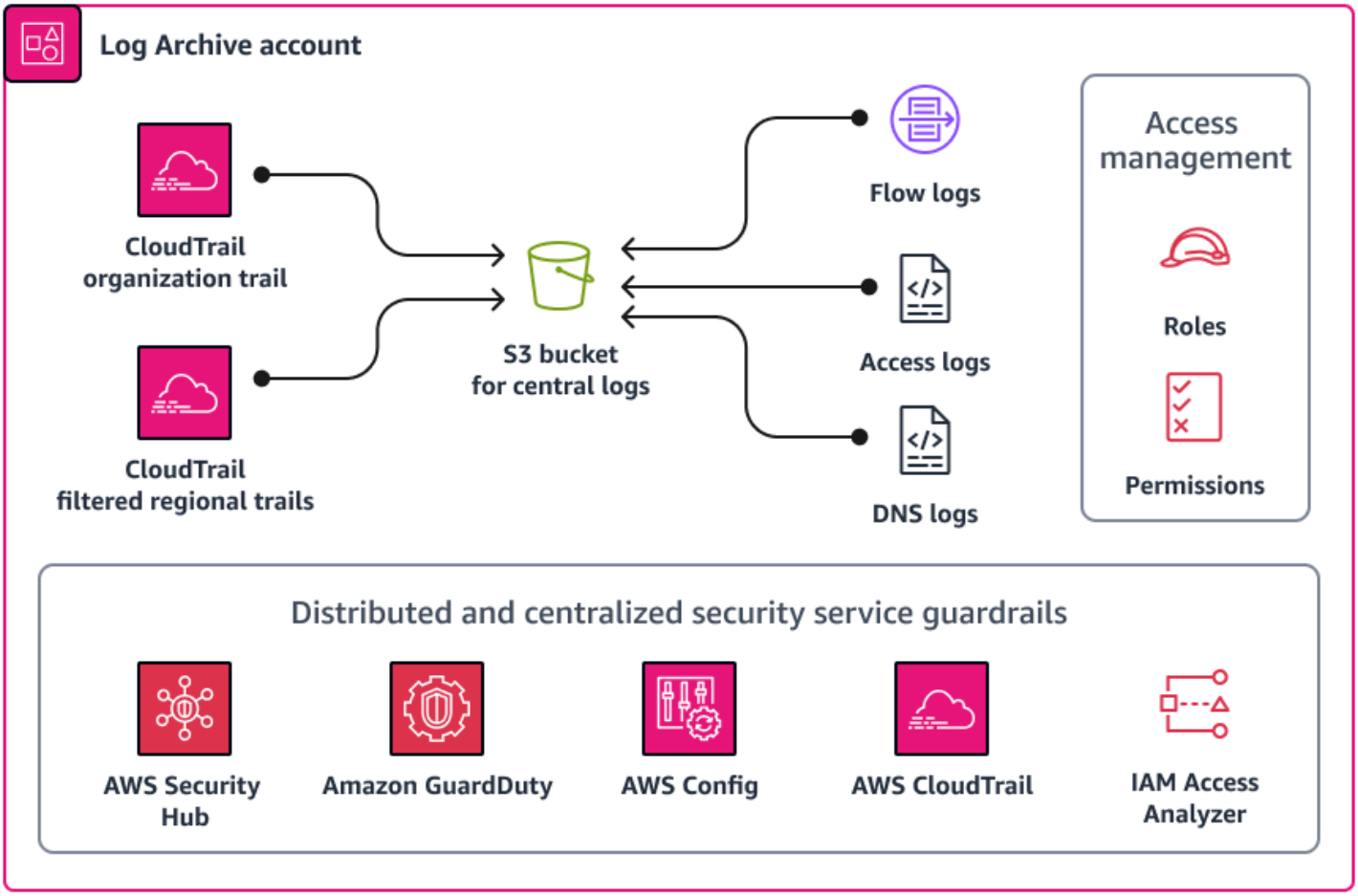
afin de garantir en permanence l'emplacement de vos données personnelles et la manière dont elles sont protégées. Pour commencer, activez Macie et configurez la découverte automatique des données sensibles. Macie analyse en permanence les objets dans tous vos compartiments S3, quels que soient les comptes et. Régions AWS Macie génère et tient à jour une carte thermique interactive qui indique où se trouvent les données personnelles. La fonctionnalité de découverte automatique des données sensibles est conçue pour réduire les coûts et minimiser le besoin de configurer manuellement les tâches de découverte. Vous pouvez vous appuyer sur la fonctionnalité de découverte automatique des données sensibles et utiliser Macie pour détecter automatiquement les nouveaux compartiments ou les nouvelles données dans les compartiments existants, puis valider les données par rapport aux balises de classification des données attribuées. Configurez cette architecture pour informer les équipes de développement et de confidentialité appropriées des buckets mal classés ou non classés en temps opportun.

Vous pouvez activer Macie pour tous les comptes de votre organisation en utilisant AWS Organizations. Pour plus d'informations, consultez la section Intégration et configuration d'une organisation dans Amazon Macie.

Security OU — Compte Log Archive

> Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Le compte Log Archive vous permet de centraliser les types de journaux d'infrastructure, de service et d'application. Pour plus d'informations sur ce compte, consultez l'architecture AWS de référence de sécurité (AWS SRA). Avec un compte dédié aux journaux, vous pouvez appliquer des alertes cohérentes à tous les types de journaux et confirmer que les intervenants en cas d'incident peuvent accéder à un ensemble de ces journaux à partir d'un seul endroit. Vous pouvez également configurer les contrôles de sécurité et les politiques de conservation des données à partir d'un seul endroit, ce qui peut simplifier les frais opérationnels liés à la confidentialité. Le schéma suivant illustre les services AWS de sécurité et de confidentialité configurés dans le compte Log Archive.



Stockage centralisé des journaux

Les fichiers journaux (tels que AWS CloudTrail les journaux) peuvent contenir des informations pouvant être considérées comme des données personnelles. Certaines organisations choisissent d'utiliser un suivi organisationnel afin de regrouper CloudTrail les journaux des comptes en un seul emplacement central, à des fins de visibilité. Régions AWS Pour plus d'informations, consultez AWS CloudTrail dans ce guide. Lors de la mise en œuvre de la centralisation des CloudTrail journaux, ceux-ci sont généralement stockés dans un compartiment Amazon Simple Storage Service (Amazon S3) situé dans une seule région.

En fonction de la définition des données personnelles de votre organisation et des réglementations régionales applicables en matière de confidentialité, vous devrez peut-être envisager des transferts de données transfrontaliers. Si votre organisation doit satisfaire aux exigences de transfert de données en vertu des réglementations régionales en matière de confidentialité, les options suivantes peuvent vous aider :

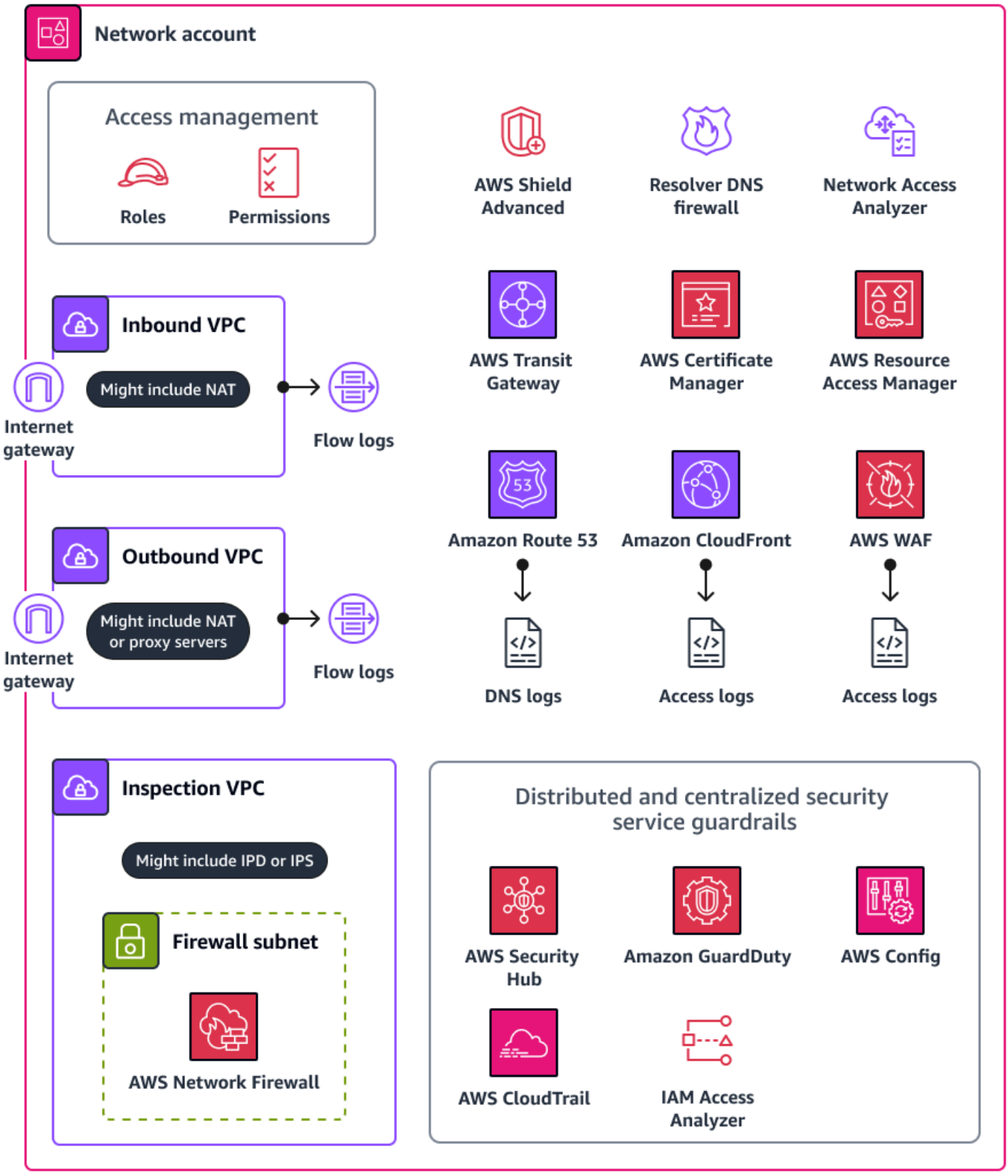
1. Si votre organisation fournit des services AWS Cloud à des personnes concernées dans plusieurs pays, vous pouvez choisir d'agréger tous les journaux dans le pays qui applique les exigences de résidence des données les plus strictes. Par exemple, si vous opérez en Allemagne et que ce pays est soumis aux exigences les plus strictes, vous pouvez agréger les données dans un compartiment S3 `eu-central-1` Région AWS afin que les données collectées en Allemagne ne quittent pas les frontières allemandes. Pour cette option, vous pouvez configurer un suivi organisationnel unique CloudTrail qui regroupe les journaux de tous les comptes et de Régions AWS la région cible.
2. Supprimez les données personnelles qui doivent rester dans le fichier Région AWS avant qu'elles ne soient copiées et agrégées dans une autre région. Par exemple, vous pouvez masquer les données personnelles dans la région hôte de l'application avant de transférer les journaux vers une autre région. Pour plus d'informations sur le masquage des données personnelles, consultez la Amazon Data Firehose section de ce guide.

Travaillez avec votre conseiller juridique pour déterminer quelles données personnelles sont concernées et quels transferts de AWS région à région sont autorisés.

Infrastructure UO – Compte réseau

> Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Dans le compte Réseau, vous gérez la mise en réseau entre vos clouds privés virtuels (VPC) et l'Internet au sens large. Dans ce compte, vous pouvez mettre en œuvre des mécanismes de contrôle de divulgation étendus en utilisant AWS WAF, use AWS Resource Access Manager (AWS RAM) pour partager des sous-réseaux VPC et des AWS Transit Gateway pièces jointes, et utiliser Amazon CloudFront pour prendre en charge une utilisation ciblée des services. Pour plus d'informations sur ce compte, consultez l'architecture AWS de référence de sécurité (AWS SRA). Le schéma suivant illustre les services AWS de sécurité et de confidentialité configurés dans le compte réseau.


Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Cette section fournit des informations plus détaillées sur Services AWS les éléments suivants utilisés dans ce compte :

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront prend en charge les restrictions géographiques pour les applications frontales et l'hébergement de fichiers. CloudFrontpeuvent diffuser du contenu par le biais d'un réseau mondial de centres de données appelés « emplacements périphériques ». Lorsqu'un utilisateur demande le contenu que vous diffusez CloudFront, la demande est acheminée vers l'emplacement périphérique offrant la latence la plus faible. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

Vous pouvez utiliser des restrictions CloudFront géographiques pour empêcher les utilisateurs situés dans des zones géographiques spécifiques d'accéder au contenu que vous distribuez par le biais d'une CloudFront distribution. Pour plus d'informations et pour connaître les options de configuration relatives aux restrictions géographiques, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Vous pouvez également configurer CloudFront pour générer des journaux d'accès contenant des informations détaillées sur chaque demande d'utilisateur CloudFront reçue. Pour plus d'informations, consultez la section Configuration et utilisation des journaux standard (journaux d'accès) dans la CloudFront documentation. Enfin, s'il CloudFront est configuré pour mettre en cache le contenu sur une série d'emplacements périphériques, vous pouvez prendre en compte l'endroit où la mise en cache a lieu. Pour certaines organisations, la mise en cache interrégionale peut être soumise à des exigences de transfert de données transfrontalier.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) vous permet de partager vos ressources en toute sécurité afin Comptes AWS de réduire les frais opérationnels et de garantir visibilité et auditabilité. Les organisations peuvent ainsi restreindre les AWS ressources qui peuvent être partagées avec d'autres membres Comptes AWS de leur organisation ou avec des comptes tiers. AWS RAM

Pour plus d'informations, consultez la section AWS Ressources partageables. Dans le compte réseau, vous pouvez l'utiliser AWS RAM pour partager des sous-réseaux VPC et des connexions de passerelle de transit. Si vous avez l'habitude AWS RAM de partager une connexion de plan de données avec une autre personne Compte AWS, envisagez de mettre en place des processus pour vérifier que les connexions sont établies conformément aux normes préapprouvées Régions AWS.

Outre le partage de VPC et de connexions aux passerelles de transit, il AWS RAM peut être utilisé pour partager des ressources qui ne prennent pas en charge les politiques basées sur les ressources IAM. Pour une charge de travail hébergée dans l'unité d'organisation des données personnelles, vous pouvez accéder AWS RAM à des données personnelles situées dans une unité séparée Compte AWS. Pour plus d'informations, consultez la section relative AWS Resource Access Manager au compte de l'UO sur les données personnelles — DP Application.

AWS Transit Gateway

Si vous souhaitez déployer AWS des ressources qui collectent, stockent ou traitent des données personnelles conformément aux exigences de votre organisation en Régions AWS matière de résidence des données et si vous disposez des garanties techniques appropriées, envisagez de mettre en place des garde-fous pour empêcher les flux de données transfrontaliers non approuvés sur les plans de contrôle et de données. Sur le plan de contrôle, vous pouvez limiter l'utilisation des régions et, par conséquent, les flux de données entre régions en utilisant des politiques IAM et de contrôle des services.

Il existe plusieurs options pour contrôler les flux de données entre régions sur le plan de données. Par exemple, vous pouvez utiliser les tables de routage, le peering VPC et les pièces jointes. AWS Transit Gateway AWS Transit Gatewayest un hub central qui connecte les clouds privés virtuels (VPC) et les réseaux sur site. Dans le cadre de votre zone d'atterrissage AWS élargie, vous pouvez envisager les différentes manières dont les données peuvent être transmises Régions AWS, notamment par le biais de passerelles Internet, par le biais du peering direct entre VPC et par le peering interrégional avec. AWS Transit Gateway Par exemple, vous pouvez effectuer les opérations suivantes dans AWS Transit Gateway :

- Vérifiez que les connexions est-ouest et nord-sud entre vos VPC et les environnements sur site sont conformes à vos exigences de confidentialité.
- Configurez les paramètres VPC conformément à vos exigences de confidentialité.
- Utilisez une politique de contrôle des services AWS Organizations et des politiques IAM pour empêcher toute modification de votre configuration AWS Transit Gateway et de celle d'Amazon

Virtual Private Cloud (Amazon VPC). Pour un exemple de politique de contrôle des services, consultez Restreindre les modifications apportées aux configurations VPC ce guide.

AWS WAF

Pour empêcher la divulgation involontaire de données personnelles, vous pouvez déployer une defense-in-depth approche pour vos applications Web. Vous pouvez intégrer la validation des entrées et la limitation du débit à votre application, mais cela AWS WAF peut également constituer une autre ligne de défense. AWS WAFest un pare-feu d'applications Web qui vous aide à surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources protégées de votre application Web. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

Avec AWS WAF, vous pouvez définir et déployer des règles qui vérifient des critères spécifiques. Les activités suivantes peuvent être associées à la divulgation involontaire de données personnelles :

- Trafic provenant d'adresses IP ou d'emplacements géographiques inconnus ou malveillants
- Les 10 principales attaques de l'Open Worldwide Application Security Project (OWASP), y compris les attaques liées à l'exfiltration telles que l'injection SQL
- Des taux élevés de demandes
- Trafic général des bots
- Grattoirs de contenu

Vous pouvez déployer des groupes de AWS WAF règles gérés par AWS. Certains groupes de règles gérés pour AWS WAF peuvent être utilisés pour détecter les menaces à la vie privée et aux données personnelles, par exemple :

- Base de données SQL — Ce groupe de règles contient des règles conçues pour bloquer les modèles de demandes associés à l'exploitation de bases de données SQL, tels que les attaques par injection SQL. Envisagez ce groupe de règles si votre application s'interface avec une base de données SQL.
- Entrées erronées connues — Ce groupe de règles contient des règles conçues pour bloquer les modèles de demandes dont on sait qu'ils ne sont pas valides et qui sont associés à l'exploitation ou à la découverte de vulnérabilités.

- Contrôle des robots : ce groupe de règles contient des règles conçues pour gérer les demandes émanant de robots, qui peuvent consommer des ressources excédentaires, fausser les indicateurs commerciaux, provoquer des interruptions de service et mener des activités malveillantes.
- Prévention du piratage de compte (ATP) : ce groupe de règles contient des règles conçues pour empêcher les tentatives malveillantes de piratage de compte. Ce groupe de règles inspecte les tentatives de connexion envoyées au point de terminaison de connexion de votre application.

Données personnelles OU — Compte d'application PDF

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

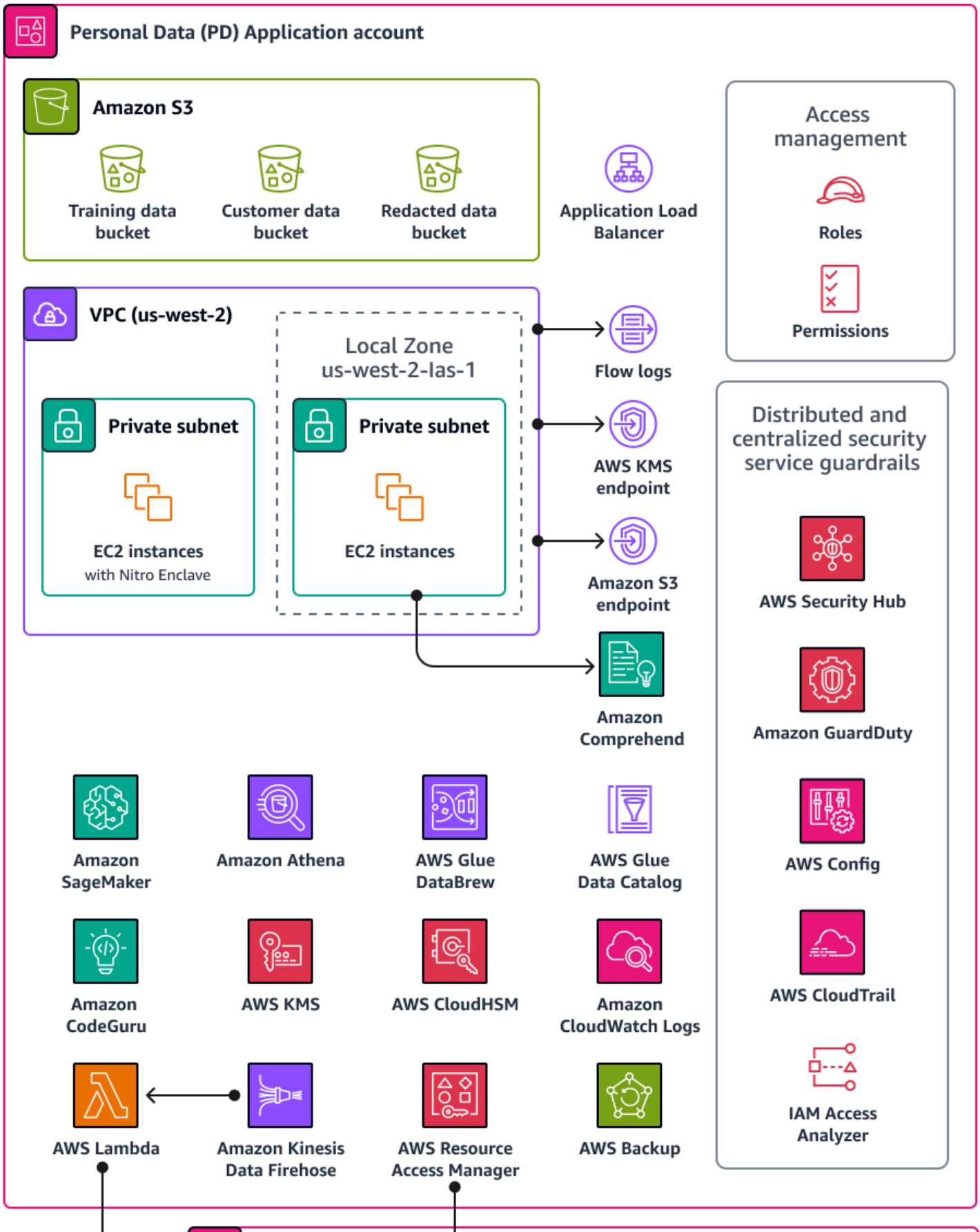
Le compte d'application de données personnelles (DP) est l'endroit où votre organisation héberge les services qui collectent et traitent les données personnelles. Plus précisément, vous pouvez stocker ce que vous définissez comme des données personnelles dans ce compte. Le AWS PRA présente un certain nombre d'exemples de configurations de confidentialité via une architecture Web sans serveur à plusieurs niveaux. Lorsqu'il s'agit d'exploiter des charges de travail dans une zone d' AWS atterrissage, les configurations de confidentialité ne doivent pas être considérées comme one-size-fits-all des solutions. Par exemple, votre objectif peut être de comprendre les concepts sous-jacents, comment ils peuvent améliorer la confidentialité et comment votre organisation peut appliquer des solutions à vos cas d'utilisation et à vos architectures particuliers.

Comptes AWS En effet, au sein de votre organisation qui collecte, stocke ou traite des données personnelles, vous pouvez utiliser AWS Organizations et AWS Control Tower déployer des garde-fous fondamentaux et reproductibles. La mise en place d'une unité organisationnelle (UO) dédiée à ces comptes est essentielle. Par exemple, vous souhaiterez peut-être appliquer des mesures de protection relatives à la résidence des données uniquement à un sous-ensemble de comptes pour lesquels la résidence des données est une considération de conception essentielle. Pour de nombreuses entreprises, il s'agit des comptes qui stockent et traitent les données personnelles.

Votre organisation peut proposer un compte de données dédié, dans lequel vous stockez la source officielle de vos ensembles de données personnels. Une source de données faisant autorité est un emplacement où vous stockez la version principale des données, qui peut être considérée comme la version la plus fiable et la plus précise des données. Par exemple, vous pouvez copier les données de la source de données officielle vers d'autres emplacements, tels que les compartiments Amazon

Simple Storage Service (Amazon S3) du compte d'application DP qui sont utilisés pour stocker les données de formation, un sous-ensemble de données clients et des données expurgées. En adoptant cette approche multi-comptes pour séparer les ensembles de données personnelles complets et définitifs du compte Data des charges de travail des consommateurs en aval dans le compte d'application DP, vous pouvez réduire l'impact en cas d'accès non autorisé à vos comptes.

Le schéma suivant illustre les services AWS de sécurité et de confidentialité configurés dans les comptes DP Application et Data.


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local Zone us-west-2-las-1
Flow logs
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
Amazon Comprehend
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
AWS Config
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS CloudTrail
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
IAM Access Analyzer
Data account
Access management

Cette section fournit des informations plus détaillées sur Services AWS les éléments suivants utilisés dans ces comptes :

- Amazon Athena
- Amazon CloudWatch Logs
- CodeGuru Réviseur Amazon
- Amazon Comprehend
- Amazon Data Firehose
- AWS Glue
- AWS Key Management Service
- AWS Zones Locales
- AWS Enclaves Nitro
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker
- AWS fonctionnalités qui aident à gérer le cycle de vie des données
- Services et fonctionnalités AWS qui aident à segmenter les données

Amazon Athena

Vous pouvez également envisager des contrôles de limitation des requêtes de données pour atteindre vos objectifs de confidentialité. Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard. Il n'est pas nécessaire de charger les données dans Athena ; cela fonctionne directement avec les données stockées dans des compartiments S3.

Un cas d'utilisation courant pour Athena consiste à fournir aux équipes d'analyse des données des ensembles de données personnalisés et nettoyés. Si les ensembles de données contiennent des données personnelles, vous pouvez nettoyer l'ensemble de données en masquant des colonnes entières de données personnelles qui n'apportent que peu de valeur aux équipes d'analyse des données. Pour plus d'informations, consultez Anonymiser et gérer les données de votre lac de données avec Amazon Athena AWS Lake Formation et AWS (article de blog).

Si votre approche de transformation des données nécessite une flexibilité supplémentaire en dehors des fonctions prises en charge par Athena, vous pouvez définir des fonctions personnalisées,

appelées fonctions définies par l'utilisateur (UDF). Vous pouvez invoquer des UDF dans une requête SQL soumise à Athena, et ils s'exécutent. AWS Lambda Vous pouvez utiliser des UDF dans `SELECT` les `FILTER SQL` requêtes et vous pouvez invoquer plusieurs UDF dans la même requête. Pour des raisons de confidentialité, vous pouvez créer des UDF qui effectuent des types spécifiques de masquage des données, par exemple en n'affichant que les quatre derniers caractères de chaque valeur d'une colonne.

Amazon CloudWatch Logs

Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes et applications, Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité. Dans CloudWatch Logs, vous pouvez utiliser une politique de protection des données pour les groupes de journaux nouveaux ou existants afin de minimiser le risque de divulgation de données personnelles. Les politiques de protection des données peuvent détecter des données sensibles, telles que des données personnelles, dans vos journaux. La politique de protection des données peut masquer ces données lorsque les utilisateurs accèdent aux journaux via le AWS Management Console. Lorsque les utilisateurs ont besoin d'un accès direct aux données personnelles, conformément à l'objectif global de votre charge de travail, vous pouvez `logs:Unmask` leur attribuer des autorisations. Vous pouvez également créer une politique de protection des données à l'échelle du compte et appliquer cette politique de manière cohérente à tous les comptes de votre organisation. Cela permet de configurer le masquage par défaut pour tous les groupes de journaux actuels et futurs dans CloudWatch Logs. Nous vous recommandons également d'activer les rapports d'audit et de les envoyer à un autre groupe de journaux, à un compartiment Amazon S3 ou à Amazon Data Firehose. Ces rapports contiennent un enregistrement détaillé des résultats relatifs à la protection des données pour chaque groupe de journaux.

CodeGuru Réviseur Amazon

Pour des raisons de confidentialité et de sécurité, il est essentiel pour de nombreuses entreprises de garantir une conformité continue pendant les phases de déploiement et après le déploiement. Le AWS PRA inclut des contrôles proactifs dans les pipelines de déploiement pour les applications qui traitent des données personnelles. Amazon CodeGuru Reviewer peut détecter les défauts potentiels susceptibles d'exposer des données personnelles dans du code Java et Python. JavaScript Il propose des suggestions aux développeurs pour améliorer le code. CodeGuru Le réviseur peut identifier les défauts dans un large éventail de bonnes pratiques générales en matière de sécurité, de confidentialité et de bonnes pratiques générales. Pour plus d'informations, consultez la bibliothèque Amazon CodeGuru Detector. Il est conçu pour fonctionner avec plusieurs fournisseurs

de sources AWS CodeCommit, notamment Bitbucket et Amazon S3. GitHub Parmi les défauts liés à la confidentialité que le CodeGuru réviseur peut détecter, citons :

- injection de code SQL
- Cookies non sécurisés
- Autorisation manquante
- Rechiffrement côté client AWS KMS

Amazon Comprehend

Amazon Comprehend est un service de traitement du langage naturel (NLP) qui utilise l'apprentissage automatique pour découvrir des informations et des connexions précieuses dans des documents texte en anglais. Amazon Comprehend peut détecter et supprimer des données personnelles dans des documents texte structurés, semi-structurés ou non structurés. Pour plus d'informations, consultez la section Informations personnelles identifiables (PII) dans la documentation Amazon Comprehend.

Vous pouvez utiliser les kits SDK AWS et l'API Amazon Comprehend pour intégrer Amazon Comprehend à de nombreuses applications. Par exemple, Amazon Comprehend permet de détecter et de supprimer des données personnelles avec Amazon S3 Object Lambda. Organisations peuvent utiliser S3 Object Lambda pour ajouter du code personnalisé aux requêtes GET d'Amazon S3 afin de modifier et de traiter les données lorsqu'elles sont renvoyées à une application. S3 Object Lambda peut filtrer les lignes, redimensionner les images de manière dynamique, supprimer des données personnelles, etc. Alimenté par AWS Lambda des fonctions, le code s'exécute sur une infrastructure entièrement gérée par AWS, ce qui élimine le besoin de créer et de stocker des copies dérivées de vos données ou d'exécuter des proxys. Vous n'avez pas besoin de modifier vos applications pour transformer des objets avec S3 Object Lambda. Vous pouvez utiliser la fonction `ComprehendPiiRedactionS3Object` Lambda AWS Serverless Application Repository pour supprimer des données personnelles. Cette fonction utilise Amazon Comprehend pour détecter les entités de données personnelles et les expédie en les remplaçant par des astérisques. Pour plus d'informations, consultez la section Détection et suppression de données personnelles avec S3 Object Lambda et Amazon Comprehend dans la documentation Amazon S3.

Amazon Comprehend propose de nombreuses options d'intégration d'applications via les kits SDK AWS. Vous pouvez donc utiliser Amazon Comprehend pour identifier les données personnelles dans de nombreux endroits où vous collectez, stockez et traitez les données. Vous pouvez utiliser les

fonctionnalités d'Amazon Comprehend ML pour détecter et supprimer les données personnelles dans les journaux des applications (article de AWS blog), les e-mails des clients, les tickets d'assistance, etc. Le schéma d'architecture du compte d'application DP montre comment exécuter cette fonction pour les journaux d'applications sur Amazon EC2. Amazon Comprehend propose deux modes de rédaction :

- `REPLACE_WITH_PII_ENTITY_TYPE`remplace chaque entité PII par ses types. Par exemple, Jane Doe serait remplacée par NAME.
- `MASK`remplace les caractères des entités PII par un personnage de votre choix (! , #, $, %, &, ou @). Par exemple, Jane Doe pourrait être remplacée par **** ***.

Amazon Data Firehose

Amazon Data Firehose peut être utilisé pour capturer, transformer et charger des données de streaming dans des services en aval, tels qu'Amazon Managed Service pour Apache Flink ou Amazon S3. Firehose est souvent utilisé pour transporter de grandes quantités de données en streaming, telles que les journaux d'applications, sans avoir à créer des pipelines de traitement à partir de zéro.

Vous pouvez utiliser les fonctions Lambda pour effectuer un traitement personnalisé ou intégré avant que les données ne soient envoyées en aval. Pour des raisons de confidentialité, cette fonctionnalité prend en charge les exigences de minimisation des données et de transfert de données transfrontalier. Par exemple, vous pouvez utiliser Lambda et Firehose pour transformer les données de journaux multirégionales avant qu'elles ne soient centralisées dans le compte Log Archive. Pour plus d'informations, voir Biogen : solution de journalisation centralisée pour plusieurs comptes (YouTube vidéo). Dans le compte DP Application, vous configurez Amazon CloudWatch et vous pouvez AWS CloudTrail transférer les journaux vers un flux de diffusion Firehose. Une fonction Lambda transforme les journaux et les envoie vers un compartiment S3 central dans le compte Log Archive. Vous pouvez configurer la fonction Lambda pour masquer des champs spécifiques contenant des données personnelles. Cela permet d'empêcher le transfert de données personnelles Régions AWS. En utilisant cette approche, les données personnelles sont masquées avant le transfert et la centralisation, plutôt qu'après. Pour les demandes émanant de juridictions qui ne sont pas soumises aux exigences de transfert transfrontalier, il est généralement plus efficace sur le plan opérationnel et rentable d'agréger les journaux par le biais du processus organisationnel. CloudTrail Pour plus d'informations, consultez AWS CloudTrail la section Security OU — Security Tooling account de ce guide.

AWS Glue

La gestion des ensembles de données contenant des données personnelles est un élément clé de la protection de la vie privée dès la conception. Les données d'une organisation peuvent exister sous des formes structurées, semi-structurées ou non structurées. Les ensembles de données personnelles dépourvus de structure peuvent compliquer l'exécution d'un certain nombre d'opérations visant à renforcer la confidentialité, notamment la minimisation des données, le suivi des données attribuées à une seule personne dans le cadre d'une demande de la personne concernée, la garantie d'une qualité constante des données et la segmentation globale des ensembles de données. AWS Glueest un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il peut vous aider à classer, nettoyer, enrichir et déplacer les données entre les magasins de données et les flux de données. AWS Glue les fonctionnalités sont conçues pour vous aider à découvrir, préparer, structurer et combiner des ensembles de données à des fins d'analyse, d'apprentissage automatique et de développement d'applications. Vous pouvez l'utiliser AWS Glue pour créer une structure prévisible et commune au-dessus de vos ensembles de données existants. AWS Glue Data Catalog AWS Glue DataBrew, et la qualité AWS Glue des données sont des AWS Glue fonctionnalités qui peuvent contribuer à répondre aux exigences de confidentialité de votre entreprise.

AWS Glue Data Catalog

AWS Glue Data Catalogvous aide à établir des ensembles de données maintenables. Le catalogue de données contient des références aux données utilisées comme sources et cibles pour les tâches d'extraction, de transformation et de chargement (ETL) dans AWS Glue. Les informations du catalogue de données sont stockées sous forme de tables de métadonnées, et chaque table indique un magasin de données unique. Vous exécutez un AWS Glue robot d'exploration pour inventorier les données dans différents types de magasins de données. Vous ajoutez des classificateurs intégrés et personnalisés au robot d'exploration, et ces classificateurs déduisent le format des données et le schéma des données personnelles. Le robot d'exploration écrit ensuite les métadonnées dans le catalogue de données. Une table de métadonnées centralisée peut faciliter la réponse aux demandes des personnes concernées (telles que le droit à l'effacement), car elle ajoute de la structure et de la prévisibilité aux différentes sources de données personnelles de votre environnement. AWS Pour un exemple complet de la façon d'utiliser Data Catalog pour répondre automatiquement à ces demandes, consultez Gérer les demandes d'effacement de données dans votre lac de données avec Amazon S3 Find and Forget (article de AWS blog). Enfin, si votre organisation a l'habitude d'AWS Lake Formationadministrer et de fournir un accès précis aux bases de données, aux tables, aux lignes et aux cellules, le catalogue de données est un élément clé. Data Catalog permet le partage

de données entre comptes et vous aide à utiliser le contrôle d'accès basé sur des balises pour gérer votre lac de données à grande échelle (article de AWS blog).

AWS Glue DataBrew

AWS Glue DataBrewvous aide à nettoyer et à normaliser les données, et il peut effectuer des transformations sur les données, telles que la suppression ou le masquage d'informations personnelles identifiables et le chiffrement de champs de données sensibles dans des pipelines de données. Vous pouvez également cartographier visuellement le lignage de vos données afin de comprendre les différentes sources de données et les étapes de transformation par lesquelles les données ont été soumises. Cette fonctionnalité devient de plus en plus importante à mesure que votre organisation s'efforce de mieux comprendre et suivre la provenance des données personnelles. DataBrew vous aide à masquer les données personnelles lors de la préparation des données. Vous pouvez détecter les données personnelles dans le cadre d'un travail de profilage des données et recueillir des statistiques, telles que le nombre de colonnes susceptibles de contenir des données personnelles et les catégories potentielles. Vous pouvez ensuite utiliser des techniques intégrées de transformation des données réversibles ou irréversibles, notamment la substitution, le hachage, le chiffrement et le déchiffrement, le tout sans écrire de code. Vous pouvez ensuite utiliser les ensembles de données nettoyés et masqués en aval pour des tâches d'analyse, de reporting et d'apprentissage automatique. Certaines des techniques de masquage de données disponibles DataBrew incluent :

- Hachage — Appliquez des fonctions de hachage aux valeurs des colonnes.
- Substitution — Remplacez les données personnelles par d'autres valeurs d'apparence authentique.
- Annulation ou suppression : remplacez un champ spécifique par une valeur nulle ou supprimez la colonne.
- Masquage : utilisez le brouillage de caractères ou masquez certaines parties des colonnes.

Les techniques de chiffrement disponibles sont les suivantes :

- Chiffrement déterministe : appliquez des algorithmes de chiffrement déterministes aux valeurs des colonnes. Le chiffrement déterministe produit toujours le même texte chiffré pour une valeur.
- Chiffrement probabiliste : appliquez des algorithmes de chiffrement probabiliste aux valeurs des colonnes. Le chiffrement probabiliste produit un texte chiffré différent chaque fois qu'il est appliqué.

Pour une liste complète des recettes de transformation des données personnelles fournies dans DataBrew, voir Étapes de recette relatives aux informations personnelles identifiables (PII).

AWS Glue Qualité des données

AWS Glue Data Quality vous aide à automatiser et à opérationnaliser la diffusion de données de haute qualité dans les pipelines de données, de manière proactive, avant qu'elles ne soient livrées à vos consommateurs de données. AWS Glue Data Quality fournit une analyse statistique des problèmes de qualité des données dans l'ensemble de vos pipelines de données, peut déclencher des alertes sur Amazon EventBridge et peut recommander des règles de qualité pour y remédier. AWS Glue Data Quality prend également en charge la création de règles dans un langage spécifique au domaine afin que vous puissiez créer des règles de qualité des données personnalisées.

AWS Key Management Service

AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données. AWS KMS utilise des modules de sécurité matériels pour protéger et valider AWS KMS keys dans le cadre du programme de validation des modules cryptographiques FIPS 140-2. Pour plus d'informations sur la manière dont ce service est utilisé dans un contexte de sécurité, consultez l'architecture AWS de référence de sécurité.

AWS KMS s'intègre à la plupart Services AWS des solutions de chiffrement, et vous pouvez utiliser des clés KMS dans vos applications qui traitent et stockent des données personnelles. Vous pouvez AWS KMS les utiliser pour répondre à diverses exigences en matière de confidentialité et protéger les données personnelles, notamment :

- Utilisation de clés gérées par le client pour un meilleur contrôle de la force, de la rotation, de l'expiration et d'autres options.
- Utilisation de clés dédiées gérées par le client pour protéger les données personnelles et les secrets permettant d'accéder aux données personnelles.
- Définition des niveaux de classification des données et désignation d'au moins une clé dédiée gérée par le client par niveau. Par exemple, vous pouvez avoir une clé pour chiffrer les données opérationnelles et une autre pour chiffrer les données personnelles.
- Empêcher l'accès involontaire aux clés KMS entre comptes.
- Stockage des clés KMS dans la même ressource Compte AWS que la ressource à chiffrer.

- Mise en œuvre de la séparation des tâches pour l'administration et l'utilisation des clés KMS. Pour plus d'informations, consultez Comment utiliser KMS et IAM pour activer des contrôles de sécurité indépendants pour les données chiffrées dans S3 (article de AWS blog).
- Renforcer la rotation automatique des clés grâce à des glissières de sécurité préventives et réactives.

Par défaut, les clés KMS sont stockées et ne peuvent être utilisées que dans la région où elles ont été créées. Si votre organisation a des exigences spécifiques en matière de résidence et de souveraineté des données, déterminez si les clés KMS multirégionales sont adaptées à votre cas d'utilisation. Les clés multirégionales sont des clés KMS spécifiques, différentes, Régions AWS qui peuvent être utilisées de manière interchangeable. Le processus de création d'une clé multirégionale déplace votre matériel clé au-delà des Région AWS frontières internes AWS KMS, de sorte que cette absence d'isolement régional peut ne pas être compatible avec les objectifs de conformité de votre organisation. L'un des moyens de résoudre ce problème consiste à utiliser un autre type de clé KMS, par exemple une clé gérée par le client spécifique à une région.

AWS Zones Locales

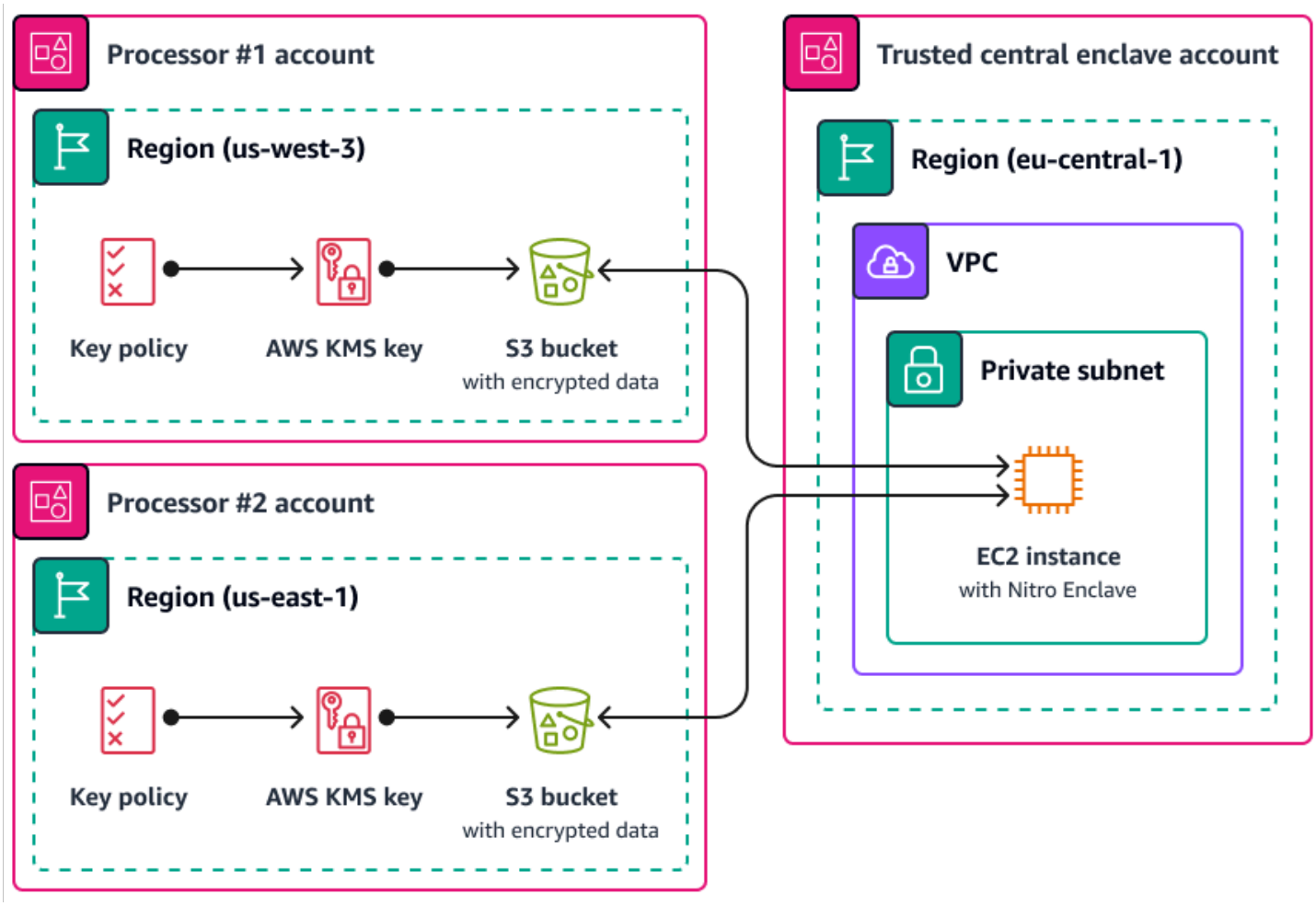
Si vous devez respecter les exigences relatives à la résidence des données, vous pouvez déployer des ressources qui stockent et traitent les données personnelles spécifiquement Régions AWS pour répondre à ces exigences. Vous pouvez également utiliser les Zones AWS Locales, qui vous permettent de placer le calcul, le stockage, les bases de données et d'autres AWS ressources sélectionnées à proximité de grands centres industriels et peuplés. Une zone locale est une extension d'une Région AWS zone située à proximité géographique d'une grande région métropolitaine. Vous pouvez placer des types spécifiques de ressources au sein d'une zone locale, à proximité de la région à laquelle correspond la zone locale. Les Zones Locales peuvent vous aider à satisfaire aux exigences de résidence des données lorsqu'une région n'est pas disponible au sein de la même juridiction légale. Lorsque vous utilisez des Zones Locales, tenez compte des contrôles de résidence des données déployés au sein de votre organisation. Par exemple, vous pourriez avoir besoin d'un contrôle pour empêcher les transferts de données d'une zone locale spécifique vers une autre région. Pour plus d'informations sur l'utilisation des SCP pour maintenir des barrières de sécurité en matière de transfert de données transfrontalier, consultez les meilleures pratiques pour gérer la résidence des données dans les zones AWS locales à l'aide des contrôles de zone d'atterrissage (AWS article de blog).

AWS Enclaves Nitro

Réfléchissez à votre stratégie de segmentation des données du point de vue du traitement, par exemple le traitement des données personnelles avec un service informatique tel qu'Amazon Elastic Compute Cloud (Amazon EC2). L'informatique confidentielle dans le cadre d'une stratégie d'architecture plus large peut vous aider à isoler le traitement des données personnelles dans une enclave CPU isolée, protégée et fiable. Les enclaves sont des machines virtuelles distinctes, renforcées et soumises à des contraintes élevées. AWS Nitro Enclaves est une fonctionnalité d'Amazon EC2 qui peut vous aider à créer ces environnements informatiques isolés. Pour plus d'informations, consultez La conception de la sécurité du système AWS Nitro (AWS livre blanc).

Les enclaves Nitro déploient un noyau séparé du noyau de l'instance parent. Le noyau de l'instance parent n'a pas accès à l'enclave. Les utilisateurs ne peuvent pas utiliser SSH ou accéder à distance aux données et aux applications de l'enclave. Les applications qui traitent des données personnelles peuvent être intégrées dans l'enclave et configurées pour utiliser le Vsock de l'enclave, le socket qui facilite la communication entre l'enclave et l'instance parent.

L'un des cas d'utilisation dans lesquels Nitro Enclaves peut être utile est le traitement conjoint entre deux processeurs de données distincts Régions AWS et susceptibles de ne pas se faire confiance. L'image suivante montre comment vous pouvez utiliser une enclave pour le traitement centralisé, une clé KMS pour chiffrer les données personnelles avant leur envoi à l'enclave et une AWS KMS key politique qui vérifie que l'enclave demandant le déchiffrement possède les mesures uniques indiquées dans son document d'attestation. Pour plus d'informations et d'instructions, consultez la section Utilisation d'une attestation cryptographique avec AWS KMS. Pour un exemple de politique clé, consultez Exiger une attestation pour utiliser une AWS KMS clé ce guide.



Avec cette implémentation, seuls les processeurs de données respectifs et l'enclave sous-jacente ont accès aux données personnelles en texte clair. Le seul endroit où les données sont exposées, en dehors de l'environnement des processeurs de données respectifs, est dans l'enclave elle-même, qui est conçue pour empêcher l'accès et la falsification.

AWS PrivateLink

De nombreuses entreprises souhaitent limiter l'exposition des données personnelles à des réseaux non fiables. Par exemple, si vous souhaitez améliorer la confidentialité de la conception globale de votre architecture d'application, vous pouvez segmenter les réseaux en fonction de la sensibilité des données (similaire à la séparation logique et physique des ensembles de données décrite dans la Services et fonctionnalités AWS qui aident à segmenter les données section). AWS PrivateLinkvous permet de créer des connexions privées unidirectionnelles entre vos clouds privés virtuels (VPC) et des services extérieurs au VPC. Vous pouvez ainsi configurer des connexions privées dédiées aux services qui stockent ou traitent des données personnelles dans votre environnement ; il

n'est pas nécessaire de vous connecter à des points de terminaison publics et de transférer ces données sur des réseaux publics non fiables. AWS PrivateLink Lorsque vous activez les points de terminaison de AWS PrivateLink service pour les services concernés, il n'est pas nécessaire de disposer d'une passerelle Internet, d'un périphérique NAT, d'une adresse IP publique, d'une AWS Direct Connect connexion ou d' AWS Site-to-Site VPN une connexion pour communiquer. Lorsque vous vous connectez AWS PrivateLink à un service qui fournit un accès aux données personnelles, vous pouvez utiliser des politiques de point de terminaison VPC et des groupes de sécurité pour contrôler l'accès, conformément à la définition du périmètre de données de votre organisation. Pour un exemple de politique de point de terminaison VPC autorisant uniquement les principes et les AWS ressources IAM d'une organisation fiable à accéder à un point de terminaison de service, consultez ce guideExiger l'adhésion à l'organisation pour accéder aux ressources VPC.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) vous permet de partager vos ressources en toute sécurité afin Comptes AWS de réduire les frais opérationnels et de garantir visibilité et auditabilité. Lorsque vous planifiez votre stratégie de segmentation multi-comptes, pensez AWS RAM à partager les banques de données personnelles que vous stockez dans un compte distinct et isolé. Vous pouvez partager ces données personnelles avec d'autres comptes fiables à des fins de traitement. Dans AWS RAM, vous pouvez gérer les autorisations qui définissent les actions pouvant être effectuées sur les ressources partagées. Tous les appels d'API AWS RAM sont connectés CloudTrail. Vous pouvez également configurer Amazon CloudWatch Events pour qu'il vous avertisse automatiquement en cas d'événements spécifiques AWS RAM, par exemple lorsque des modifications sont apportées à un partage de ressources.

Bien que vous puissiez partager de nombreux types de AWS ressources avec d'autres personnes en Comptes AWS utilisant des politiques basées sur les ressources dans IAM ou des politiques de compartiment dans Amazon S3, cela AWS RAM offre plusieurs avantages supplémentaires en termes de confidentialité. AWS fournit aux propriétaires de données une visibilité supplémentaire sur la manière dont les données sont partagées et avec qui Comptes AWS, notamment :

- Possibilité de partager une ressource avec une unité d'organisation complète au lieu de mettre à jour manuellement les listes d'identifiants de compte
- Mise en œuvre du processus d'invitation pour l'initiation du partage si le compte client ne fait pas partie de votre organisation
- Visibilité sur les principaux responsables de l'IAM ayant accès à chaque ressource individuelle

Si vous avez déjà utilisé une politique basée sur les ressources pour gérer un partage de ressources et que vous souhaitez l'utiliser à la AWS RAM place, utilisez l'opération PromoteResourceShareCreatedFromPolicyAPI.

Amazon SageMaker

Amazon SageMaker est un service géré d'apprentissage automatique (ML) qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production. SageMaker est conçu pour faciliter la préparation des données d'entraînement et la création des fonctionnalités du modèle.

Amazon SageMaker Model Monitor

De nombreuses entreprises prennent en compte la dérive des données lors de la formation de modèles de machine learning. La dérive des données est une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML. Si la nature statistique des données qu'un modèle ML reçoit en production s'éloigne de la nature des données de référence sur lesquelles il a été entraîné, la précision des prédictions peut diminuer. Amazon SageMaker Model Monitor peut surveiller en permanence la qualité des modèles d'apprentissage SageMaker automatique Amazon en production et surveiller la qualité des données. La détection précoce et proactive de la dérive des données peut vous aider à mettre en œuvre des mesures correctives, telles que la reconversion des modèles, l'audit des systèmes en amont ou la résolution des problèmes de qualité des données. Model Monitor peut réduire le besoin de surveiller manuellement les modèles ou de créer des outils supplémentaires.

Amazon SageMaker Clarifier

Amazon SageMaker Clarify fournit des informations sur le biais et l'explicabilité du modèle. SageMakerClarify est couramment utilisé lors de la préparation des données du modèle ML et de la phase globale de développement. Les développeurs peuvent spécifier des attributs intéressants, tels que le sexe ou l'âge, et SageMaker Clarify exécute un ensemble d'algorithmes pour détecter toute présence de biais dans ces attributs. Une fois l'algorithme exécuté, SageMaker Clarify fournit un rapport visuel avec une description des sources et des mesures du biais possible afin que vous puissiez identifier les étapes à suivre pour remédier au biais. Par exemple, dans un ensemble de données financières qui ne contient que quelques exemples de prêts commerciaux accordés à un groupe d'âge par rapport à d'autres, vous SageMaker pourriez détecter des déséquilibres afin d'éviter

un modèle qui défavorise ce groupe d'âge. Vous pouvez également vérifier la présence de biais dans les modèles déjà entraînés en examinant leurs prévisions et en surveillant en permanence la présence de biais dans ces modèles de ML. Enfin, SageMaker Clarify est intégré à Amazon SageMaker Experiments pour fournir un graphique qui explique les fonctionnalités qui ont le plus contribué au processus global de prévision d'un modèle. Ces informations peuvent être utiles pour obtenir des résultats d'explicabilité, et elles peuvent vous aider à déterminer si une entrée de modèle particulière a plus d'influence qu'elle ne le devrait sur le comportement global du modèle.

Carte SageMaker modèle Amazon

Amazon SageMaker Model Card peut vous aider à documenter les détails essentiels de vos modèles de machine learning à des fins de gouvernance et de reporting. Ces informations peuvent inclure le propriétaire du modèle, l'objectif général, les cas d'utilisation prévus, les hypothèses formulées, l'évaluation du risque d'un modèle, les détails et les indicateurs de formation, ainsi que les résultats de l'évaluation. Pour plus d'informations, consultez Modéliser l'explicabilité avec les solutions d'intelligence AWS artificielle et de Machine Learning (AWS livre blanc).

AWS fonctionnalités qui aident à gérer le cycle de vie des données

Lorsque les données personnelles ne sont plus nécessaires, vous pouvez utiliser le cycle de vie et time-to-live les politiques des données dans de nombreux magasins de données différents. Lors de la configuration des politiques de conservation des données, tenez compte des emplacements suivants susceptibles de contenir des données personnelles :

- Bases de données, telles qu'Amazon DynamoDB et Amazon Relational Database Service (Amazon RDS)
- Compartiments Amazon S3
- Logs provenant de CloudWatch et CloudTrail
- Données mises en cache provenant de migrations dans AWS Database Migration Service (AWS DMS) et AWS Glue DataBrew de projets
- Sauvegardes et instantanés

Les fonctionnalités Services AWS et fonctionnalités suivantes peuvent vous aider à configurer les politiques de conservation des données dans vos AWS environnements :

- Amazon S3 Lifecycle : ensemble de règles qui définissent les actions qu'Amazon S3 applique à un groupe d'objets. Dans la configuration du cycle de vie d'Amazon S3, vous pouvez créer des actions

d'expiration qui définissent le moment où Amazon S3 supprime les objets expirés en votre nom. Pour plus d'informations, voir Gestion du cycle de vie de votre stockage.

- Amazon Data Lifecycle Manager — Dans Amazon EC2, créez une politique qui automatise la création, la conservation et la suppression des instantanés Amazon Elastic Block Store (Amazon EBS) et des Amazon Machine Images (AMI) soutenues par EBS.
- DynamoDB Time to Live (TTL) : définissez un horodatage par élément qui détermine le moment où un élément n'est plus nécessaire. Peu après la date et l'heure de l'horodatage spécifié, DynamoDB supprime l'élément de votre tableau.
- Paramètres de conservation CloudWatch des journaux dans Logs : vous pouvez ajuster la politique de conservation de chaque groupe de journaux à une valeur comprise entre 1 jour et 10 ans.
- AWS Backup— Déployez de manière centralisée des politiques de protection des données pour configurer, gérer et gouverner votre activité de sauvegarde sur diverses AWS ressources, notamment les compartiments S3, les instances de base de données RDS, les tables DynamoDB, les volumes EBS, etc. Appliquez des politiques de sauvegarde à vos AWS ressources en spécifiant les types de ressources ou en fournissant une granularité supplémentaire en les appliquant en fonction des balises de ressources existantes. Auditez et générez des rapports sur les activités de sauvegarde à partir d'une console centralisée afin de répondre aux exigences de conformité en matière de sauvegarde.

Services et fonctionnalités AWS qui aident à segmenter les données

La segmentation des données est le processus par lequel vous stockez les données dans des conteneurs distincts. Cela peut vous aider à fournir des mesures de sécurité et d'authentification différenciées pour chaque ensemble de données et à réduire l'impact de l'exposition sur votre ensemble de données dans son ensemble de données. Par exemple, au lieu de stocker toutes les données clients dans une grande base de données, vous pouvez segmenter ces données en groupes plus petits et plus faciles à gérer.

Vous pouvez utiliser la séparation physique et logique pour segmenter les données personnelles :

- Séparation physique — Le fait de stocker des données dans des magasins de données distincts ou de distribuer vos données dans AWS des ressources distinctes. Bien que les données soient physiquement séparées, les deux ressources peuvent être accessibles aux mêmes personnes. C'est pourquoi nous recommandons de combiner séparation physique et séparation logique.
- Séparation logique — Action d'isoler des données à l'aide de contrôles d'accès. Les différentes fonctions professionnelles nécessitent différents niveaux d'accès à des sous-ensembles de

données personnelles. Pour un exemple de politique qui implémente la séparation logique, consultez Accorder l'accès à des attributs Amazon DynamoDB spécifiques ce guide.

La combinaison d'une séparation logique et physique apporte flexibilité, simplicité et granularité lors de la rédaction de politiques basées sur l'identité et les ressources afin de permettre un accès différencié entre les fonctions professionnelles. Par exemple, il peut être complexe d'un point de vue opérationnel de créer les politiques qui séparent logiquement les différentes classifications de données dans un même compartiment S3. L'utilisation de compartiments S3 dédiés pour chaque classification de données simplifie la configuration et la gestion des politiques.

Exemples de politiques relatives à la confidentialité

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

De nombreuses entreprises qui traitent des données sensibles adoptent une approche préventive, en mettant en œuvre plusieurs niveaux de détection et de contrôles réactifs. Cette section fournit des exemples de politiques relatives à la confidentialité pour AWS Identity and Access Management (IAM) AWS Organizations, et (). AWS Key Management Service AWS KMS Ces politiques peuvent aider votre entreprise à atteindre divers objectifs de confidentialité en matière d'utilisation, de limitation de divulgation et de transfert transfrontalier de données en utilisant une approche préventive. Bon nombre de ces politiques sont référencées dans les sections précédentes de ce guide.

Cette section contient les exemples de politiques suivants :

- Exiger un accès à partir d'adresses IP spécifiques
- Exiger l'adhésion à l'organisation pour accéder aux ressources VPC
- Limitez les transferts de données entre Régions AWS
- Accorder l'accès à des attributs Amazon DynamoDB spécifiques
- Restreindre les modifications apportées aux configurations VPC
- Exiger une attestation pour utiliser une AWS KMS clé

Exiger un accès à partir d'adresses IP spécifiques

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Cette politique permet à l'`john_stiles`utilisateur d'assumer des rôles IAM uniquement si l'appel provient d'une adresse IP comprise dans les plages `192.0.2.0/24` ou`203.0.113.0/24`. Cette politique peut aider à prévenir la divulgation involontaire de données personnelles et les transferts

de données transfrontaliers indésirables. Par exemple, si le personnel du service clientèle de votre organisation a besoin d'accéder à des données personnelles, vous souhaiterez peut-être que ce personnel d'assistance n'accède à ces données qu'à partir des bureaux situés dans un sous-ensemble spécifique Régions AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

Exiger l'adhésion à l'organisation pour accéder aux ressources VPC

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Cette politique de point de terminaison VPC autorise uniquement les principaux AWS Identity and Access Management (IAM) et les ressources de l'`o-1abcde123`organisation à accéder aux points de terminaison Amazon Personalize (Amazon S3). Ce contrôle préventif permet d'établir une zone de confiance et de définir le périmètre des données personnelles. Pour plus d'informations sur la manière dont cette politique peut contribuer à protéger la confidentialité et les données personnelles au sein de votre organisation, consultez AWS PrivateLink ce guide.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

Limitez les transferts de données entre Régions AWS

> Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

À l'exception de deux rôles AWS Identity and Access Management (IAM), cette politique de contrôle des services refuse les appels d'API Services AWS aux entités régionales Régions AWS autres que `eu-west-1` et`eu-central-1`. Ce SCP peut aider à empêcher la création de services de AWS stockage et de traitement dans les régions non approuvées. Cela peut contribuer à empêcher le traitement des données personnelles Services AWS dans toutes ces régions. Cette politique utilise un `NotAction` paramètre car elle prend en compte les services AWS mondiaux, tels que IAM, et les services intégrés aux services mondiaux, tels que AWS Key Management Service (AWS KMS) et

Amazon CloudFront. Dans les valeurs des paramètres, vous pouvez spécifier ces services globaux et autres services non applicables en tant qu'exceptions. Pour plus d'informations sur la manière dont cette politique peut contribuer à protéger la confidentialité et les données personnelles au sein de votre organisation, consultez AWS Organizations ce guide.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
```

```
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Accorder l'accès à des attributs Amazon DynamoDB spécifiques

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Lorsque votre entreprise discute des stratégies visant à séparer physiquement et logiquement les données personnelles, déterminez quels services de AWS stockage prennent en charge les politiques de contrôle d'accès détaillées dans AWS Identity and Access Management (IAM).

La politique basée sur l'identité suivante permet de récupérer uniquement les `LastLoggedIn` attributs`UserID`,`SignUpTime`, et d'une table Amazon DynamoDB nommée. `Users` Par exemple, vous pouvez associer cette politique à un rôle de support client au lieu de donner à ce rôle l'accès à l'ensemble de données personnel complet. Pour plus d'informations sur la manière dont cette politique peut contribuer à protéger la confidentialité et les données personnelles au sein de votre organisation, consultez Services et fonctionnalités AWS qui aident à segmenter les données ce guide.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan",
            "dynamodb:TransactGetItems"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynanamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

Restreindre les modifications apportées aux configurations VPC

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Après avoir conçu et déployé l' AWS infrastructure qui répond à vos besoins en matière de transfert de données transfrontalier, y compris les flux de données réseau, vous souhaiterez peut-être empêcher toute modification. La politique de contrôle des services suivante permet d'éviter toute dérive ou modification involontaire de la configuration du VPC. Il refuse les nouvelles connexions de passerelle Internet, les connexions de peering VPC, les pièces jointes de passerelle de transit et les nouvelles connexions VPN. Pour plus d'informations sur la manière dont cette politique peut contribuer à protéger la confidentialité et les données personnelles au sein de votre organisation, consultez AWS Transit Gateway ce guide.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:AttachEgressOnlyInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
```

```
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Exiger une attestation pour utiliser une AWS KMS clé

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

La politique de clé suivante AWS Key Management Service (AWS KMS) autorise les instances de AWS Nitro Enclave à utiliser une clé KMS uniquement si le document d'attestation de l'enclave figurant dans la demande correspond aux mesures indiquées dans la déclaration de condition. Cette politique autorise uniquement les enclaves fiables à déchiffrer les données. Pour plus d'informations sur la manière dont cette politique peut contribuer à protéger la confidentialité et les données personnelles au sein de votre organisation, consultez AWS Enclaves Nitro ce guide. Pour obtenir la liste complète des clés de AWS KMS condition pouvant être utilisées dans les politiques clés et dans les politiques AWS Identity and Access Management (IAM), consultez la section Clés de condition pour AWS KMS.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
```

```
            "kms:GenerateRandom"
         ],
         "Resource": "*",
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
               "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
               "kms:RecipientAttestation:PCR2":
 "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
               "kms:RecipientAttestation:PCR3":
 "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
               "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
               "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
         }
      }
   ]
}
```

Ressources

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

AWS Conseils prescriptifs

- AWS Architecture de référence de sécurité (AWS SRA)

AWS documentation

- Protection des données (AWS Well-Architected Framework)
- Classification des données (AWS livre blanc)
- Amazon Web Services : risques et conformité (AWS livre blanc)
- Architectures hybrides pour répondre aux exigences en matière de traitement des données personnelles (AWS livre blanc)
- Gérer la conformité au RGPD sur AWS (AWS livre blanc)
- Création d'un périmètre de données sur AWS (AWS livre blanc)
- AWS Documentation de sécurité

Autres AWS ressources

- AWS Programmes de conformité
- AWS Modèle de responsabilité partagée
- Questions fréquentes (FAQ) relatives à la confidentialité des données
- AWS Services d'assurance de sécurité
- AWS Engagement en faveur de la souveraineté numérique : un contrôle sans compromis (article de AWS blog)
- AWS Formation en matière de sécurité

Collaborateurs

Nous aimerions avoir de vos nouvelles. Veuillez nous faire part de vos commentaires sur le AWS PRA en répondant à un court sondage.

Ce guide a été rédigé par l'équipe des services d'assurance AWS de sécurité. Pour obtenir de l'aide concernant la mise en œuvre des recommandations de ce guide et l'opérationnalisation de vos charges de travail, contactez l'équipe des services d'assurance AWS sécurité.

Principaux auteurs

- Daniel Nieters, consultant AWS principal en matière de confidentialité
- Amber Welch, consultante AWS principale en protection de la vie privée
- Robert Carter, directeur du programme AWS technique

Collaborateurs

- Avik Mukherjee, consultant principal en sécurité AWS
- David Bounds, architecte de solutions AWS senior
- Jeff Lombardo, architecte AWS principal des solutions de sécurité
- Ram Ramani, architecte AWS principal des solutions de sécurité
- Vanessa Jacobs, consultante AWS principale en sécurité

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Mises à jour importantes	Nous avons apporté des mises à jour importantes tout au long.	26 mars 2024
Publication initiale	—	2 octobre 2023

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. Pour suggérer des entrées, veuillez utiliser le lien Faire un commentaire à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (RDSAmazon) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle locale vers Oracle sur une EC2 instance du AWS Cloud.
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer un Microsoft Hyper-V application à AWS.
- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACID

Voir atomicité, consistance, isolation, durabilité.

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration active-passive.

migration active-passive

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

SQLFonction qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent `SUM` et`MAX`.

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour le processus de découverte et d'analyse du portefeuille et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter Qu'est-ce que l'intelligence artificielle ?

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur son AIOps utilisation dans la stratégie de AWS migration, consultez le guide d'intégration des opérations.

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, consistance, isolation, durabilité () ACID

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès basé sur les attributs () ABAC

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez ABAC AWS la documentation AWS Identity and Access Management (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Un emplacement distinct au sein d'un Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS CAForganise les directives en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer

l'organisation à une adoption réussie du cloud. Pour plus d'informations, consultez le AWS CAFsite Web et le AWS CAFlivre blanc.

AWS Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS WQFest inclus avec AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

Un bot destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les API appels suspects et les actions similaires. Pour plus d'informations, veuillez consulter Data in a behavior graph dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi endianité.

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, appelés « bots malveillants », sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de robots infectés par des logiciels malveillants et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, c'est un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur Implementation break-glass procedures dans le guide Well-Architected AWS .

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCoE

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

modifier la capture de données (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez l'utiliser à diverses CDC fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser AWS Fault Injection Service (AWS FIS) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données localement, avant que la cible ne les Service AWS reçoive.

Centre d'excellence du cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, consultez les CCoEarticles du blog sur la stratégie AWS Cloud d'entreprise.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie informatique de pointe.

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section Création de votre modèle d'exploitation cloud.

étapes d'adoption du cloud

Les quatre phases que les entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir uneCCoE, établir un modèle d'exploitation)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Consultez la base de données de gestion des configurations.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub or Bitbucket Cloud. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, AWS Panorama propose des appareils qui ajoutent des CV aux réseaux de caméras locaux, et Amazon SageMaker fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

base de données de gestion de configuration (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs configurations. Vous utilisez généralement les données issues de la phase CMDB de découverte et d'analyse du portefeuille lors de la migration.

pack de conformité

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un YAML modèle. Pour plus d'informations, consultez la section Packs de conformité dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes source, de génération, de test, intermédiaire et de production du processus de publication du logiciel. CI/CD is commonly described as a pipeline. CI/CDpeut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du AWS Well-Architected Framework. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir Création d'un périmètre de données sur AWS.

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir langage de définition de base de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de

la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte AWS membre pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations .

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir environnement.

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique Contrôles de détection dans Implementing security controls on AWS.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSMétend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un schéma en étoile, table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un sinistre. Pour plus d'informations, consultez Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur la façon dont vous pouvez utiliser le design piloté par domaine avec le motif Strangler Fig, voir Modernisation de l'ancienne version de Microsoft. ASP NET(ASMX) des services Web de manière incrémentielle à l'aide de conteneurs et d'Amazon API Gateway.

DR

Consultez la section Reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower

pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au cloud computing, l'informatique de pointe peut réduire la latence des communications et améliorer le temps de réponse.

échange de données informatisé () EDI

L'échange automatique de documents commerciaux entre les organisations. Pour plus d'informations, voir Qu'est-ce que l'échange de données informatisé ?

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger dans un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de VPC terminaison d'interface. Pour plus d'informations, consultez la section Créer un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (AmazonVPC).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité et la gestion de projet) pour une entreprise. MES

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes dans la documentation AWS Key Management Service (AWS KMS).

environment

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un pipeline CI/CD, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des

environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les grands enjeux en matière de AWS CAF sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le guide d'implémentation du programme.

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données () EDA

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. EDAest réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un schéma en étoile. Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des

charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Ceci est généralement exprimé sous la forme d'un score numérique qui peut être calculé à l'aide de diverses techniques, telles que les explications additives de Shapley (SHAP) et les dégradés intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec :AWS.

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en « 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

invitation en quelques coups

Fournir un LLMpetit nombre d'exemples illustrant la tâche et le résultat souhaité avant de lui demander d'effectuer une tâche similaire. Cette technique est une application de l'apprentissage contextuel, dans le cadre de laquelle les modèles apprennent à partir d'exemples (prises de vue) intégrés dans des instructions. Les instructions en quelques étapes peuvent être efficaces pour les tâches qui nécessitent un formatage, un raisonnement ou des connaissances de domaine spécifiques. Voir également l'invite Zero-Shot.

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé () FGAC

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données par le biais de la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

FM

Voir le modèle de fondation.

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'est entraîné sur d'énormes ensembles de données généralisées et non étiquetées. FMssont capables d'effectuer une grande variété de tâches générales, telles que comprendre le langage, générer du texte et des images et converser en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

G

IA générative

Sous-ensemble de modèles d'IA qui ont été entraînés sur de grandes quantités de données et qui peuvent utiliser une simple invite textuelle pour créer de nouveaux contenus et artefacts, tels que des images, des vidéos, du texte et du son. Pour plus d'informations, consultez Qu'est-ce que l'IA générative.

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le flux de travail basé sur les troncs est l'approche moderne préférée.

image dorée

Un instantané d'un système ou d'un logiciel utilisé comme modèle pour déployer de nouvelles instances de ce système ou logiciel. Par exemple, dans le secteur de la fabrication, une image dorée peut être utilisée pour fournir des logiciels sur plusieurs appareils et contribue à améliorer la vitesse, l'évolutivité et la productivité des opérations de fabrication des appareils.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée brownfield. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Ils sont mis en œuvre à l'aide de politiques de contrôle des services et de limites IAM d'autorisations. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration

hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. AWS propose AWS SCT qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'apprentissage automatique. Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

Politique attachée à un ou plusieurs IAM principaux qui définit leurs autorisations au sein de l' AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne CPU de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIoT

Voir Internet industriel des objets.

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures mutables. Pour plus d'informations, consultez les meilleures pratiques de déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

entrant (entrée) VPC

Dans une architecture AWS multi-comptes, une architecture VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions

entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Terme introduit par Klaus Schwab en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, voir Élaborer une stratégie de transformation numérique industrielle pour l'Internet des objets (IIoT).

inspection VPC

Dans une architecture AWS multi-comptes, système centralisé VPC qui gère les inspections du trafic réseau entre VPCs (identiques ou différents Régions AWS), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte

réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section Qu'est-ce que l'IoT ?.

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

IoT

Voir Internet des objets.

bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. ITILconstitue la base deITSM.

Gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux ITSM outils, consultez le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes () LBAC

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection

entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

grand modèle de langage (LLM)

Un modèle d'intelligence artificielle basé sur le deep learning qui est préentraîné sur une grande quantité de données. An LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir Que sont LLMs.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, consultez la section Appliquer les autorisations du moindre privilège dans la IAM documentation.

lift and shift

Voir 7 Rs.

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi endianité.

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter Machine Learning.

branche principale

Voir succursale.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

Services AWS pour lequel AWS fonctionnent la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

MAP

Voir Migration Acceleration Program.

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore au fur et à mesure de son fonctionnement. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

Tous, à l' Comptes AWS exception du compte de gestion, qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

MES

Voir le système d'exécution de la fabrication.

Transport de télémétrie en file d'attente de messages () MQTT

Protocole de communication léger machine-to-machine (M2M), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie en utilisant Lightweight. APIs Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section Implémentation de microservices sur AWS.

Migration Acceleration Program (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir une base opérationnelle solide pour passer au cloud, et pour aider à compenser le coût initial des migrations. MAPinclut une méthodologie de migration pour exécuter les migrations existantes de manière méthodique et un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la stratégie de migration AWS.

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement les opérations, les analystes commerciaux et les propriétaires, les ingénieurs de migration, les développeurs et les DevOps professionnels travaillant dans le cadre de sprints. Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 avec le service de migration AWS d'applications.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le. AWS Cloud MPAfournit une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, TCO comparaisons, analyse des coûts de migration) ainsi que la planification de la migration (analyse et collecte des données des applications, regroupement des applications, hiérarchisation des migrations et planification des vagues). L'MPAoutil (nécessite une connexion) est disponible gratuitement pour tous les AWS consultants et consultants APN partenaires.

Évaluation de l'état de préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une entreprise au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du AWS CAF. Pour plus d'informations, veuillez consulter le guide de préparation à la migration. MRAest la première phase de la stratégie de AWS migration.

stratégie de migration

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. Pour plus d'informations, reportez-vous aux 7 R de ce glossaire et à Mobiliser votre organisation pour accélérer les migrations à grande échelle.

ML

Voir apprentissage automatique.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez la section Stratégie de modernisation des applications dans le AWS Cloud.

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le AWS Cloud.

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter Decomposing monoliths into microservices.

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation d'une infrastructure immuable comme meilleure pratique.

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Consultez la section Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

OPC-États-Unis

Voir Open Process Communications - Architecture unifiée.

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

accord au niveau opérationnel () OLA

Un accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de soutenir un accord de niveau de service (). SLA

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, à évaluer, à prévenir ou à réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de l'industrie 4.0.

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le guide d'intégration des opérations.

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. OCMaide les organisations à se préparer et à passer à de nouveaux systèmes et stratégies en accélérant l'adoption des changements, en résolvant les problèmes de transition et en suscitant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, consultez le OCMguide.

contrôle d'accès à l'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). OACprend en charge tous les compartiments S3 Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les `DELETE` requêtes dynamiques `PUT` adressées au compartiment S3.

identité d'accès à l'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisezOAI, CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés ne peuvent accéder au contenu d'un compartiment S3 que par le biais d'une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus granulaire et amélioré.

ORR

Voir l'examen de l'état de préparation opérationnelle.

DE

Voir technologie opérationnelle.

sortant (sortie) VPC

Dans une architecture AWS multi-comptes, VPC qui gère les connexions réseau initiées depuis une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

P

limite des autorisations

Une politique de IAM gestion attachée IAM aux principaux pour définir les autorisations maximales que l'utilisateur ou le rôle peut avoir. Pour plus d'informations, consultez la section Limites des autorisations dans la IAM documentation.

informations personnellement identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. PIILes exemples incluent les noms, les adresses et les coordonnées.

PII

Voir les informations personnelles identifiables.

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations

maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter Evaluating migration readiness.

predicate

Une condition de requête qui renvoie `true` ou`false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

Entité capable d'effectuer AWS des actions et d'accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS, un IAM rôle ou un utilisateur. Pour plus d'informations, consultez les termes et concepts de Principal in Roles dans la IAM documentation.

confidentialité dès la conception

Une approche d'ingénierie système qui prend en compte la confidentialité tout au long du processus de développement.

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux DNS requêtes relatives à un domaine et à ses sous-domaines au sein d'un ou de plusieurs VPCs domaines. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

chaînage rapide

Utiliser le résultat d'une LLMinvite comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un environnement basé sur des microservices MES, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données SQL relationnelle.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

RACImatrice

Voir responsable, responsable, consulté, informé (RACI).

RAG

Voir Retrieval Augmented Generation.

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

RASCImatrice

Voir responsable, responsable, consulté, informé (RACI).

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir 7 Rs.

objectif du point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir 7 Rs.

Région

Un ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir 7 Rs.

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. La haute disponibilité et la reprise après sinistre sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez la section AWS Cloud Résilience.

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, responsable, consultée, informée (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée RASCImatrice, et si vous l'excluez, elle est appelée RACImatrice.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique Responsive controls dans Implementing security controls on AWS.

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération () RAG

Technologie d'intelligence artificielle générative dans laquelle un système LLMfait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données d'entraînement avant de générer une réponse. Par exemple, un RAG modèle peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, reportez-vous à la section Qu'est-ce que c'est RAG.

rotation

Processus de mise à jour périodique d'un secret pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

L'utilisation d'SQLexpressions simples et flexibles qui ont défini des règles d'accès. RCACconsiste en des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif en matière de temps de rétablissement.

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML2,0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter

AWS Management Console ou appeler les AWS API opérations sans que vous ayez à créer un compte utilisateur IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML basée sur la version 2.0, consultez la section À propos de la fédération SAML basée sur la version 2.0 dans la documentation. IAM

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, voir Que contient le secret d'un Secrets Manager ? dans la documentation de Secrets Manager.

sécurité dès la conception

Une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : préventifs, détectifs, réactifs et proactifs.

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui combinent des systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un SIEM système collecte, surveille et analyse les

données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité et de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe VPC de sécurité, l'application de correctifs à une EC2 instance Amazon ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par celui Service AWS qui les reçoit.

politique de contrôle des services (SCP)

Politique qui propose un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPsdéfinissez des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

point de terminaison du service

Le URL point d'entrée d'un Service AWS. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique Service AWS endpoints dans Références générales AWS.

accord de niveau de service () SLA

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service () SLI

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service () SLO

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de niveau de service.

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Consultez les informations de sécurité et le système de gestion des événements.

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, consultez la section Approche progressive de la modernisation des applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus

petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour un exemple de la façon d'appliquer ce modèle, voir Modernisation de l'ancienne version de MicrosoftASP.NET(ASMX) des services Web de manière incrémentielle à l'aide de conteneurs et d'Amazon API Gateway.

sous-réseau

Une série d'adresses IP dans votreVPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer ces tests.

invite du système

Technique permettant de fournir un contexte, des instructions ou des directives à un LLMhomme pour orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

T

balises

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources.

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir environnement.

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, voir Qu'est-ce qu'une passerelle de transit dans la AWS Transit Gateway documentation.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La

branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données. Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir environnement.

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

VPCpeering

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, consultez What is VPC peering dans la VPC documentation Amazon.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

SQLFonction qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le

calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

WORM

Voir écrire une fois, lire plusieurs.

WQF

Voir le cadre AWS de qualification de la charge de travail.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire, mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une vulnérabilité de type « jour zéro ».

vulnérabilité de type « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

invite Zero-Shot

Fournir LLMdes instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. LLMIl doit utiliser ses connaissances pré-entraînées pour effectuer la tâche. L'efficacité de l'invite zéro dépend de la complexité de la tâche et de la qualité de l'invite. Voir également les instructions en quelques clics.

application zombie

Application dont l'utilisation moyenne de CPU la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

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.