AWS Architecture de référence de sécurité (AWS SRA) : architecture de base

AWS Conseils prescriptifs

AWS Conseils prescriptifs: AWS Architecture de référence de sécurité (AWS SRA) : architecture de base

Table of Contents

AWS Architecture de référence de sécurité (AWS SRA) : architecture de base

Équipe chargée de la sécurité des services mondiaux, Amazon Web Services (contributeurs)

Décembre 2025 (historique du document)

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

L'architecture de référence de sécurité (AWS SRA AWS) d'Amazon Web Services () est un ensemble global de directives pour le déploiement de l'ensemble des services de AWS sécurité dans un environnement multi-comptes. Utilisez-le pour concevoir, mettre en œuvre et gérer les services AWS de sécurité afin qu'ils soient conformes aux pratiques AWS recommandées. Les recommandations s'articulent autour d'une architecture à page unique qui inclut les services de AWS sécurité : comment ils contribuent à atteindre les objectifs de sécurité, où ils peuvent être déployés et gérés au mieux dans le vôtre Comptes AWS, et comment ils interagissent avec les autres services de sécurité. Ces directives architecturales générales complètent les recommandations détaillées spécifiques aux services, telles que celles disponibles sur le site Web de documentation AWS de sécurité.

L'architecture et les recommandations qui l'accompagnent sont basées sur nos expériences collectives avec les AWS entreprises clientes. Ce document est une référence, un ensemble complet de directives Services AWS à utiliser pour sécuriser un environnement particulier. Les modèles de solution du référentiel de code AWS SRA ont été conçus pour l'architecture spécifique illustrée dans cette référence. Chaque client aura des exigences différentes. Par conséquent, la conception de votre AWS environnement peut différer des exemples fournis ici. Vous devrez modifier et adapter ces recommandations en fonction de votre environnement individuel et de vos besoins en matière de sécurité. Tout au long du document, le cas échéant, nous suggérons des options pour les scénarios alternatifs fréquemment utilisés.

Le AWS SRA est un ensemble de directives évolutives et est mis à jour périodiquement en fonction des nouveaux services et fonctionnalités, des commentaires des clients et de l'évolution constante du paysage des menaces. Chaque mise à jour inclura la date de révision et le journal des modifications associé.

Bien que nous nous basions sur un schéma d'une page comme base, l'architecture va bien au-delà d'un simple schéma fonctionnel et doit être construite sur une base bien structurée de principes fondamentaux et de principes de sécurité. Vous pouvez utiliser ce document de deux manières : comme récit ou comme référence. Les sujets sont organisés sous forme d'histoire, afin que vous puissiez les lire du début (conseils de sécurité fondamentaux) à la fin (discussion sur des exemples de code que vous pouvez implémenter). Vous pouvez également parcourir le document pour vous concentrer sur les principes de sécurité, les services, les types de comptes, les conseils et les exemples les plus adaptés à vos besoins.

Ce document comprend les sections suivantes et une annexe :

- À propos de la bibliothèque AWS SRA fournit un aperçu des conseils techniques et du code inclus dans la collection de publications de la AWS SRA.
- La valeur du AWS SRA décrit les motivations qui ont motivé la création du AWS SRA, décrit comment vous pouvez l'utiliser pour améliorer votre sécurité et répertorie les principaux points à retenir.
- Security Foundations passe en revue le AWS Cloud Adoption Framework (AWS CAF), le AWS Well-Architected Framework et AWS le Shared Responsibility Model, et met en évidence les éléments particulièrement pertinents pour le SRA. AWS
- AWS Organizations, accounts, and IAM guardrails présente le AWS Organizations service, décrit les fonctionnalités de sécurité de base et les garde-fous, et donne un aperçu de la stratégie multi-comptes que nous recommandons.
- L'architecture AWS de référence de sécurité est un schéma d'architecture d'une page qui montre Comptes AWS les fonctionnalités ainsi que les services et fonctionnalités de sécurité généralement disponibles.
- L'intelligence artificielle et le machine learning (AI/ML) au service de la sécurité décrivent comment différents acteurs Services AWS utilisent l'intelligence artificielle et l'apprentissage automatique (AI/ML) en arrière-plan pour vous aider à atteindre des objectifs de sécurité spécifiques. Vous pouvez les inclure Services AWS dans votre conception pour tirer parti des fonctionnalités de sécurité avancées.
- Création de votre architecture de sécurité – Une approche progressive fournit des conseils sur la manière de créer votre propre architecture de sécurité en six phases itératives, sur la base de la référence fournie par la AWS SRA.

- AWS La liste des meilleures pratiques de la SRA résume les recommandations abordées tout au long du guide dans une liste de contrôle que vous pouvez suivre lors de la création de votre version de l'architecture de sécurité.
- Les ressources IAM présentent un résumé et un ensemble de conseils Gestion des identités et des accès AWS (IAM) importants pour votre architecture de sécurité.
- Le référentiel de code pour les exemples AWS SRA fournit une vue d'ensemble du GitHub référentiel associé qui aidera les développeurs et les ingénieurs à déployer certains des conseils et modèles d'architecture présentés dans ce document. Vous pouvez déployer les exemples en utilisant AWS CloudFormation ou Terraform by. HashiCorp Ils prennent en charge à la fois les environnements AWS Control Tower et les AWS Control Tower environnements non –.

L'annexe contient une liste des différents services de AWS sécurité, d'identité et de conformité, ainsi que des liens vers des informations supplémentaires sur chaque service. La section Historique du document fournit un journal des modifications pour le suivi des versions de ce document. Vous pouvez également vous abonner à un flux RSS pour recevoir les notifications de modification.

À propos de la AWS bibliothèque SRA

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Ce guide fait partie d'une bibliothèque qui fournit des plans architecturaux et des conseils techniques pour la conception et la construction d'architectures de sécurité. AWS La bibliothèque comprend un code d'implémentation (bibliothèque de code AWS SRA), un outil de validation (SRA Verify) et deux catégories complémentaires de guides qui couvrent l'architecture de base et les architectures approfondies.

AWS SRA — architecture de base (ce guide)

Ce guide constitue la base de l'architecture AWS de sécurité recommandée. C'est le point de départ qui s'applique à toutes les organisations, quels que soient leur secteur d'activité, leur type d'application ou toute autre considération. Cette base vous permet de créer une architecture solide et évolutive et de créer une base de sécurité AWS multi-comptes solide qui évolue en toute sécurité au fur AWS et à mesure de la croissance de votre entreprise.

AWS SRA : architectures de plongée approfondie

Le guide de l'architecture de base du AWS SRA est complété par des publications supplémentaires qui fournissent des modèles architecturaux adaptés à des capacités de sécurité spécifiques, à des types d'applications et à des exigences réglementaires ou de conformité. Ces modèles étendent l'architecture de base et doivent être utilisés conjointement avec le guide d'architecture de base AWS SRA.

Les guides suivants fournissent des modèles architecturaux adaptés à des fonctionnalités de sécurité spécifiques :

- AWS SRA — Identity Management fournit des conseils sur la manière de mettre en œuvre une solution de gestion des identités et des accès évolutive, robuste et centralisée sur AWS.
- AWS SRA — Perimeter Security traite des modèles d'architecture et de Services AWS la mise en œuvre de la sécurité périphérique dans un compte central ou dans des comptes individuels.

- AWS SRA — cyber forensics décrit comment configurer un compte AWS Forensics comme point de départ pour développer les capacités de criminalistique de votre organisation et améliorer votre préparation à la réponse aux incidents de sécurité (IR).

Les guides suivants fournissent des modèles architecturaux pour des types d'applications spécifiques. Vous souhaiterez peut-être vous concentrer sur ces points après avoir créé votre architecture de sécurité de base :

- AWS SRA — AI security fournit des recommandations en matière d'architecture de sécurité pour la conception et le développement d'applications intégrant des capacités d'IA génératives en utilisant des services d'IA AWS génératifs.
- AWS SRA — IoT fournit des recommandations en matière d'architecture de sécurité pour la conception et le développement d'applications IoT. AWS

En outre, le guide suivant décrit les modèles architecturaux conformes à des cadres réglementaires ou de conformité spécifiques :

- AWS L'architecture de référence de confidentialité (AWS PRA) fournit une architecture de sécurité pour les applications qui traitent des données personnelles et doivent respecter les exigences générales de conformité en matière de confidentialité, telles que le règlement général sur la protection des données (RGPD), la loi californienne sur la protection de la vie privée des consommateurs (CCPA) ou la loi générale brésilienne sur la protection des données (LRGPD). La AWS PRA fournit un ensemble de directives spécifiques à la conception et à la configuration des contrôles de confidentialité dans Services AWS.

Nous vous recommandons de commencer par le guide de l'architecture de base AWS SRA pour comprendre l'architecture de base, puis de consulter les guides complémentaires pour tirer parti des fonctionnalités et des implémentations avancées. Pour plus d'informations sur cet ensemble de contenus, consultez Architecture AWS de référence de sécurité.

> **Schémas d'architecture**
>
> Pour personnaliser les diagrammes d'architecture de référence de la bibliothèque AWS SRA en fonction des besoins de votre entreprise, vous pouvez télécharger le fichier .zip suivant et en extraire le contenu.

Téléchar

le fichier source du diagramme (PowerPointformat Microsoft)

La valeur du AWS SRA

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

AWS dispose d'un ensemble important (et croissant) de services liés à la sécurité. Les clients ont exprimé leur appréciation pour les informations détaillées disponibles dans la documentation de notre service, nos articles de blog, nos tutoriels, nos sommets et nos conférences. Ils nous disent également qu'ils souhaitent mieux comprendre la situation dans son ensemble et avoir une vision stratégique des services de AWS sécurité. Lorsque nous travaillons avec les clients pour mieux comprendre leurs besoins, trois priorités se dégagent :

- Les clients souhaitent obtenir plus d'informations et des modèles recommandés sur la manière dont ils peuvent déployer, configurer et exploiter les services AWS de sécurité de manière globale. Dans quels comptes et pour quels objectifs de sécurité les services doivent-ils être déployés et gérés ? Existe-t-il un compte de sécurité sur lequel tous les services ou la plupart des services devraient fonctionner ? Comment le choix de l'emplacement (unité organisationnelle ou Compte AWS) influence-t-il les objectifs de sécurité ? Quels compromis (considérations de conception) les clients doivent-ils prendre en compte ?
- Les clients souhaitent voir différentes perspectives pour organiser de manière logique les nombreux services de AWS sécurité. Au-delà de la fonction principale de chaque service (par exemple, les services d'identité ou les services de journalisation), ces points de vue alternatifs aident les clients à planifier, concevoir et mettre en œuvre leur architecture de sécurité. Un exemple présenté plus loin dans ce document regroupe les services en fonction des couches de protection alignées sur la structure recommandée de votre AWS environnement.
- Les clients recherchent des conseils et des exemples pour intégrer les services de sécurité de la manière la plus efficace possible. Par exemple, comment devraient-ils s'aligner et se connecter au mieux AWS Config aux autres services pour effectuer le gros du travail dans les pipelines d'audit et de surveillance automatisés ? Les clients demandent des conseils sur la manière dont chaque service AWS de sécurité s'appuie sur les autres services de sécurité ou les prend en charge.

Nous abordons chacune de ces questions dans le AWS SRA. La première priorité de la liste (où vont les choses) est au centre du schéma d'architecture principal et des discussions qui l'accompagnent dans ce document. Nous fournissons une AWS Organizations architecture recommandée et une

account-by-account description des services destinés à chacun. Pour commencer avec la deuxième priorité de la liste (comment envisager l'ensemble complet des services de sécurité), lisez la section Appliquer les services de sécurité dans l'ensemble de votre AWS organisation. Cette section décrit un moyen de regrouper les services de sécurité en fonction de la structure des éléments de votre AWS organisation. En outre, ces mêmes idées se reflètent dans la discussion sur le compte d'application, qui met en évidence la manière dont les services de sécurité peuvent être gérés de manière à se concentrer sur certaines couches du compte : les instances Amazon Elastic Compute Cloud (Amazon EC2), les réseaux Amazon Virtual Private Cloud (Amazon VPC) et le compte au sens large. Enfin, la troisième priorité (intégration des services) est reflétée tout au long du guide, en particulier dans la discussion sur les services individuels dans les guides détaillés de la bibliothèque AWS SRA et dans le code du référentiel de codes SRA. AWS

Comment utiliser le AWS SRA

Il existe différentes manières d'utiliser le AWS SRA en fonction de l'état d'avancement de votre parcours d'adoption du cloud. Voici une liste des moyens de tirer le meilleur parti des actifs de la AWS SRA (schéma d'architecture, conseils écrits et exemples de code).

- Définissez l'état cible de votre propre architecture de sécurité.

  Que vous commenciez tout juste votre AWS Cloud parcours (création de votre premier ensemble de comptes) ou que vous envisagiez d'améliorer un AWS environnement établi, la AWS SRA est le point de départ idéal pour créer votre architecture de sécurité. Commencez par une base complète de structure de compte et de services de sécurité, puis ajustez en fonction de votre infrastructure technologique, de vos compétences, de vos objectifs de sécurité et de vos exigences de conformité spécifiques. Si vous savez que vous allez créer et lancer davantage de charges de travail, vous pouvez utiliser votre version personnalisée de la AWS SRA comme base pour l'architecture de référence de sécurité de votre organisation. Pour savoir comment atteindre l'état cible décrit par la AWS SRA, consultez la section Création de votre architecture de sécurité — Une approche progressive.
- Passez en revue (et révisez) les conceptions et les fonctionnalités que vous avez déjà mises en œuvre.

  Si vous avez déjà une conception et une mise en œuvre de la sécurité, il vaut la peine de prendre le temps de comparer ce que vous avez à la AWS SRA. Le AWS SRA est conçu pour être complet et fournit une base de diagnostic pour évaluer votre propre sécurité. Lorsque vos conceptions de sécurité sont conformes à la AWS SRA, vous pouvez être plus sûr de suivre les meilleures

pratiques lors de l'utilisation Services AWS. Si vos conceptions de sécurité divergent ou ne sont pas conformes aux directives de la AWS SRA, cela ne signifie pas nécessairement que vous faites quelque chose de mal. Cette observation vous donne plutôt l'occasion de revoir votre processus de décision. Il existe des raisons commerciales et technologiques légitimes pour lesquelles vous pourriez vous écarter des meilleures pratiques de la AWS SRA. Peut-être que vos exigences spécifiques en matière de conformité, de réglementation ou de sécurité organisationnelle nécessitent des configurations de service spécifiques. Ou, au lieu de l'utiliser Services AWS, vous pouvez avoir une préférence de fonctionnalité pour un produit AWS Partner Network ou une application personnalisée que vous avez créée et gérée. Parfois, au cours de cet examen, vous découvrirez peut-être que vos décisions précédentes ont été prises en fonction de technologies, de AWS fonctionnalités ou de contraintes commerciales plus anciennes qui ne s'appliquent plus. C'est une bonne occasion de passer en revue les mises à jour, de les classer par ordre de priorité et de les ajouter à l'endroit approprié de votre carnet de commandes d'ingénierie. Quoi que vous découvriez en évaluant votre architecture de sécurité à la lumière de la AWS SRA, il vous sera utile de documenter cette analyse. Le fait de disposer de cet historique des décisions et de leurs justifications peut aider à éclairer et à prioriser les décisions futures.

- Démarrez la mise en œuvre de votre propre architecture de sécurité.

  Les modules d'infrastructure sous forme de code (IaC) AWS SRA constituent un moyen rapide et fiable de commencer à créer et à mettre en œuvre votre architecture de sécurité. Ces modules sont décrits plus en détail dans la section du référentiel de code et dans le GitHub référentiel public. Ils permettent non seulement aux ingénieurs de s'appuyer sur des exemples de haute qualité des modèles présentés dans les directives de la AWS SRA, mais ils intègrent également les contrôles de sécurité recommandés tels que les politiques de mot de passe IAM, l'accès public aux comptes de blocage Amazon Simple Storage Service (Amazon S3), le chiffrement Amazon Elastic Block Store (EC2 Amazon EBS) par défaut d'Amazon, et l'intégration AWS Control Tower afin que les contrôles soient appliqués ou supprimés au fur et à mesure que les nouveaux sont intégrés ou mis hors service. Comptes AWS

- En savoir plus sur les services et fonctionnalités de AWS sécurité.

  Les conseils et les discussions au sein de la AWS SRA incluent des fonctionnalités importantes ainsi que des considérations relatives au déploiement et à la gestion de la AWS sécurité individuelle et des services liés à la sécurité. L'une des caractéristiques du AWS SRA est qu'il fournit une introduction de haut niveau à l'étendue des services de AWS sécurité et à la manière dont ils fonctionnent ensemble dans un environnement multi-comptes. Cela complète l'étude approfondie des fonctionnalités et de la configuration de chaque service trouvée dans

d'autres sources. La discussion sur la manière dont AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) intègre les résultats de sécurité provenant de divers AWS Partner produits Services AWS, voire de vos propres applications, en est un exemple.

- Menez une discussion sur la gouvernance organisationnelle et les responsabilités en matière de sécurité.

  Un élément important de la conception et de la mise en œuvre de toute architecture ou stratégie de sécurité consiste à comprendre qui au sein de votre organisation a quelles responsabilités en matière de sécurité. Par exemple, la question de savoir où agréger et surveiller les résultats de sécurité est liée à la question de savoir quelle équipe sera responsable de cette activité. Tous les résultats de l'organisation sont-ils surveillés par une équipe centrale qui a besoin d'accéder à un compte Security Tooling dédié ? Ou bien les équipes d'application individuelles (ou unités commerciales) sont-elles responsables de certaines activités de surveillance et ont-elles donc besoin d'accéder à certains outils d'alerte et de surveillance ? Autre exemple, si votre organisation dispose d'un groupe qui gère toutes les clés de chiffrement de manière centralisée, cela influencera les personnes autorisées à créer AWS Key Management Service (AWS KMS) les clés et les comptes dans lesquels ces clés seront gérées. Comprendre les caractéristiques de votre organisation (les différentes équipes et responsabilités) vous aidera à adapter le SRA à vos besoins. AWS À l'inverse, la discussion sur l'architecture de sécurité donne parfois lieu à une discussion sur les responsabilités organisationnelles existantes et à la prise en compte des changements potentiels. AWS recommande un processus décisionnel décentralisé dans le cadre duquel les équipes chargées de la charge de travail sont chargées de définir les contrôles de sécurité en fonction de leurs fonctions et exigences en matière de charge de travail. L'objectif d'une équipe de sécurité et de gouvernance centralisée est de créer un système permettant aux responsables de la charge de travail de prendre des décisions éclairées et à toutes les parties d'avoir une visibilité sur la configuration, les résultats et les événements. Le AWS SRA peut être un moyen d'identifier et d'éclairer ces discussions.

Principales directives de mise en œuvre de la AWS SRA

Voici huit points essentiels à retenir de la AWS SRA à prendre en compte lors de la conception et de la mise en œuvre de votre sécurité.

- AWS Organizations et une stratégie multi-comptes appropriée sont des éléments nécessaires de votre architecture de sécurité. La séparation correcte des charges de travail, des équipes et des

fonctions constitue le fondement de la séparation des tâches et des defense-in-depth stratégies. Le guide aborde cette question plus en détail dans une section ultérieure.

- Defense-in-depth est une considération de conception importante lors de la sélection des contrôles de sécurité pour votre organisation. Il vous aide à injecter les contrôles de sécurité appropriés aux différentes couches de la AWS Organizations structure, ce qui permet de minimiser l'impact d'un problème : en cas de problème avec une couche, des contrôles sont en place pour isoler d'autres ressources informatiques précieuses. Le AWS SRA montre comment les différentes Services AWS fonctions varient selon les couches AWS technologiques et comment l'utilisation combinée de ces services peut vous aider à y parvenir defense-in-depth. Ce defense-in-depth concept AWS est discuté plus en détail dans une section ultérieure avec des exemples de conception présentés sous Compte d'application.
- Utilisez la grande variété de composants de sécurité associés à de multiples Services AWS fonctionnalités pour créer une infrastructure cloud robuste et résiliente. Lorsque vous adaptez le AWS SRA à vos besoins particuliers, tenez compte non seulement de la fonction Services AWS et des fonctionnalités principales (par exemple, authentification, chiffrement, surveillance, politique d'autorisation), mais également de la manière dont elles s'intègrent dans la structure de votre architecture. Une section ultérieure du guide décrit le fonctionnement de certains services dans l'ensemble de votre AWS organisation. D'autres services fonctionnent mieux avec un seul compte, et certains sont conçus pour accorder ou refuser l'autorisation à des directeurs individuels. La prise en compte de ces deux points de vue vous aide à élaborer une approche de sécurité à plusieurs niveaux plus flexible.
- Dans la mesure du possible (comme indiqué dans les sections suivantes), utilisez-le pour chaque compte (distribué plutôt Services AWS que centralisé) et créez un ensemble cohérent de garde-fous partagés qui peuvent aider à protéger vos charges de travail contre toute utilisation abusive et à réduire l'impact des événements de sécurité. La AWS SRA utilise AWS Security Hub CSPM (surveillance centralisée des résultats et contrôles de conformité), Amazon GuardDuty (détection des menaces et détection des anomalies), AWS Config (surveillance des ressources et détection des modifications), IAM Access Analyzer (surveillance de l'accès aux ressources), AWS CloudTrail (activité des API du service de journalisation dans votre environnement) et Amazon Macie (classification des données) comme ensemble de Services AWS base à déployer dans tous les domaines. Compte AWS
- Utilisez la fonctionnalité d'administration déléguée de AWS Organizations, lorsqu'elle est prise en charge, comme expliqué plus loin dans la section Administration déléguée du guide. Cela vous permet d'enregistrer un compte de AWS membre en tant qu'administrateur pour les services pris en charge. L'administration déléguée permet aux différentes équipes de votre entreprise d'utiliser

des comptes distincts, en fonction de leurs responsabilités, pour gérer l' Services AWS ensemble de l'environnement. En outre, le recours à un administrateur délégué vous permet de limiter l'accès au compte de gestion et de gérer le surcroît d'autorisations associé AWS Organizations à ce compte.

- Mettez en œuvre une surveillance, une gestion et une gouvernance centralisées au sein de vos AWS organisations. En utilisant Services AWS cette prise en charge de l'agrégation multicompte (et parfois multirégionale), ainsi que des fonctionnalités d'administration déléguée, vous permettez à vos équipes centrales chargées de la sécurité, du réseau et du cloud d'avoir une visibilité et un contrôle étendus sur la configuration de sécurité et la collecte de données appropriées. En outre, les données peuvent être renvoyées aux équipes chargées de la charge de travail pour leur permettre de prendre des décisions de sécurité efficaces plus tôt dans le cycle de vie du développement logiciel (SDLC).
- AWS Control Tower À utiliser pour configurer et gérer votre AWS environnement multi-comptes grâce à la mise en œuvre de contrôles de sécurité prédéfinis pour démarrer la création de votre architecture de référence de sécurité. AWS Control Tower fournit un plan pour assurer la gestion des identités, l'accès fédéré aux comptes, la journalisation centralisée et des flux de travail définis pour le provisionnement de comptes supplémentaires. Vous pouvez ensuite utiliser la solution Customizations for AWS Control Tower (CfCT) pour définir les comptes gérés par des contrôles de sécurité, AWS Control Tower des configurations de service et une gouvernance supplémentaires, comme le montre le référentiel de code AWS SRA. La fonctionnalité Account Factory fournit automatiquement aux nouveaux comptes des modèles configurables basés sur une configuration de compte approuvée afin de standardiser les comptes au sein de vos AWS organisations. Vous pouvez également étendre la gouvernance à une personne existante en l' Compte AWS inscrivant dans une unité organisationnelle (UO) déjà gouvernée par AWS Control Tower.
- Les exemples de code AWS SRA montrent comment automatiser la mise en œuvre de modèles dans le guide AWS SRA en utilisant l'infrastructure en tant que code (IaC). En codifiant les modèles, vous pouvez traiter IaC comme les autres applications de votre organisation et automatiser les tests avant de déployer le code. IaC contribue également à garantir la cohérence et la répétabilité en déployant des garde-fous dans plusieurs environnements (par exemple, SDLC ou spécifiques à une région). Les exemples de code SRA peuvent être déployés dans un environnement AWS Organizations multi-comptes avec ou sans. AWS Control Tower Les solutions requises dans ce référentiel AWS Control Tower ont été déployées et testées dans un AWS Control Tower environnement à l'aide de AWS CloudFormation et de personnalisations pour AWS Control Tower (CfCT). Les solutions qui n'en nécessitent pas AWS Control Tower ont été testées dans un AWS Organizations environnement à l'aide de AWS CloudFormation. Si vous ne l'utilisez

pas AWS Control Tower, vous pouvez utiliser la solution de déploiement AWS Organizations basée.

Bases de la sécurité

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le AWS SRA repose sur trois piliers de AWS sécurité : le AWS Cloud Adoption Framework (AWS CAF), AWS Well-Architected et le Shared Responsibility Model. AWS

AWS Les services professionnels ont créé la AWS CAF pour aider les entreprises à concevoir et à suivre une voie accélérée vers une adoption réussie du cloud. Les conseils et les meilleures pratiques fournis par le framework vous aident à élaborer une approche globale du cloud computing au sein de votre entreprise et tout au long de votre cycle de vie informatique. La AWS CAF organise l'orientation en six domaines d'intérêt, appelés perspectives. Chaque point de vue couvre des responsabilités distinctes détenues ou gérées par des parties prenantes liées sur le plan fonctionnel. En général, les perspectives commerciales, humaines et de gouvernance se concentrent sur les capacités commerciales, tandis que les perspectives liées à la plate-forme, à la sécurité et aux opérations se concentrent sur les capacités techniques.

La perspective de sécurité de la AWS CAF vous aide à structurer la sélection et la mise en œuvre des contrôles dans l'ensemble de votre entreprise. Le respect AWS des recommandations actuelles du pilier de sécurité peut vous aider à répondre à vos exigences commerciales et réglementaires.

AWS Well-Architected aide les architectes du cloud à créer une infrastructure sécurisée, performante, résiliente et efficace pour leurs applications et leurs charges de travail. Le cadre repose sur six piliers (excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité) et fournit une approche cohérente permettant aux AWS clients et aux partenaires d'évaluer les architectures et de mettre en œuvre des conceptions évolutives dans le temps. Nous pensons que le fait d’avoir des charges de travail bien structurées augmente considérablement les chances de réussite métier.

Le pilier de sécurité Well-Architected Framework décrit comment tirer parti des technologies cloud pour protéger les données, les systèmes et les actifs de manière à améliorer votre posture de sécurité. Cela vous aidera à répondre à vos exigences commerciales et réglementaires en suivant les AWS recommandations actuelles. Il existe d'autres domaines d'intérêt du Well-Architected Framework qui fournissent plus de contexte pour des domaines spécifiques tels que la gouvernance,

le sans serveur, l'IA/ML et les jeux vidéo. Ces lentilles sont connues sous le nom de AWS lentilles Well-Architected.

La sécurité et la conformité sont une responsabilité partagée entre le client AWS et le client. Ce modèle partagé peut vous aider à alléger votre charge opérationnelle en AWS exploitant, en gérant et en contrôlant les composants, depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles le service fonctionne. Par exemple, vous assumez la responsabilité et la gestion du système d'exploitation client (y compris les mises à jour et les correctifs de sécurité), du logiciel d'application, du chiffrement des données côté serveur, des tables de routage du trafic réseau et de la configuration du pare-feu du groupe de sécurité AWS fourni. Pour les services abstraits tels qu'Amazon S3 et Amazon AWS DynamoDB, il gère la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Vous êtes responsable de la gestion de vos données (y compris les options de chiffrement), de la classification de vos actifs et de l'utilisation des outils IAM pour appliquer les autorisations appropriées. Ce modèle partagé est souvent décrit en disant qu'il AWS est responsable de la sécurité du cloud (c'est-à-dire de la protection de l'infrastructure qui exécute tous les services proposés dans le AWS Cloud), et que vous êtes responsable de la sécurité dans le cloud (telle que déterminée par les AWS Cloud services que vous sélectionnez).

Dans le cadre des directives fournies par ces documents fondamentaux, deux ensembles de concepts sont particulièrement pertinents pour la conception et la compréhension de la AWS SRA : les capacités de sécurité et les principes de conception de sécurité.

Capacités de sécurité

Le point de vue de la sécurité de la AWS CAF décrit neuf fonctionnalités qui vous aident à garantir la confidentialité, l'intégrité et la disponibilité de vos données et de vos charges de travail dans le cloud.

- Gouvernance de la sécurité pour développer et communiquer les rôles, les responsabilités, les politiques, les processus et les procédures de sécurité dans l' AWS environnement de votre entreprise.
- Assurance de sécurité pour surveiller, évaluer, gérer et améliorer l'efficacité de vos programmes de sécurité et de confidentialité.
- Gestion des identités et des accès pour gérer les identités et les autorisations à grande échelle.
- Détection des menaces pour comprendre et identifier les erreurs de configuration, les menaces ou les comportements inattendus potentiels en matière de sécurité.

- Gestion des vulnérabilités pour identifier, classer, corriger et atténuer en permanence les vulnérabilités de sécurité.
- Protection de l'infrastructure pour vérifier que les systèmes et les services de vos charges de travail sont protégés.
- Protection des données pour maintenir la visibilité et le contrôle des données, ainsi que de la manière dont elles sont consultées et utilisées dans votre organisation.
- Sécurité des applications pour aider à détecter et à corriger les failles de sécurité au cours du processus de développement logiciel.
- Réponse aux incidents pour réduire les dommages potentiels en répondant efficacement aux incidents de sécurité.

Principes de conception de la sécurité

Le pilier de sécurité du Well-Architected Framework comprend un ensemble de sept principes de conception qui transforment des domaines de sécurité spécifiques en conseils pratiques pouvant vous aider à renforcer la sécurité de votre charge de travail. Lorsque les capacités de sécurité encadrent la stratégie de sécurité globale, ces principes de Well-Architected Framework décrivent ce que vous pouvez commencer à faire. Ils sont reflétés de manière très délibérée dans cette AWS SRA et se composent des éléments suivants :

- Mettez en place une base d'identité solide – Mettez en œuvre le principe du moindre privilège et appliquez la séparation des tâches avec les autorisations appropriées pour chaque interaction avec vos AWS ressources. Centralisez la gestion des identités et visez l’élimination de la dépendance aux informations d’identification statiques de longue durée.
- Activez la traçabilité – Surveillez, générez des alertes et auditez les actions et les modifications apportées à votre environnement en temps réel. Intégrez la collecte des journaux et des métriques aux systèmes pour effectuer des analyses et prendre des mesures automatiquement.
- Appliquer la sécurité à tous les niveaux – Appliquez une defense-in-depth approche comportant plusieurs contrôles de sécurité. Appliquez plusieurs types de contrôles (par exemple, des contrôles préventifs et de détection) à toutes les couches, y compris la périphérie du réseau, le cloud privé virtuel (VPC), l'équilibrage de charge, les services d'instance et de calcul, le système d'exploitation, la configuration des applications et le code.
- Automatisez les meilleures pratiques de sécurité – Les mécanismes de sécurité automatisés basés sur des logiciels améliorent votre capacité à évoluer en toute sécurité, plus rapidement et

à moindre coût. Créez des architectures sécurisées et implémentez des contrôles définis et gérés sous forme de code dans des modèles contrôlés par version.

- Protégez les données en transit et au repos – Classez vos données selon les niveaux de sensibilité et utilisez des mécanismes tels que le chiffrement, la tokenisation et le contrôle d'accès, le cas échéant.
- Éloignez les personnes des données – Utilisez des mécanismes et des outils pour réduire ou éliminer le besoin d'accéder directement aux données ou de les traiter manuellement. Cette approche permet de réduire les risques de mauvaise manipulation ou de modification ainsi que les erreurs humaines lors d'interventions sur des données sensibles.
- Préparation aux événements de sécurité – Préparez-vous à un incident grâce à une politique et à des processus d'investigation et de gestion des incidents conformes aux exigences de votre organisation. Exécutez des simulations de réponse aux incidents et utilisez des outils d'automatisation pour améliorer votre vitesse de détection, d'investigation et de récupération.

Comment utiliser le AWS SRA avec AWS CAF et Well-Architected Framework AWS

Le AWS CAF, AWS Well-Architected Framework AWS et le SRA sont des frameworks complémentaires qui fonctionnent ensemble pour soutenir vos efforts de migration et de modernisation vers le cloud.

- La AWS CAF s'appuie sur AWS l'expérience et les meilleures pratiques pour vous aider à aligner les valeurs de l'adoption du cloud sur les résultats commerciaux souhaités. Utilisez la AWS CAF pour identifier et hiérarchiser les opportunités de transformation, évaluer et améliorer la préparation au cloud et faire évoluer de manière itérative votre feuille de route de transformation.
- Le AWS Well-Architected Framework AWS fournit des recommandations pour créer une infrastructure sécurisée, performante, résiliente et efficace pour une variété d'applications et de charges de travail répondant aux objectifs de votre entreprise.
- Le AWS SRA vous aide à comprendre comment déployer et gérer les services de sécurité conformément aux recommandations de la AWS CAF et du Well-Architected Framework. AWS

Par exemple, le point de vue de la sécurité de la AWS CAF suggère que vous évaluiez comment gérer de manière centralisée les identités de vos employés et leur authentification dans AWS. Sur la base de ces informations, vous pouvez décider d'utiliser une solution de fournisseur d'identité

d'entreprise (IdP) nouvelle ou existante telle qu'Okta, Active Directory ou Ping Identity à cette fin. Vous suivez les instructions du AWS Well-Architected Framework et décidez d'intégrer votre IdP au afin d'offrir à vos employés une expérience d' AWS IAM Identity Center authentification unique capable de synchroniser leurs adhésions à des groupes et leurs autorisations. Vous passez en revue la recommandation de la AWS SRA visant à activer IAM Identity Center dans le compte de gestion de votre AWS organisation et à l'administrer via un compte d'outils de sécurité utilisé par votre équipe des opérations de sécurité. Cet exemple montre comment la AWS CAF vous aide à prendre des décisions initiales concernant la posture de sécurité que vous souhaitez adopter, le AWS Well-Architected Framework fournit des conseils sur la manière d'évaluer Services AWS les capacités disponibles pour atteindre cet objectif, et la SRA fournit ensuite des recommandations sur AWS la manière de déployer et de gérer les services de sécurité que vous sélectionnez.

Éléments de base de la SRA : AWS Organizations comptes et garde-fous

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

AWS les services de sécurité, leurs contrôles et leurs interactions sont mieux utilisés sur la base d'une stratégie AWS multi-comptes et de garde-fous en matière de gestion des identités et des accès. Ces garde-fous vous permettent de mettre en œuvre le principe du moindre privilège, de la séparation des tâches et de la confidentialité, et vous aident à prendre des décisions concernant les types de contrôles nécessaires, l'endroit où chaque service de sécurité est géré et la manière dont ils peuvent partager les données et les autorisations au sein de la AWS SRA.

An Compte AWS fournit des limites de sécurité, d'accès et de facturation pour vos AWS ressources et vous permet de garantir l'indépendance et l'isolation des ressources. L'utilisation de plusieurs comptes Comptes AWS joue un rôle important dans la manière dont vous répondez à vos exigences en matière de sécurité, comme indiqué dans la Comptes AWS section Avantages de l'utilisation de plusieurs comptes du livre blanc Organiser votre AWS environnement à l'aide de plusieurs comptes. Par exemple, vous pouvez organiser vos charges de travail dans des comptes distincts et des comptes de groupe au sein d'une unité organisationnelle (UO) en fonction de la fonction, des exigences de conformité ou d'un ensemble de contrôles communs au lieu de refléter la structure hiérarchique de votre entreprise. Gardez à l'esprit la sécurité et l'infrastructure pour permettre à votre entreprise de définir des garde-fous communs à mesure que vos charges de travail augmentent. Cette approche fournit des limites et des contrôles robustes entre les charges de travail. La séparation au niveau des comptes, associée à AWS Organizations, est utilisée pour isoler les environnements de production des environnements de développement et de test, ou pour établir une limite logique solide entre les charges de travail qui traitent des données de différentes classifications, telles que la norme de sécurité des données du secteur des cartes de paiement (PCI DSS) ou la Health Insurance Portability and Accountability Act (HIPAA). Bien que vous puissiez commencer votre AWS parcours avec un seul compte, il est AWS recommandé de configurer plusieurs comptes à mesure que votre charge de travail augmente en taille et en complexité.

Les autorisations vous permettent de définir l'accès aux AWS ressources. Les autorisations sont accordées aux entités IAM appelées entités principales (utilisateurs, groupes et rôles). Par défaut,

les principaux démarrent sans aucune autorisation. Les responsables IAM ne peuvent rien faire AWS tant que vous ne leur accordez pas d'autorisations, et vous pouvez mettre en place des garde-fous applicables à AWS l'ensemble de votre organisation ou aussi précis qu'une combinaison individuelle de principe, d'action, de ressource et de conditions.

Utilisation à AWS Organizations des fins de sécurité

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

AWS Organizationsvous permet de gérer et de gouverner votre environnement de manière centralisée à mesure que vous développez et faites évoluer vos AWS ressources. En utilisant AWS Organizations, vous pouvez créer de nouveaux comptes par programmation Comptes AWS, allouer des ressources, regrouper des comptes pour organiser vos charges de travail et appliquer des politiques à des comptes ou à des groupes de comptes à des fins de gouvernance. Une AWS organisation consolide les vôtres Comptes AWS afin que vous puissiez les administrer en tant qu'unité unique. Il possède un compte de gestion et zéro ou plusieurs comptes membres. La plupart de vos charges de travail résident dans des comptes membres, à l'exception de certains processus gérés de manière centralisée qui doivent résider soit dans le compte de gestion, soit dans des comptes désignés en tant qu'administrateurs délégués pour des raisons spécifiques Services AWS. Vous pouvez fournir des outils et un accès à partir d'un emplacement central à votre équipe de sécurité afin qu'elle puisse gérer les besoins de sécurité au nom d'une AWS organisation. Vous pouvez réduire la duplication des ressources en partageant les ressources critiques au sein de votre AWS organisation. Vous pouvez regrouper les comptes en unités AWS organisationnelles (OUs), qui peuvent représenter différents environnements en fonction des exigences et de l'objectif de la charge de travail. AWS Organizations fournit également plusieurs politiques qui vous permettent d'appliquer de manière centralisée des contrôles de sécurité supplémentaires à tous les comptes membres de vos organisations. Cette section se concentre sur les politiques de contrôle des services (SCPs), les politiques de contrôle des ressources (RCPs) et les politiques déclaratives.

Avec AWS Organizations, vous pouvez utiliser SCPset appliquer des RCPsbarrières d'autorisation au niveau de l' AWS organisation, de l'unité d'organisation ou du compte. SCPs sont des garde-fous qui s'appliquent aux principaux du compte d'une organisation, à l'exception du compte de gestion (c'est l'une des raisons de ne pas gérer les charges de travail sur ce compte). Lorsque vous attachez un SCP à une unité d'organisation, le SCP est hérité par l'enfant OUs et les comptes

associés à cette unité d'organisation. SCPs n'accordez aucune autorisation. Ils spécifient plutôt les autorisations maximales disponibles pour vos principaux au sein d'une AWS organisation, d'une unité d'organisation ou d'un compte. Vous devez toujours associer des politiques basées sur l'identité ou les ressources aux principaux ou aux ressources de votre entreprise Comptes AWS pour leur accorder des autorisations. Par exemple, si un SCP refuse l'accès à l'ensemble d'Amazon S3, le principal concerné par le SCP n'aura pas accès à Amazon S3 même s'il y est explicitement autorisé par le biais d'une politique IAM. Pour plus d'informations sur la manière dont les politiques IAM sont évaluées, le rôle de SCPs celles-ci et la manière dont l'accès est finalement accordé ou refusé, consultez la section Logique d'évaluation des politiques dans la documentation IAM.

RCPs sont des garde-fous qui s'appliquent aux ressources figurant dans les comptes d'une organisation, qu'elles appartiennent ou non à la même organisation. Par exemple SCPs, RCPs n'affectez pas les ressources du compte de gestion et n'accordez aucune autorisation. Lorsque vous attachez un RCP à une UO, le RCP est hérité par l'enfant OUs et les comptes associés à l'UO. RCPs fournissent un contrôle centralisé sur le maximum d'autorisations disponibles pour les ressources de votre organisation et prennent actuellement en charge un sous-ensemble de Services AWS. Lorsque vous concevez SCPs pour votre OUs, nous vous recommandons d'évaluer les modifications à l'aide du simulateur de politique IAM. Vous devez également consulter les données du dernier accès au service dans IAM et les utiliser AWS CloudTrail pour enregistrer l'utilisation du service au niveau de l'API afin de comprendre l'impact potentiel des modifications du SCP.

SCPs et RCPs sont des commandes indépendantes. Vous pouvez choisir d'activer uniquement SCPs ou RCPs d'utiliser les deux types de politiques ensemble en fonction des contrôles d'accès que vous souhaitez appliquer. Par exemple, si vous souhaitez empêcher les responsables de votre organisation d'accéder à des ressources extérieures à votre organisation, vous devez appliquer ce contrôle en utilisant SCPs. Si vous souhaitez restreindre ou empêcher les identités externes d'accéder à vos ressources, vous devez appliquer ce contrôle en utilisant RCPs. Pour plus d'informations et des cas d'utilisation pour RCPs et SCPs, consultez la section Utilisation de SCPs et RCPs dans la AWS Organizations documentation.

Vous pouvez utiliser des politiques AWS Organizations déclaratives pour déclarer et appliquer de manière centralisée la configuration souhaitée pour une donnée Service AWS à grande échelle au sein d'une organisation. Par exemple, vous pouvez bloquer l'accès public à Internet aux ressources Amazon VPC au sein de votre organisation. Contrairement aux politiques d'autorisation telles que SCPs et RCPs, les politiques déclaratives sont appliquées dans le plan de contrôle d'un AWS service. Les politiques d'autorisation régulent l'accès à APIs, tandis que les politiques déclaratives sont appliquées directement au niveau du service pour faire respecter une intention durable. Ces

politiques permettent de garantir que la configuration de base d'un Service AWS est toujours maintenue, même lorsque le service introduit de nouvelles fonctionnalités ou APIs. La configuration de base est également maintenue lorsque de nouveaux comptes sont ajoutés à une organisation ou lorsque de nouveaux directeurs et ressources sont créés. Les politiques déclaratives peuvent être appliquées à l'ensemble d'une organisation ou à des comptes spécifiques OUs .

Chacun Compte AWS dispose d'un seul utilisateur root qui dispose des autorisations complètes sur toutes les AWS ressources par défaut. Pour des raisons de sécurité, nous vous recommandons de ne pas utiliser l'utilisateur root, sauf pour quelques tâches qui nécessitent explicitement un utilisateur root. Si vous gérez plusieurs comptes Comptes AWS AWS Organizations, vous pouvez désactiver la connexion root de manière centralisée, puis effectuer des actions privilégiées root pour le compte de tous les comptes membres. Après avoir géré de manière centralisée l'accès root pour les comptes membres, vous pouvez supprimer le mot de passe de l'utilisateur root, les clés d'accès et les certificats de signature, et désactiver l'authentification multifactorielle (MFA) pour les comptes membres. Les nouveaux comptes créés dans le cadre d'un accès root géré de manière centralisée ne disposent par défaut d'aucun identifiant d'utilisateur root. Les comptes membres ne peuvent pas se connecter avec leur utilisateur root ni récupérer le mot de passe de leur utilisateur root.

AWS Control Towerpropose un moyen simplifié de configurer et de gérer plusieurs comptes. Il automatise la configuration des comptes dans votre AWS organisation, automatise le provisionnement, applique des contrôles (y compris des contrôles préventifs et de détection) et vous fournit un tableau de bord pour plus de visibilité. Une politique de gestion IAM supplémentaire, une limite d'autorisations, est attachée à des principes IAM spécifiques (utilisateurs ou rôles) et définit les autorisations maximales qu'une politique basée sur l'identité peut accorder à un principal IAM.

AWS Organizations vous permet de les configurer pour Services AWSqu'elles s'appliquent à tous vos comptes. Par exemple, vous pouvez configurer la journalisation centralisée de toutes les actions effectuées au sein de votre AWS organisation en utilisant CloudTrail et en empêchant les comptes membres de désactiver la journalisation. Vous pouvez également agréger de manière centralisée les données pour les règles que vous avez définies à l'aide de celles-ci AWS Config, afin de vérifier la conformité de vos charges de travail et de réagir rapidement aux modifications. Vous pouvez l'utiliser AWS CloudFormation StackSetspour gérer de manière centralisée les CloudFormation stacks entre les comptes et OUs au sein de votre AWS organisation, afin de pouvoir configurer automatiquement un nouveau compte pour répondre à vos exigences de sécurité.

La configuration par défaut des AWS Organizations supports utilisés SCPs comme listes de refus. En utilisant une stratégie de liste de refus, les administrateurs des comptes membres peuvent déléguer tous les services et actions jusqu'à ce que vous créiez et associiez un SCP refusant un service ou un

ensemble d'actions spécifique. Les instructions de refus nécessitent moins de maintenance qu'une liste d'autorisation, car vous n'avez pas à les mettre à jour lors de l' AWS ajout de nouveaux services. Les instructions de refus sont généralement plus courtes en caractères, il est donc plus facile de respecter la taille maximale pour SCPs. Dans une instruction dont la valeur de l'`Effect`élément est égale à`Deny`, vous pouvez également restreindre l'accès à des ressources spécifiques ou définir les conditions d'entrée en vigueur. SCPs En revanche, une `Allow` déclaration dans un SCP s'applique à toutes les ressources (`"*"`) et ne peut pas être limitée par des conditions. Pour plus d'informations et des exemples, consultez la section Stratégies d'utilisation SCPs dans la AWS Organizations documentation.

Considérations relatives à la conception

- Sinon, pour l'utiliser SCPs comme liste d'autorisations, vous devez remplacer le *`FullAWSAccess`* SCP géré par AWS par un SCP qui n'autorise explicitement que les services et les actions que vous souhaitez autoriser. Pour qu'une autorisation soit activée pour un compte spécifique, chaque SCP (de la racine à chaque unité d'organisation sur le chemin direct vers le compte et même attaché au compte lui-même) doit autoriser cette autorisation. Ce modèle est de nature plus restrictive et pourrait convenir à des charges de travail sensibles et hautement réglementées. Cette approche nécessite que vous autorisiez explicitement chaque service ou action IAM sur le chemin allant de l'unité d'organisation Compte AWS à l'unité d'organisation.
- Idéalement, vous devriez utiliser une combinaison de stratégies de liste de refus et de liste d'autorisation. Utilisez la liste des autorisations pour définir la liste des autorisations Services AWS approuvées à utiliser au sein d'une AWS organisation et attachez ce SCP à la racine de votre AWS organisation. Si un ensemble de services différent est autorisé par votre environnement de développement, vous devez les associer SCPs à chaque unité d'organisation. Vous pouvez ensuite utiliser la liste de refus pour définir les garde-fous de l'entreprise en refusant explicitement des actions IAM spécifiques.
- RCPs s'appliquent aux ressources d'un sous-ensemble de. Services AWS Pour plus d'informations, consultez la liste de Services AWS ce support RCPs dans la AWS Organizations documentation. La configuration par défaut des AWS Organizations supports utilisés RCPs comme listes de refus. Lorsque vous l'activez RCPs dans votre organisation, une politique AWS gérée appelée `RCPFullAWSAccess` est automatiquement attachée à la racine de l'organisation, à chaque unité d'organisation et à chaque compte de votre organisation. Vous ne pouvez pas dissocier cette politique. Ce RCP par défaut permet à tous les principaux et à tous les accès aux actions de passer par une évaluation

RCP. Cela signifie que jusqu'à ce que vous commenciez à créer et à joindre RCPs, toutes vos autorisations IAM existantes continuent de fonctionner comme avant. Cette politique AWS gérée n'accorde pas d'accès. Vous pouvez ensuite en créer une nouvelle RCPs sous forme de liste de déclarations de refus afin de bloquer l'accès aux ressources de votre organisation.

Le compte de gestion, l'accès sécurisé et les administrateurs délégués

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le compte de gestion (également appelé compte de gestion de l' AWS organisation ou compte de gestion de l'organisation) est unique et différencié de tous les autres comptes de AWS Organizations. C'est le compte qui crée l' AWS organisation. À partir de ce compte, vous pouvez créer des comptes Comptes AWS au AWS sein de l'organisation, inviter d'autres comptes existants à rejoindre l' AWS organisation (les deux types sont considérés comme des comptes membres), supprimer des comptes de l' AWS organisation et appliquer des politiques IAM à la racine ou à des comptes au sein de l' AWS organisation. OUs

Le compte de gestion déploie des garde-fous de sécurité universels par le biais SCPs de déploiements de services (tels que CloudTrail) qui affecteront tous les comptes membres de l'organisation. RCPs AWS Pour restreindre davantage les autorisations dans le compte de gestion, ces autorisations peuvent être déléguées à un autre compte approprié, tel qu'un compte de sécurité, dans la mesure du possible.

Le compte de gestion possède les responsabilités d'un compte souscripteur et est responsable du paiement de tous les frais accumulés par les comptes membres. Vous ne pouvez pas changer de compte de gestion d'une AWS organisation. An Compte AWS ne peut être membre que d'une seule AWS organisation à la fois.

En raison des fonctionnalités et de l'étendue de l'influence du compte de gestion, nous vous recommandons de limiter l'accès à ce compte et d'accorder des autorisations uniquement aux rôles qui en ont besoin. Les deux fonctionnalités qui vous y aident sont l'accès sécurisé et l'administrateur

délégué. Vous pouvez utiliser l'accès sécurisé pour activer un service Service AWS que vous spécifiez, appelé service sécurisé, pour effectuer des tâches dans votre AWS organisation et ses comptes en votre nom. Cela implique l'octroi d'autorisations au service approuvé mais n'affecte pas par ailleurs les autorisations pour les utilisateurs et les rôles IAM. Vous pouvez utiliser l'accès sécurisé pour spécifier les paramètres et les détails de configuration que vous souhaitez que le service sécurisé conserve en votre nom dans les comptes de votre AWS organisation. Par exemple, la section relative au compte de gestion de l'organisation de la AWS SRA explique comment accorder au CloudTrail service un accès sécurisé afin de créer un suivi de CloudTrail l'organisation dans tous les comptes de votre AWS organisation.

Certains Services AWS prennent en charge la fonctionnalité d'administrateur délégué dans AWS Organizations. Grâce à cette fonctionnalité, les services compatibles peuvent enregistrer un compte de AWS membre dans l' AWS organisation en tant qu'administrateur des comptes de AWS l'organisation dans ce service. Cette fonctionnalité permet aux différentes équipes de votre entreprise d'utiliser des comptes distincts, en fonction de leurs responsabilités, pour gérer l' Services AWS ensemble de l'environnement. Les services AWS de sécurité de la AWS SRA qui prennent actuellement en charge l'administrateur délégué incluent IAM Identity Center, AWS Config, AWS Firewall Manager Amazon GuardDuty, IAM Access Analyzer, Amazon Macie, AWS Security Hub Cloud Security Posture Management (), Amazon Detective,AWS Security Hub CSPM Amazon AWS Audit Manager Inspector et. AWS Systems Manager L'utilisation de la fonctionnalité d'administrateur délégué est soulignée dans la AWS SRA en tant que meilleure pratique, et nous déléguons l'administration des services liés à la sécurité au compte Security Tooling.

Structure de comptes dédiée

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

An Compte AWS fournit des limites de sécurité, d'accès et de facturation pour vos AWS ressources, et vous permet de garantir l'indépendance et l'isolation des ressources. Par défaut, aucun accès n'est autorisé entre les comptes.

Lorsque vous concevez votre unité d'organisation et votre structure de compte, commencez par penser à la sécurité et à l'infrastructure. Nous vous recommandons de créer un ensemble de bases OUs pour ces fonctions spécifiques, réparties entre infrastructure et sécurité OUs. Ces recommandations relatives aux unités d'organisation et aux comptes reflètent un sous-ensemble de

nos directives plus générales AWS Organizations et plus complètes pour la conception de structures multicomptes. Pour un ensemble complet de recommandations, consultez la section Organisation de votre AWS environnement à l'aide de plusieurs comptes dans la AWS documentation et dans le billet de blog Meilleures pratiques pour les unités organisationnelles dotées de AWS Organizations.

La AWS SRA utilise les comptes suivants pour réaliser des opérations de sécurité efficaces sur. AWS Ces comptes dédiés permettent de garantir la séparation des tâches, de prendre en charge différentes politiques de gouvernance et d'accès pour différents types d'applications et de données sensibles, et d'atténuer l'impact d'un événement de sécurité. Dans les discussions qui suivent, nous nous concentrons sur les comptes de production (production) et leurs charges de travail associées. Les comptes du cycle de vie du développement logiciel (SDLC) (souvent appelés comptes de développement et de test) sont destinés à la préparation des livrables et peuvent fonctionner selon une politique de sécurité différente de celle des comptes de production.

Compte	UO	Rôle de sécurité
Gestion	—	Gouvernance et gestion centralisées de tous Régions AWS les comptes. Celui Compte AWS qui héberge la racine de l' AWS organisation.
Outillage de sécurité	Sécurité	Dédié Comptes AWS à l'exploitation de services de sécurité largement applicables (tels que GuardDuty Security Hub CSPM, Audit Manager, Detective, Amazon Inspector , etc. AWS Config), à la surveillance Comptes AWS et à l'automatisation des alertes et réponses de sécurité. (Dans AWS Control Tower, le nom par défaut du compte dans l'unité d'organisation de sécurité est Audit account.)

Archive du journal	Sécurité	Dédié Comptes AWS à l'ingestion et à l'archivage de tous les journaux et sauvegard es pour tous Régions AWS et. Comptes AWS Cela doit être conçu comme un stockage immuable.
Réseau	Infrastructures	La passerelle entre votre application et l'Internet au sens large. Le compte réseau isole l'ensemble des services réseau, de la configuration et du fonctionnement des charges de travail, de la sécurité et des autres infrastru ctures des applications individuelles.
Services partagés	Infrastructures	Ce compte prend en charge les services utilisés par de nombreuses applications et équipes pour obtenir leurs résultats. Les exemples incluent les services d'annuair e Identity Center (Active Directory), les services de messagerie et les services de métadonnées.

Application	Charges de travail	Comptes AWS qui hébergent les applications de AWS l'organisation et exécutent les charges de travail. (Ces comptes sont parfois appelés comptes de charge de travail.) Les comptes d'applications doivent être créés pour isoler les services logiciels au lieu d'être mappés à vos équipes. Cela rend l'application déployée plus résilient e face aux changements organisationnels.

AWS organisation et structure des comptes de la AWS SRA

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

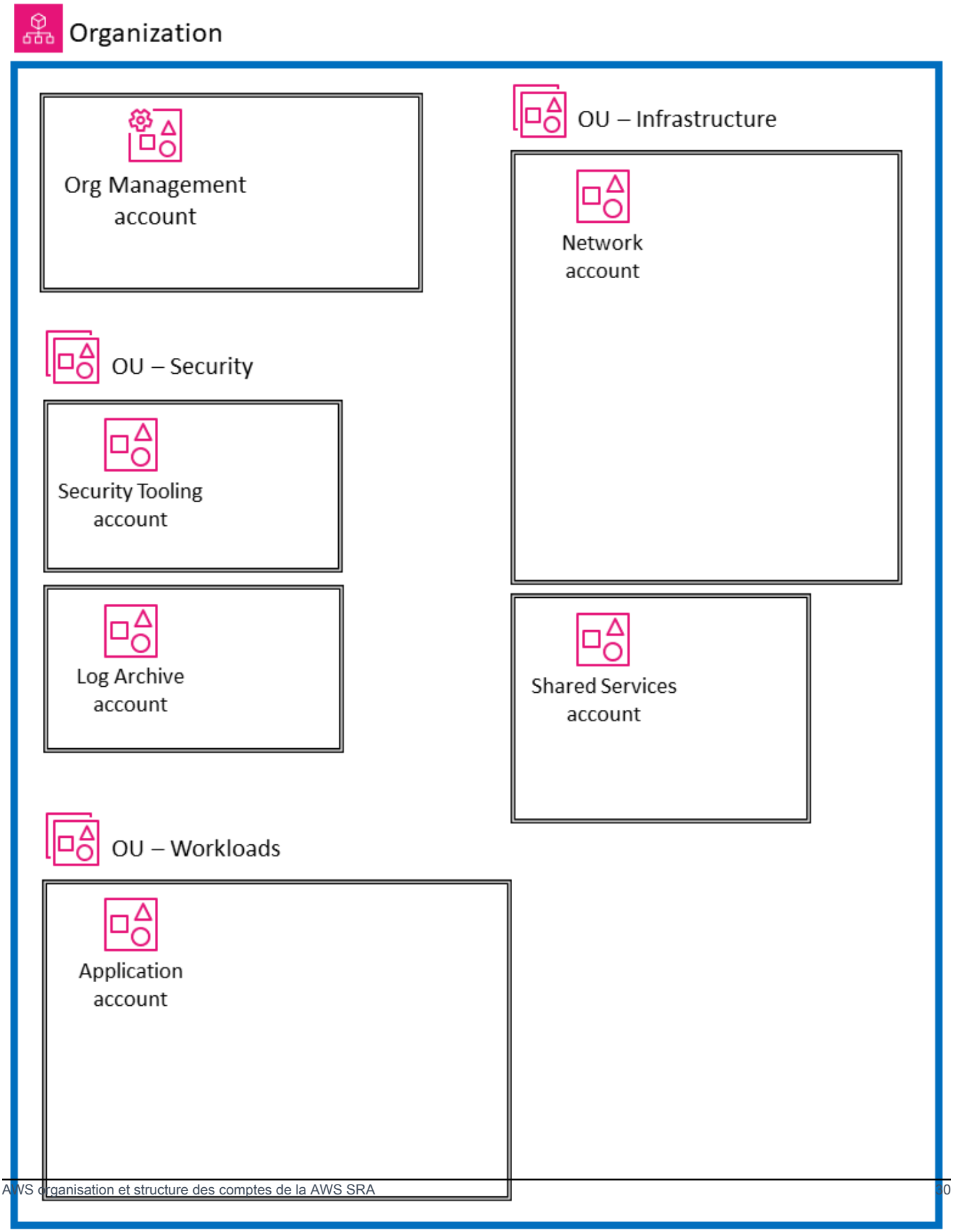
Le schéma suivant illustre la structure de haut niveau de la AWS SRA sans afficher de services spécifiques. Il reflète la structure de comptes dédiés décrite dans la section précédente, et nous incluons le schéma ici pour orienter la discussion autour des principaux composants de l'architecture :

- Tous les comptes présentés dans le diagramme font partie d'une seule AWS organisation.
- En haut à gauche du diagramme se trouve le compte de gestion de l'organisation, qui est utilisé pour créer l' AWS organisation.
- Sous le compte Org Management se trouve l'unité d'organisation de sécurité avec deux comptes spécifiques : l'un pour Security Tooling et l'autre pour Log Archive.
- Sur le côté droit se trouve l'unité d'organisation d'infrastructure avec le compte réseau et le compte Shared Services.

- Au bas du diagramme se trouve l'unité d'organisation Workloads, qui est associée à un compte d'application hébergeant l'application d'entreprise.

Aux fins de ces directives, tous les comptes sont considérés comme des comptes de production (prod) fonctionnant en un seul Région AWS. La plupart Services AWS (à l'exception des services mondiaux) ont une portée régionale, ce qui signifie que les plans de contrôle et de données du service existent indépendamment dans chacune d'elles. Région AWS Pour cette raison, vous devez reproduire cette architecture sur tout ce Régions AWS que vous prévoyez d'utiliser, afin de garantir la couverture de l'ensemble de votre AWS paysage. Si vous n'avez aucune charge de travail dans une région spécifique Région AWS, vous devez désactiver la région en utilisant SCPsou en utilisant des mécanismes de journalisation et de surveillance. Vous pouvez utiliser Security Hub CSPM pour agréger les résultats et les scores de sécurité de plusieurs régions d'agrégation Régions AWS vers une seule région d'agrégation pour une visibilité centralisée.

Lorsque vous hébergez une AWS organisation disposant d'un grand nombre de comptes, il est avantageux de disposer d'une couche d'orchestration qui facilite le déploiement et la gouvernance des comptes. AWS Control Tower offre un moyen simple de configurer et de gérer un environnement AWS multi-comptes. Les exemples de code AWS SRA contenus dans le GitHub référentiel montrent comment utiliser la solution Customizations for AWS Control Tower (CfCT) pour déployer les structures recommandées par la AWS SRA.

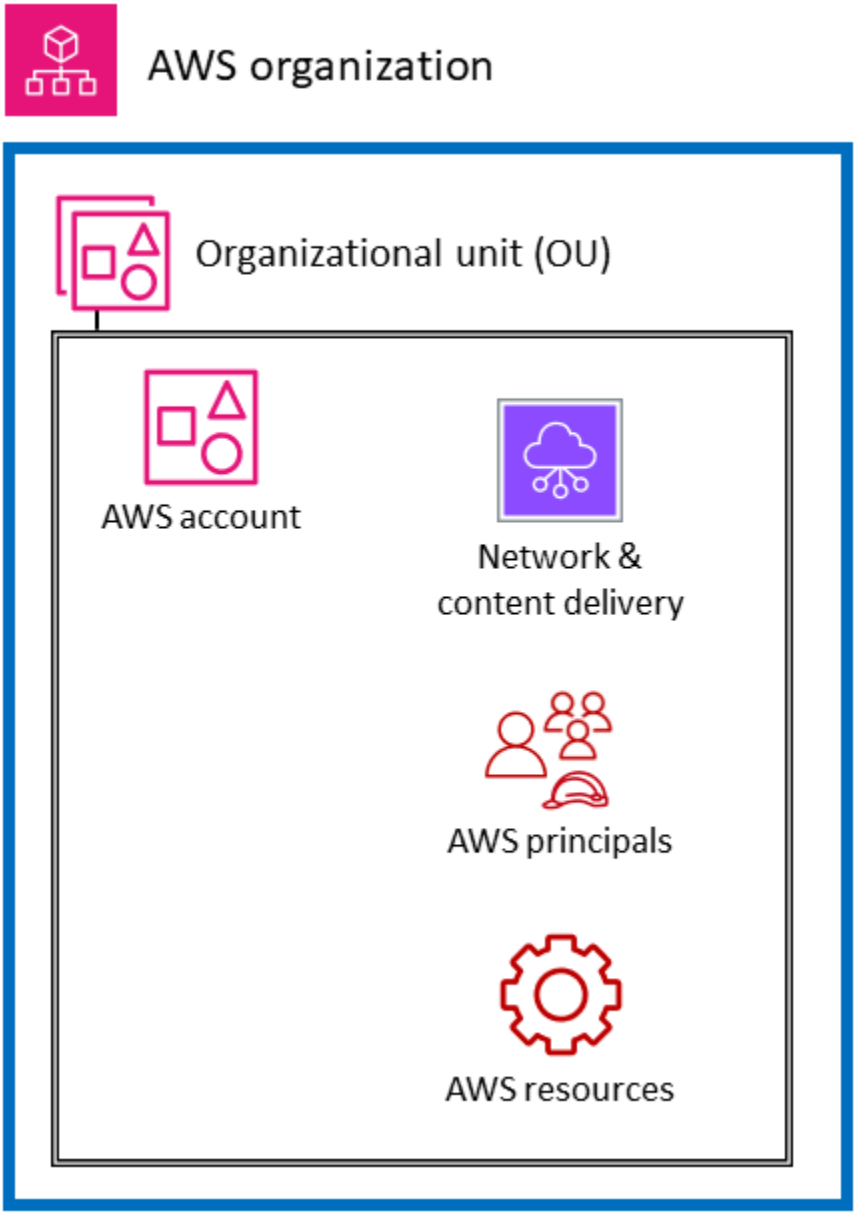

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

Appliquez des services de sécurité à l'ensemble de votre AWS organisation

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Comme décrit dans une section précédente, les clients recherchent un autre moyen de réfléchir à l'ensemble des services de AWS sécurité et de les organiser de manière stratégique. L'approche organisationnelle la plus courante aujourd'hui consiste à regrouper les services de sécurité par fonction principale, en fonction de ce que fait chaque service. Le point de vue de la sécurité de la AWS CAF répertorie neuf capacités fonctionnelles, notamment la gestion des identités et des accès, la protection de l'infrastructure, la protection des données et la détection des menaces. L'adaptation Services AWS à ces capacités fonctionnelles est un moyen pratique de prendre des décisions de mise en œuvre dans chaque domaine. Par exemple, lorsqu'il s'agit de la gestion des identités et des accès, IAM et IAM Identity Center sont des services à prendre en compte. Lors de l'architecture de votre approche de détection des menaces, GuardDuty cela peut être votre première considération.

En complément de cette vue fonctionnelle, vous pouvez également visualiser votre sécurité à l'aide d'une vue structurelle transversale. C'est-à-dire, en plus de demander : « Lequel Services AWS dois-je utiliser pour contrôler et protéger mes identités, mon accès logique ou mes mécanismes de détection des menaces ? » , vous pouvez également demander : « Lequel Services AWS dois-je appliquer dans l'ensemble de mon AWS organisation ? Quelles sont les couches de défense que je dois mettre en place pour protéger les instances Amazon EC2 au cœur de mon application ? » Dans cette vue, vous cartographiez Services AWS les entités et les couches de votre AWS environnement. 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 à cette couche. Il est préférable de le faire au niveau de l'organisation racine plutôt que de faire partie de la configuration du compte individuel. Il est préférable d'utiliser les autres services et fonctionnalités pour protéger les ressources individuelles au sein d'un Compte AWS. La mise en œuvre d'une autorité de certification (CA) subordonnée au sein d'un compte qui nécessite des certificats TLS privés est un exemple de cette catégorie. Un autre groupe tout aussi important comprend les services qui ont un effet sur la couche réseau virtuelle de votre AWS infrastructure. Le schéma suivant montre six couches dans un AWS environnement typique : AWS organisation, unité organisationnelle (UO), compte, infrastructure réseau, principaux et ressources.



Comprendre les services dans ce contexte structurel, y compris les contrôles et les protections à chaque niveau, vous aide à planifier et à mettre en œuvre une defense-in-depth stratégie dans votre AWS environnement. Dans cette perspective, vous pouvez répondre aux questions du haut vers le bas (par exemple, « Quels services utilisez-vous pour mettre en œuvre des contrôles de sécurité dans AWS l'ensemble de mon organisation ? ») et de bas en haut (par exemple, « Quels services gèrent les contrôles sur cette instance EC2 ? »). Dans cette section, nous examinons les éléments d'un AWS environnement et identifions les services et fonctionnalités de sécurité associés. Bien entendu, certains Services AWS proposent de vastes ensembles de fonctionnalités et répondent à de

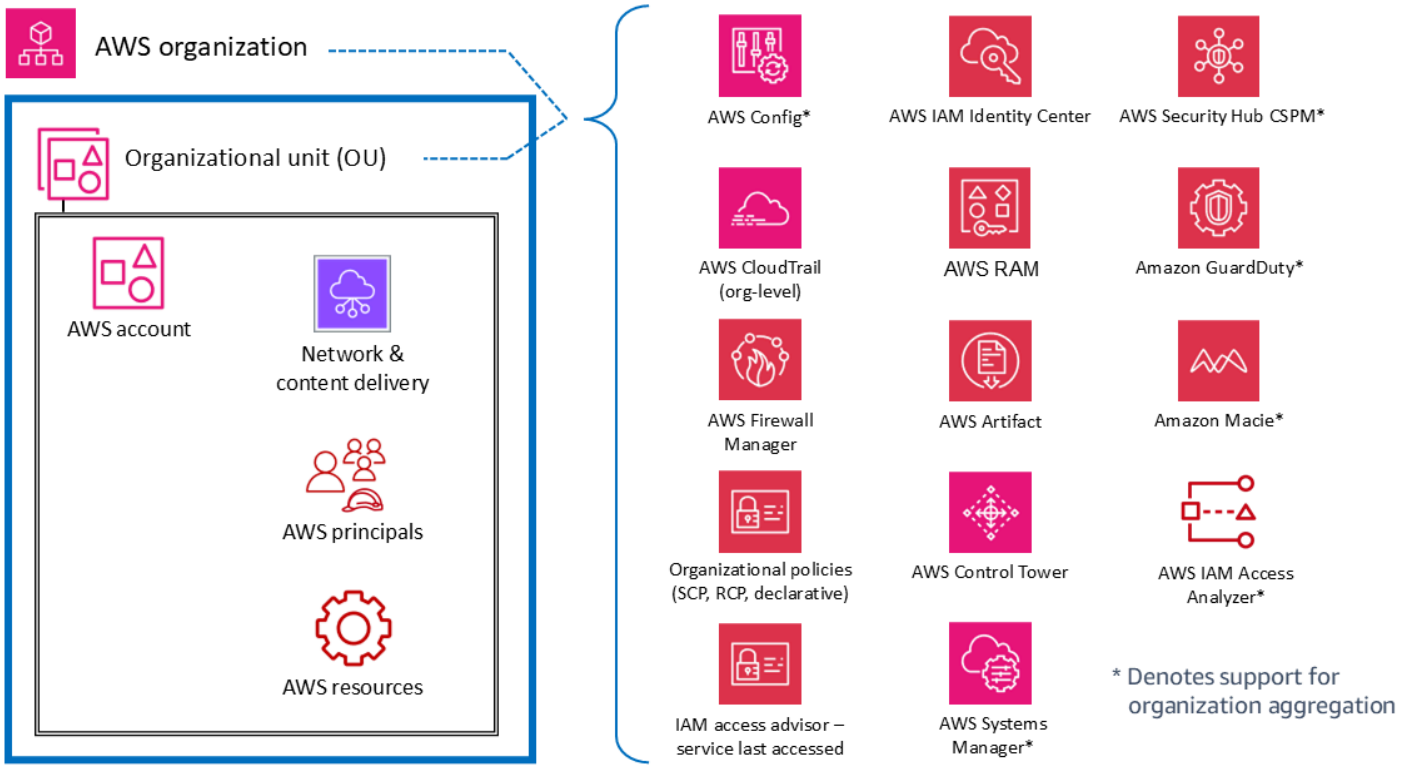
multiples objectifs de sécurité. Ces services peuvent prendre en charge plusieurs éléments de votre AWS environnement.

Pour plus de clarté, nous fournissons de brèves descriptions de la manière dont certains services répondent aux objectifs énoncés. La section suivante fournit une discussion plus approfondie sur les services individuels de chacun d'entre eux Compte AWS.

Comptes multiples ou à l'échelle de l'organisation

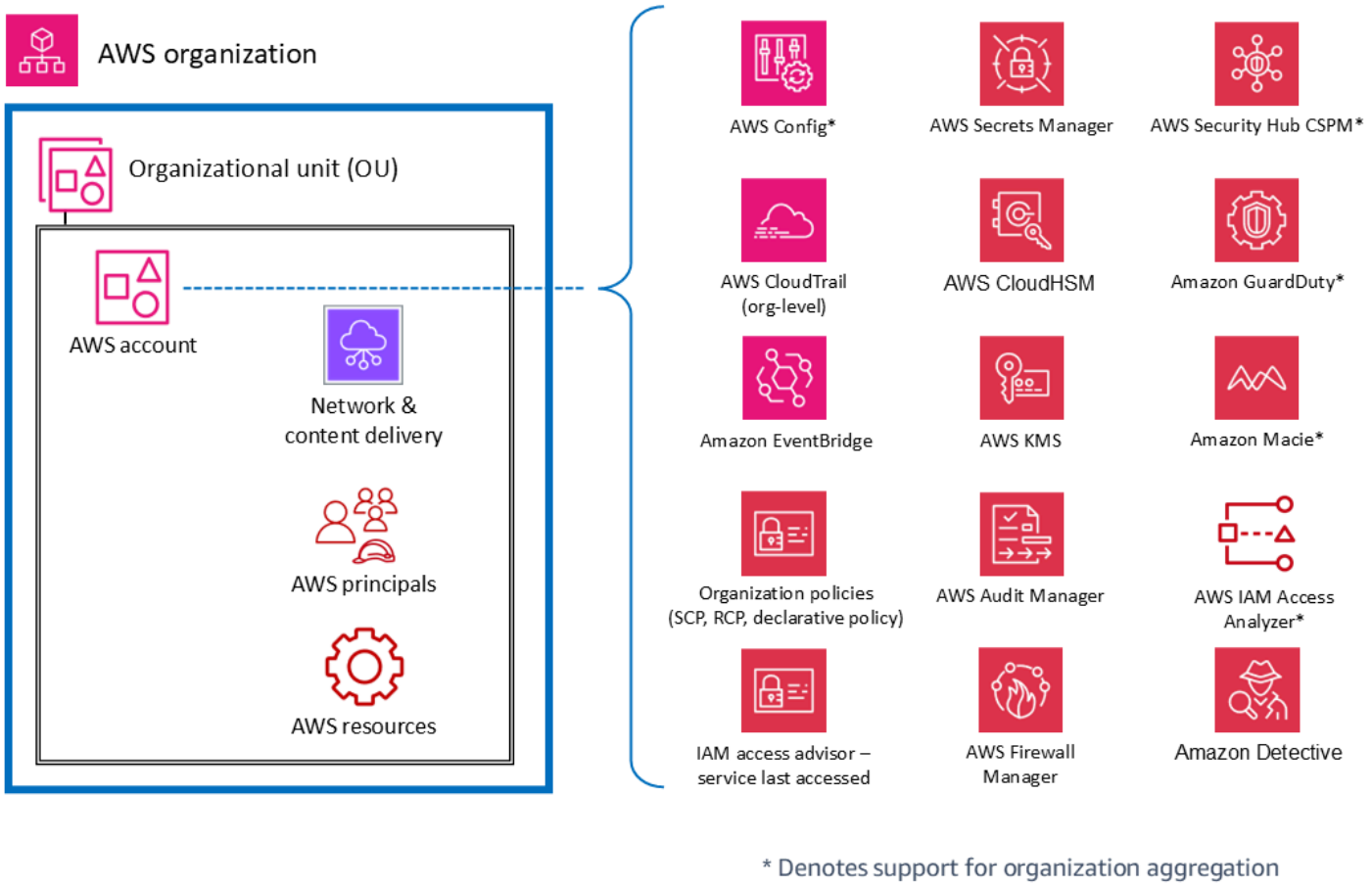
Au niveau supérieur, certaines fonctionnalités sont Services AWS conçues pour appliquer des fonctionnalités de gouvernance et de contrôle ou des garde-fous à plusieurs comptes d'une AWS organisation (y compris l'ensemble de l'organisation ou un compte spécifique OUs). Les politiques de contrôle des services (SCPs) et les politiques de contrôle des ressources (RCPs) sont de bons exemples de fonctionnalités IAM qui fournissent des garde-fous préventifs à l'échelle de l' AWS organisation. AWS Organizations fournit également une politique déclarative qui définit et applique de manière centralisée la configuration de base pour Services AWS at scale. Un autre exemple est CloudTrail celui qui fournit une surveillance par le biais d'un journal d'organisation qui enregistre tous les événements pour tous Comptes AWS les membres de cette AWS organisation. Ce parcours complet est distinct des parcours individuels qui peuvent être créés dans chaque compte. Un troisième exemple est AWS Firewall Manager celui que vous pouvez utiliser pour configurer, appliquer et gérer plusieurs ressources sur tous les comptes de votre AWS organisation : AWS WAF règles, règles AWS WAF classiques, AWS Shield Advanced protections, groupes de sécurité Amazon Virtual Private Cloud (Amazon VPC), AWS Network Firewall politiques et politiques de pare-feu Amazon Route 53 Resolver DNS.

Les services marqués d'un astérisque (*) dans le schéma suivant ont une double portée : à l'échelle de l'organisation et axés sur les comptes. Ces services surveillent ou aident essentiellement à contrôler la sécurité d'un compte individuel. Cependant, ils offrent également la possibilité d'agréger les résultats de plusieurs comptes dans un compte à l'échelle de l'organisation pour une visibilité et une gestion centralisées. Pour plus de clarté, considérez SCPs que cela s'applique à l'ensemble d'une unité Compte AWS d' AWS organisation ou d'une organisation. En revanche, vous pouvez configurer et gérer à la GuardDuty fois au niveau du compte (où les résultats individuels sont générés) et au niveau de l' AWS organisation (à l'aide de la fonctionnalité d'administrateur délégué) où les résultats peuvent être visualisés et gérés de manière agrégée.



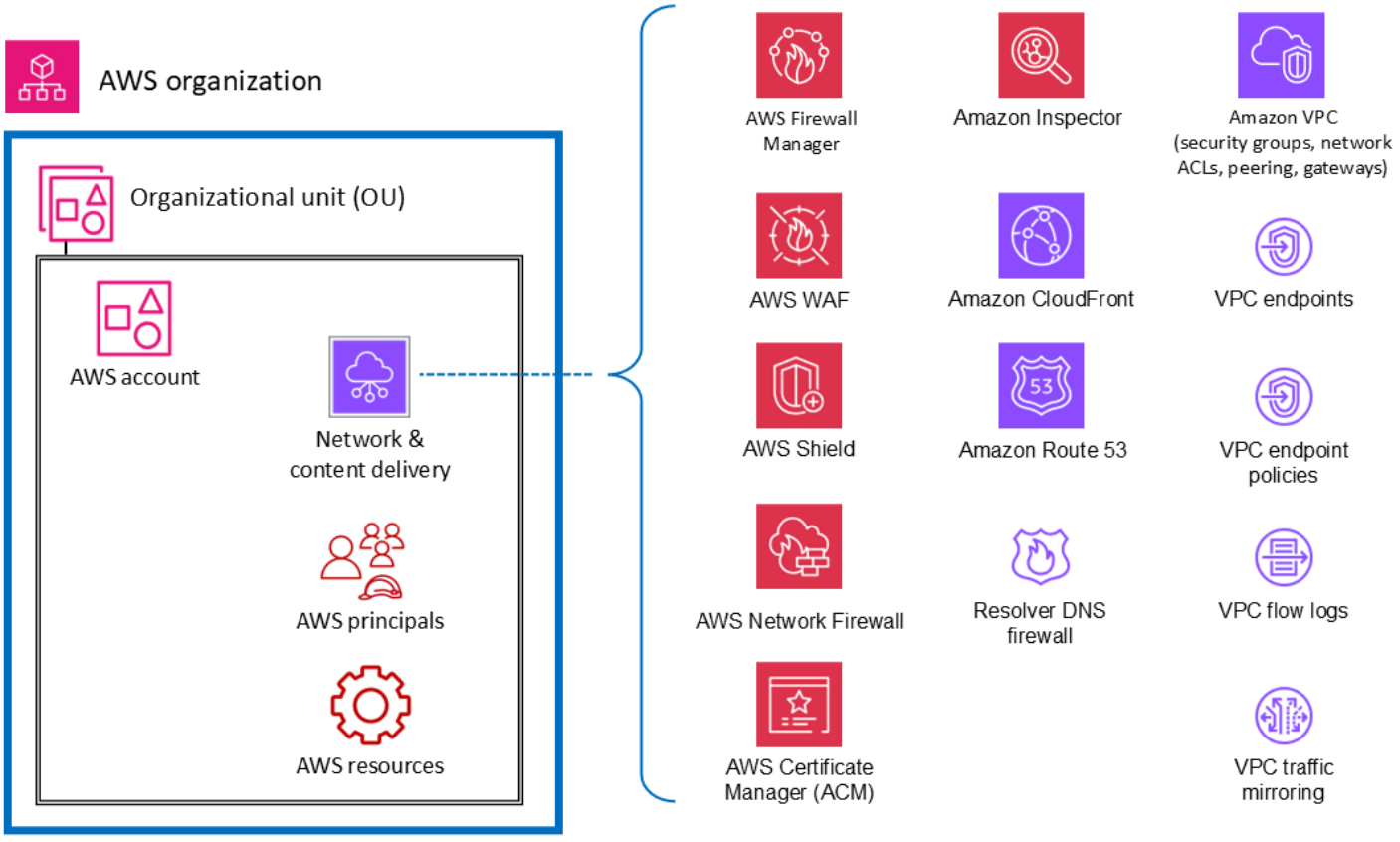
AWS comptes

À l'intérieur OUs, il existe des services qui aident à protéger plusieurs types d'éléments au sein d'un Compte AWS. Par exemple, AWS Secrets Manager il est souvent géré à partir d'un compte spécifique et protège les ressources (telles que les informations d'identification de base de données ou d'authentification), les applications et le Services AWS contenu de ce compte. L'analyseur d'accès IAM peut être configuré pour générer des résultats lorsque des ressources spécifiées sont accessibles par des principaux extérieurs à. Compte AWS Comme indiqué dans la section précédente, bon nombre de ces services peuvent également être configurés et administrés en interne AWS Organizations, de sorte qu'ils peuvent être gérés sur plusieurs comptes. Ces services sont marqués d'un astérisque (*) dans le schéma. Ils facilitent également l'agrégation des résultats de plusieurs comptes et leur transfert vers un seul compte. Cela donne aux équipes d'application individuelles la flexibilité et la visibilité nécessaires pour gérer les besoins de sécurité spécifiques à leur charge de travail, tout en offrant une gouvernance et une visibilité aux équipes de sécurité centralisées. GuardDuty est un exemple d'un tel service. GuardDuty surveille les ressources et les activités associées à un seul compte, et GuardDuty les résultats provenant de plusieurs comptes membres (tels que tous les comptes d'une AWS organisation) peuvent être collectés, consultés et gérés à partir d'un compte d'administrateur délégué.



Réseau virtuel, calcul et diffusion de contenu

Étant donné que l'accès au réseau est essentiel en matière de sécurité et que l'infrastructure informatique est un élément fondamental de nombreuses AWS charges de travail, de nombreux services et fonctionnalités de AWS sécurité sont dédiés à ces ressources. Par exemple, Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos AWS charges de travail pour détecter les vulnérabilités. Ces analyses incluent des contrôles d'accessibilité au réseau qui indiquent qu'il existe des chemins réseau autorisés vers les instances Amazon EC2 dans votre environnement. Amazon VPC vous permet de définir un réseau virtuel dans lequel vous pouvez lancer AWS des ressources. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel et inclut une variété de fonctionnalités et d'avantages. Les points de terminaison VPC vous permettent de connecter en privé votre VPC aux services de point de terminaison pris en charge Services AWS et alimentés par celui-ci AWS PrivateLink sans avoir besoin d'un chemin d'accès à Internet. Le schéma suivant illustre les services de sécurité axés sur le réseau, le calcul et l'infrastructure de diffusion de contenu.



Principes et ressources

AWS les principes et les AWS ressources (ainsi que les politiques IAM) sont les éléments fondamentaux de la gestion des identités et des accès. AWS Un utilisateur principal authentifié AWS peut effectuer des actions et accéder aux AWS ressources. Un principal peut être authentifié en tant qu'utilisateur Compte AWS root et utilisateur IAM, ou en assumant un rôle.

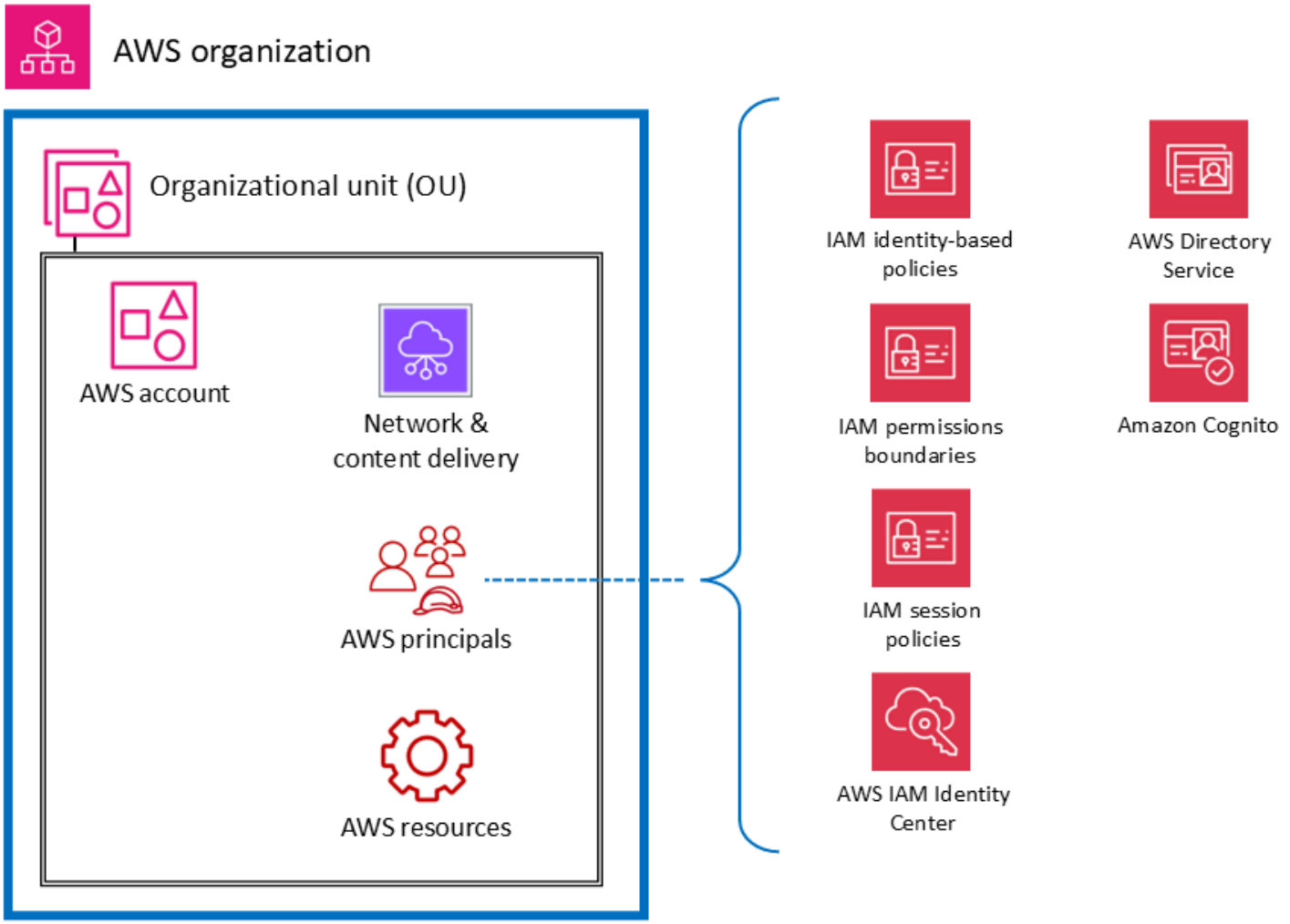
> **Note**
>
> Ne créez pas de clés d'API persistantes associées au compte utilisateur AWS root. L'accès au compte utilisateur root doit être limité uniquement aux tâches qui nécessitent un utilisateur root, et uniquement par le biais d'un processus d'exception et d'approbation rigoureux. Pour connaître les meilleures pratiques permettant de protéger l'utilisateur root de votre compte, consultez la documentation IAM.

Une AWS ressource est un objet qui existe dans un objet Service AWS que vous pouvez utiliser. Les exemples incluent une instance EC2, une CloudFormation pile, une rubrique Amazon Simple

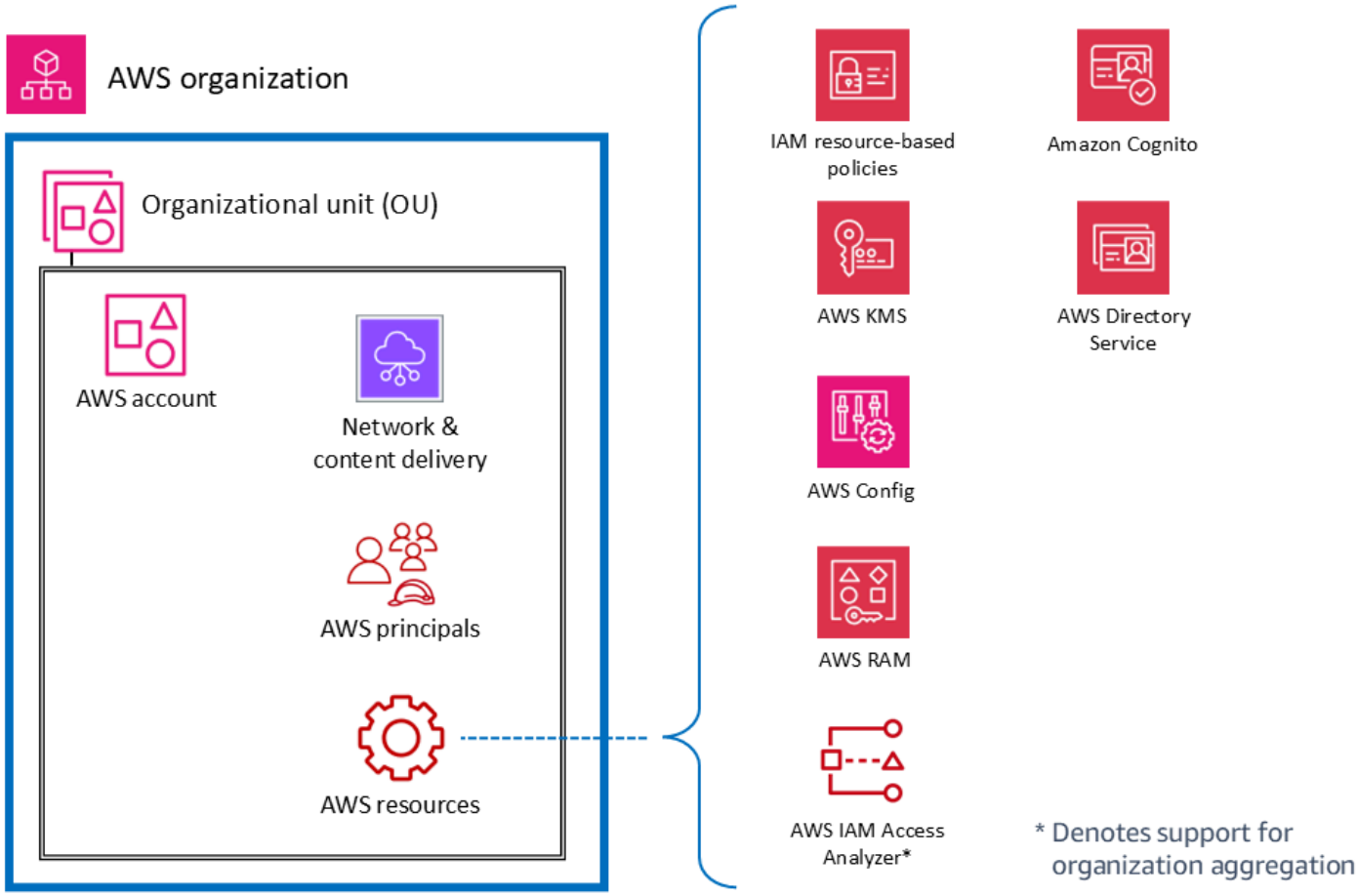
Notification Service (Amazon SNS) et un compartiment S3. Les politiques IAM sont des objets qui définissent les autorisations lorsqu'elles sont associées à un principal IAM (utilisateur, groupe ou rôle) ou AWS à une ressource. Les politiques basées sur l'identité sont des documents de stratégie que vous attachez à un principal (rôles, utilisateurs et groupes d'utilisateurs) pour contrôler les actions qu'un principal peut effectuer, sur quelles ressources et dans quelles conditions. Les politiques basées sur les ressources sont des documents de politique que vous attachez à une ressource telle qu'un compartiment S3. Ces politiques accordent l'autorisation principale spécifiée pour effectuer des actions spécifiques sur cette ressource et définissent les conditions de cette autorisation. Les politiques basées sur les ressources sont des politiques intégrées. La section des ressources IAM approfondit les types de politiques IAM et leur mode d'utilisation.

Pour simplifier les choses dans cette discussion, nous listons les services et fonctionnalités de AWS sécurité destinés aux principaux IAM dont l'objectif principal est d'opérer ou de s'appliquer aux principaux responsables de comptes. Nous conservons cette simplicité tout en reconnaissant la flexibilité et l'étendue des effets des politiques d'autorisation IAM. Une seule déclaration dans une politique peut avoir des effets sur plusieurs types d' AWS entités. Par exemple, bien qu'une politique basée sur l'identité IAM soit associée à un principal IAM et définisse des autorisations (autoriser, refuser) pour ce principal, la stratégie définit également implicitement des autorisations pour les actions, les ressources et les conditions spécifiées. Ainsi, une politique basée sur l'identité peut être un élément essentiel dans la définition des autorisations pour une ressource.

Le schéma suivant illustre les services et fonctionnalités de AWS sécurité destinés AWS aux principaux. Les politiques basées sur une identité sont attachées à un utilisateur, un groupe ou un rôle IAM. Ces politiques vous permettent de spécifier ce que peut faire cette identité (ses autorisations). Une stratégie de session IAM est une politique d'autorisation intégrée que les utilisateurs transmettent au cours de la session lorsqu'ils assument le rôle. Vous pouvez transmettre la politique vous-même ou configurer votre courtier d'identité pour qu'il insère la politique lorsque vos identités se fédérent. AWS Cela permet à vos administrateurs de réduire le nombre de rôles qu'ils doivent créer, car plusieurs utilisateurs peuvent assumer le même rôle tout en disposant d'autorisations de session uniques. Le service IAM Identity Center est intégré aux opérations d' AWS API AWS Organizations et vous aide à gérer l'accès SSO et les autorisations des utilisateurs sur l'ensemble de votre Comptes AWS site. AWS Organizations



Le schéma suivant illustre les services et les fonctionnalités des ressources du compte. Les politiques basées sur les ressources sont attachées à une ressource. Par exemple, vous pouvez associer des politiques basées sur les ressources aux compartiments S3, aux files d'attente Amazon Simple Queue Service (Amazon SQS), aux points de terminaison VPC et aux clés de chiffrement. AWS KMS Vous pouvez utiliser des politiques basées sur les ressources pour spécifier qui a accès à la ressource et quelles actions ils peuvent effectuer sur celle-ci. Les politiques de compartiment S3, les politiques AWS KMS clés et les politiques de point de terminaison VPC sont des types de politiques basées sur les ressources. IAM Access Analyzer vous aide à identifier les ressources de votre organisation et les comptes, tels que les compartiments S3 ou les rôles IAM, qui sont partagés avec une entité externe. Cela vous permet d'identifier les accès involontaires à vos ressources et à vos données, qui constituent un risque pour la sécurité. AWS Config vous permet d'évaluer, d'auditer et d'évaluer les configurations des AWS ressources prises en charge dans votre Comptes AWS. AWS Config surveille et enregistre en permanence les configurations AWS des ressources, et évalue automatiquement les configurations enregistrées par rapport aux configurations souhaitées.


AWS organization
Organizational unit (OU)
AWS account
Network & content delivery
AWS principals
AWS resources
IAM resource-based policies
Amazon Cognito
AWS KMS
AWS Directory Service
AWS Config
AWS RAM
AWS IAM Access Analyzer*
* Denotes support for organization aggregation

Architecture de référence en AWS matière de sécurité

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le schéma suivant illustre le AWS SRA. Ce schéma architectural regroupe tous les services AWS liés à la sécurité. Il est construit autour d'une architecture Web simple à trois niveaux pouvant tenir sur une seule page. Dans une telle charge de travail, il existe un niveau Web par lequel les utilisateurs se connectent et interagissent avec le niveau application, qui gère la logique métier réelle de l'application : réception des entrées de l'utilisateur, exécution de certains calculs et génération de sorties. Le niveau application stocke et extrait les informations du niveau données. L'architecture est délibérément modulaire et fournit une abstraction de haut niveau pour de nombreuses applications Web modernes.

Schémas d'architecture

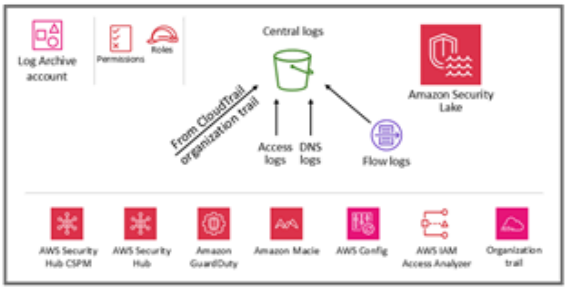
Pour personnaliser les diagrammes d'architecture de référence de ce guide en fonction des besoins de votre entreprise, vous pouvez télécharger le fichier .zip suivant et en extraire le contenu.

Téléchar

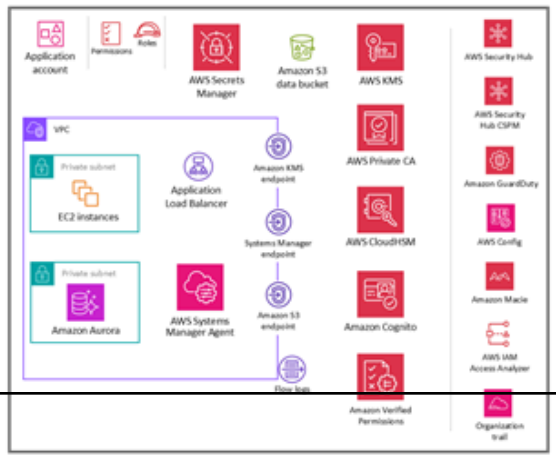
le fichier source du diagramme (PowerPoint format Microsoft)

Organization

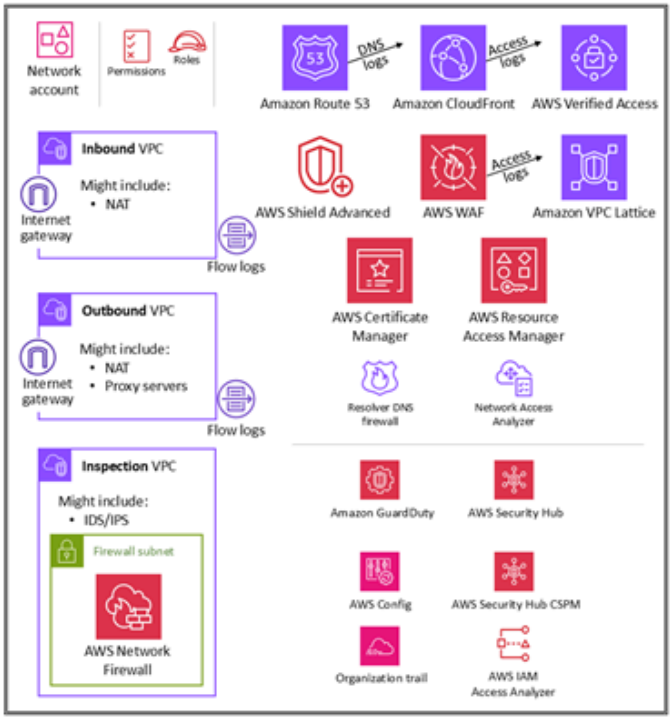
OU – Security

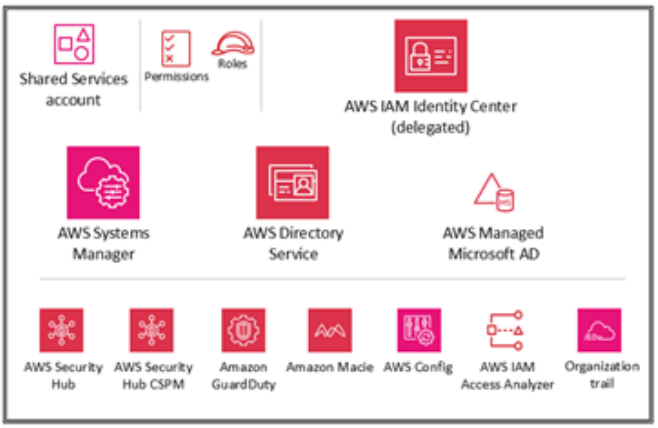


OU – Workloads



OU – Infrastructure





Pour cette architecture de référence, l'application Web et le niveau de données réels sont délibérément représentés aussi simplement que possible, par le biais d' EC2 instances Amazon et d'une base de données Amazon Aurora, respectivement. La plupart des diagrammes d'architecture se concentrent et explorent en profondeur le Web, les applications et les niveaux de données. Pour des raisons de lisibilité, ils omettent souvent les contrôles de sécurité. Ce schéma inverse cette tendance pour mettre en évidence la sécurité dans la mesure du possible, et simplifie autant que nécessaire les niveaux d'application et de données afin de présenter les fonctionnalités de sécurité de manière significative.

La AWS SRA contient tous les services AWS liés à la sécurité disponibles au moment de sa publication. (Voir l'historique du document.) Cependant, il n'est pas nécessaire de déployer tous les services de sécurité pour chaque charge de travail ou environnement, compte tenu de leur exposition unique aux menaces. Notre objectif est de fournir une référence pour une gamme d'options, y compris des descriptions de la manière dont ces services s'intègrent sur le plan architectural, afin que votre entreprise puisse prendre les décisions les mieux adaptées à votre infrastructure, à votre charge de travail et à vos besoins en matière de sécurité, en fonction des risques.

Les sections suivantes présentent chaque unité d'organisation et chaque compte afin de comprendre ses objectifs et les différents services AWS de sécurité qui y sont associés. Pour chaque élément (généralement un Service AWS), ce document fournit les informations suivantes :

- Bref aperçu de l'élément et de son objectif de sécurité dans le AWS SRA. Pour des descriptions plus détaillées et des informations techniques sur les différents services, consultez l'annexe.
- Emplacement recommandé pour activer et gérer le service le plus efficacement possible. Cela est capturé dans les diagrammes d'architecture individuels pour chaque compte et unité d'organisation.
- Liens de configuration, de gestion et de partage de données vers d'autres services de sécurité. Comment ce service s'appuie-t-il sur les autres services de sécurité, ou en quoi les appuie-t-il ?
- Considérations relatives à la conception. Tout d'abord, le document met en évidence les fonctionnalités ou configurations optionnelles qui ont des implications importantes en matière de sécurité. Ensuite, lorsque l'expérience de nos équipes inclut des variations courantes dans les recommandations que nous formulons, généralement en raison d'autres exigences ou contraintes, le document décrit ces options.

OUs et comptes

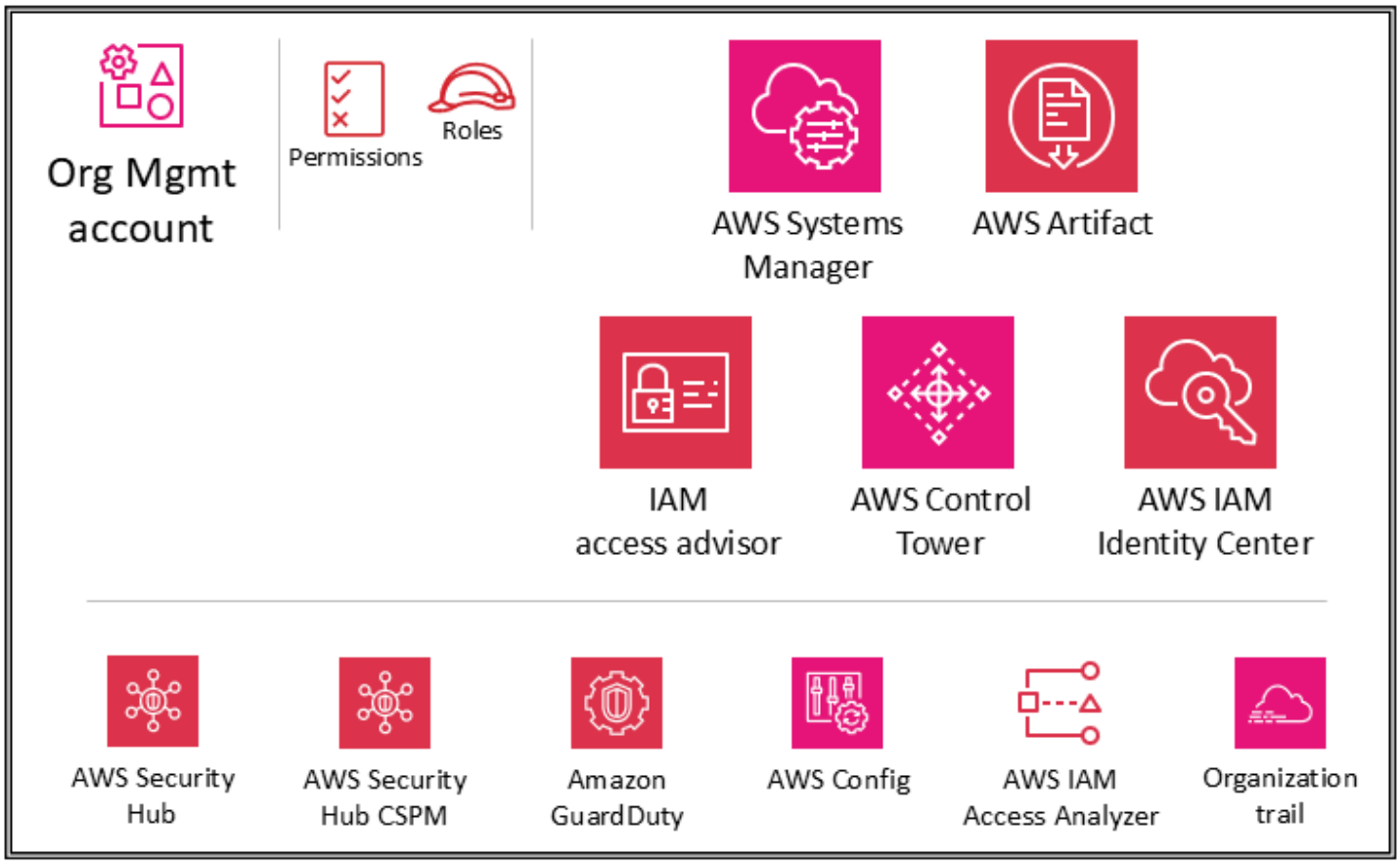
- Compte de gestion de l'organisation
- Security OU — Compte Security Tooling

- Security OU — Compte Log Archive
- Infrastructure UO – Compte réseau
- Infrastructure OU — Compte Shared Services
- Workloads OU — Compte d'application

Compte de gestion de l'organisation

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le schéma suivant illustre les services AWS de sécurité configurés dans le compte Org Management.



Les sections Utilisation à des AWS Organizations fins de sécurité et Compte de gestion, accès sécurisé et administrateurs délégués figurant plus haut dans ce guide ont décrit en détail le but et les objectifs de sécurité du compte de gestion de l'organisation. Suivez les meilleures pratiques

de sécurité pour votre compte de gestion d'organisation. Il s'agit notamment d'utiliser une adresse e-mail gérée par votre entreprise, de conserver les informations de contact administratives et de sécurité correctes (par exemple, joindre un numéro de téléphone au compte au cas où il AWS faudrait contacter le propriétaire du compte), d'activer l'authentification multifactorielle (MFA) pour tous les utilisateurs et de vérifier régulièrement qui a accès au compte de gestion de l'organisation. Les services déployés dans le compte de gestion de l'organisation doivent être configurés avec des rôles, des politiques de confiance et d'autres autorisations appropriés afin que les administrateurs de ces services (qui doivent y accéder dans le compte de gestion de l'organisation) ne puissent pas également accéder de manière inappropriée à d'autres services.

Politiques de contrôle des services

Avec AWS Organizations, vous pouvez gérer les politiques de manière centralisée sur plusieurs Comptes AWS. Par exemple, vous pouvez appliquer des politiques de contrôle des services (SCPs) Comptes AWS à plusieurs membres d'une organisation. SCPs vous permettent de définir ce qui Service AWS APIs peut ou ne peut pas être géré par les responsables IAM (tels que les utilisateurs et les rôles IAM) parmi les membres de votre organisation. Comptes AWS SCPs sont créés et appliqués à partir du compte Org Management, qui est celui Compte AWS que vous avez utilisé lors de la création de votre organisation. Pour SCPs en savoir plus, consultez la section Utilisation AWS Organizations à des fins de sécurité plus haut dans cette référence.

Si vous l'utilisez AWS Control Tower pour gérer votre AWS organisation, celle-ci déploiera un ensemble de SCPs garde-fous préventifs (classés comme obligatoires, fortement recommandés ou facultatifs). Ces garde-fous vous aident à gérer vos ressources en appliquant des contrôles de sécurité à l'échelle de l'organisation. Ils utilisent SCPs automatiquement une aws-control-tower balise dont la valeur est de managed-by-control-tower.

> **Considération relative à la conception**
>
> SCPs concernent uniquement les comptes des membres de l' AWS organisation. Bien qu'elles soient appliquées depuis le compte Org Management, elles n'ont aucun effet sur les utilisateurs ou les rôles de ce compte. Pour en savoir plus sur le fonctionnement de la logique d'évaluation SCP et pour voir des exemples de structures recommandées, consultez le billet de AWS blog Comment utiliser les politiques de contrôle des services dans AWS Organizations.

Politiques de contrôle des ressources

Les politiques de contrôle des ressources (RCPs) offrent un contrôle centralisé des autorisations maximales disponibles pour les ressources de votre organisation. Un RCP définit un garde-fou en matière d'autorisations ou fixe des limites aux actions que les identités peuvent effectuer sur les ressources de votre organisation. Vous pouvez l'utiliser RCPs pour restreindre les personnes autorisées à accéder à vos ressources et appliquer des exigences relatives à la manière dont les membres de votre organisation peuvent accéder à vos ressources Comptes AWS. Vous pouvez les joindre RCPs directement à des comptes individuels ou à la racine de l'organisation. OUs Pour une explication détaillée du RCPs fonctionnement, voir l'évaluation du RCP dans la AWS Organizations documentation. Pour RCPs en savoir plus, consultez la section Utilisation AWS Organizations à des fins de sécurité plus haut dans cette référence.

Si vous l'utilisez AWS Control Tower pour gérer votre AWS organisation, elle déploiera un ensemble de RCPs garde-fous préventifs (classés comme obligatoires, fortement recommandés ou facultatifs). Ces garde-fous vous aident à gérer vos ressources en appliquant des contrôles de sécurité à l'échelle de l'organisation. Ils utilisent SCPs automatiquement une `aws-control-tower` balise dont la valeur est de`managed-by-control-tower`.

Considérations relatives à la conception

- RCPs affectent uniquement les ressources des comptes des membres de l'organisation. Ils n'ont aucun effet sur les ressources du compte de gestion. Cela signifie également que cela RCPs s'applique aux comptes de membres désignés comme administrateurs délégués.
- RCPs s'appliquent aux ressources d'un sous-ensemble de. Services AWS Pour plus d'informations, consultez la liste de Services AWS ce support RCPs dans la AWS Organizations documentation. Vous pouvez utiliser AWS Config Rulesdes AWS Lambda fonctions pour surveiller et automatiser l'application des contrôles de sécurité sur les ressources qui ne sont pas actuellement prises en charge par RCPs.

Politiques déclaratives

Une politique déclarative est un type de politique de AWS Organizations gestion qui vous permet de déclarer et d'appliquer de manière centralisée la configuration souhaitée pour une donnée

Service AWS à grande échelle au sein d'une organisation. Les politiques déclaratives prennent actuellement en charge les services Amazon EC2, Amazon VPC et Amazon EBS. Les attributs de service disponibles incluent l'application de la version 2 du service de métadonnées d'instance (IMDSv2), la possibilité de résoudre les problèmes via la console série EC2, l'autorisation des paramètres Amazon Machine Image (AMI) et le blocage de l'accès public aux instantanés Amazon EBS, Amazon EC2 AMIs et Amazon VPC. Pour connaître les derniers services et attributs pris en charge, consultez la section Politiques déclaratives dans la AWS Organizations documentation.

Vous pouvez appliquer la configuration de base pour un Service AWS en effectuant quelques sélections sur les AWS Control Tower consoles AWS Organizations et ou en utilisant quelques commandes AWS Command Line Interface (AWS CLI) et du AWS SDK. Les politiques déclaratives sont appliquées dans le plan de contrôle du service, ce qui signifie que la configuration de base d'un Service AWS est toujours maintenue, même lorsque le service introduit de nouvelles fonctionnalités ou APIs lorsque de nouveaux comptes sont ajoutés à une organisation, ou lorsque de nouveaux principes et ressources sont créés. Les politiques déclaratives peuvent être appliquées à l'ensemble d'une organisation ou à des comptes spécifiques OUs . La stratégie efficace est l'ensemble des règles héritées de la racine de l'organisation OUs ainsi que les politiques directement associées au compte. Si une politique déclarative est détachée, l'état de l'attribut reviendra à son état antérieur à l'attachement de la politique déclarative.

Vous pouvez utiliser des politiques déclaratives pour créer des messages d'erreur personnalisés. Par exemple, si une opération d'API échoue en raison d'une politique déclarative, vous pouvez définir le message d'erreur ou fournir une URL personnalisée, telle qu'un lien vers un wiki interne ou un lien vers un message décrivant l'échec. Cela permet de fournir aux utilisateurs plus d'informations afin qu'ils puissent résoudre eux-mêmes le problème. Vous pouvez également auditer le processus de création de politiques déclaratives, de mise à jour des politiques déclaratives et de suppression de politiques déclaratives en utilisant. AWS CloudTrail

Les politiques déclaratives fournissent des rapports sur l'état des comptes, qui vous permettent de consulter l'état actuel de tous les attributs pris en charge par les politiques déclaratives des comptes concernés. Vous pouvez choisir les comptes OUs à inclure dans le champ d'application du rapport ou choisir une organisation entière en sélectionnant la racine. Ce rapport vous aide à évaluer le niveau de préparation en fournissant une ventilation Région AWS et en spécifiant si l'état actuel d'un attribut est uniforme entre les comptes (par la `numberOfMatchedAccounts` valeur) ou incohérent entre les comptes (par la `numberOfUnmatchedAccounts` valeur).

Considération relative à la conception

Lorsque vous configurez un attribut de service à l'aide d'une politique déclarative, celle-ci peut avoir un impact sur plusieurs APIs. Toute action non conforme échouera. Les administrateurs de compte ne seront pas en mesure de modifier la valeur de l'attribut de service au niveau du compte individuel.

Accès root centralisé

Tous les comptes membres AWS Organizations ont leur propre utilisateur root, qui est une identité qui a un accès complet à toutes Services AWS les ressources de ce compte membre. IAM fournit une gestion centralisée de l'accès root pour gérer l'accès root sur tous les comptes membres. Cela permet d'empêcher l'utilisation des utilisateurs root par les membres et de permettre une restauration à grande échelle. La fonctionnalité d'accès root centralisé possède deux fonctionnalités essentielles : la gestion des informations d'identification root et les sessions root.

- La fonctionnalité de gestion des informations d'identification root permet une gestion centralisée et permet de sécuriser l'utilisateur root sur tous les comptes de gestion. Cette fonctionnalité inclut la suppression des informations d'identification root à long terme, la prévention de la récupération des informations d'identification root par les comptes membres et le provisionnement de nouveaux comptes membres sans informations d'identification root par défaut. Il constitue également un moyen facile de démontrer la conformité. Lorsque la gestion des utilisateurs root est centralisée, vous pouvez supprimer les mots de passe, les clés d'accès et les certificats de signature des utilisateurs root, et désactiver l'authentification multifactorielle (MFA) de tous les comptes membres.
- La fonctionnalité des sessions root vous permet d'effectuer des actions d'utilisateur root privilégiés en utilisant des informations d'identification à court terme sur les comptes des membres depuis le compte de gestion de l'organisation ou depuis des comptes d'administrateur délégué. Cette fonctionnalité vous permet d'activer un accès root à court terme limité à des actions spécifiques, conformément au principe du moindre privilège.

Pour une gestion centralisée des informations d'identification root, vous devez activer les fonctionnalités de gestion des informations d'identification root et de sessions root au niveau de l'organisation à partir du compte de gestion de l'organisation ou d'un compte d'administrateur délégué. Conformément aux meilleures pratiques de la AWS SRA, nous déléguons cette

fonctionnalité au compte Security Tooling. Pour plus d'informations sur la configuration et l'utilisation de l'accès utilisateur root centralisé, consultez le billet AWS de blog sur la sécurité, Gestion centralisée de l'accès root pour les clients utilisateurs AWS Organizations.

IAM Identity Center

AWS IAM Identity Centerest un service de fédération d'identité qui vous aide à gérer de manière centralisée l'accès SSO à toutes vos charges de travail Comptes AWS, à vos principaux acteurs et au cloud. IAM Identity Center vous aide également à gérer l'accès et les autorisations aux applications logicielles en tant que service (SaaS) tierces couramment utilisées. Les fournisseurs d'identité s'intègrent à IAM Identity Center à l'aide de SAML 2.0. Le just-in-time provisionnement en masse et le provisionnement peuvent être effectués à l'aide du système de gestion des identités interdomaines (SCIM). IAM Identity Center peut également s'intégrer à des domaines Microsoft Active Directory (AD) sur site ou AWS gérés en tant que fournisseur d'identité grâce à l'utilisation de. AWS Directory Service IAM Identity Center inclut un portail utilisateur sur lequel vos utilisateurs finaux peuvent trouver et accéder au centre d'identité Comptes AWS IAM qui leur est attribué, aux rôles, aux applications cloud et aux applications personnalisées en un seul endroit.

IAM Identity Center s'intègre nativement au compte de gestion de l'organisation AWS Organizations et s'exécute dans celui-ci par défaut. Toutefois, pour exercer le moindre privilège et contrôler étroitement l'accès au compte de gestion, l'administration d'IAM Identity Center peut être déléguée à un compte de membre spécifique. Dans la AWS SRA, le compte Shared Services est le compte d'administrateur délégué d'IAM Identity Center. Avant d'activer l'administration déléguée pour IAM Identity Center, prenez en compte ces considérations. Vous trouverez plus d'informations sur la délégation dans la section relative au compte Shared Services. Même après avoir activé la délégation, IAM Identity Center doit toujours s'exécuter dans le compte de gestion de l'organisation pour effectuer certaines tâches liées à IAM Identity Center, notamment la gestion des ensembles d'autorisations fournis dans le compte de gestion de l'organisation.

Dans la console IAM Identity Center, les comptes sont affichés par leur unité d'organisation encapsulée. Cela vous permet de découvrir rapidement vos autorisations Comptes AWS, d'appliquer des ensembles courants d'autorisations et de gérer l'accès à partir d'un emplacement central.

IAM Identity Center inclut un magasin d'identité dans lequel les informations spécifiques des utilisateurs doivent être stockées. Cependant, IAM Identity Center ne doit pas nécessairement être la source officielle d'informations sur le personnel. Dans les cas où votre entreprise dispose déjà d'une source faisant autorité, IAM Identity Center prend en charge les types de fournisseurs d'identité suivants ()IdPs.

- Boutique d'identités IAM Identity Center : choisissez cette option si les deux options suivantes ne sont pas disponibles. Des utilisateurs sont créés, des attributions de groupes sont effectuées et des autorisations sont attribuées dans le magasin d'identités. Même si votre source officielle est externe à IAM Identity Center, une copie des principaux attributs sera stockée dans le magasin d'identités.
- Microsoft Active Directory (AD) : choisissez cette option si vous souhaitez continuer à gérer les utilisateurs dans votre annuaire dans Active Directory AWS Directory Service for Microsoft Active Directory ou dans votre annuaire autogéré dans Active Directory.
- Fournisseur d'identité externe : choisissez cette option si vous préférez gérer les utilisateurs dans un IdP externe basé sur SAML.

Vous pouvez compter sur un IdP existant déjà en place au sein de votre entreprise. Cela facilite la gestion de l'accès à plusieurs applications et services, car vous créez, gérez et révoquez l'accès à partir d'un seul emplacement. Par exemple, si quelqu'un quitte votre équipe, vous pouvez révoquer son accès à toutes les applications et à tous les services (y compris Comptes AWS) à partir d'un seul endroit. Cela réduit le besoin d'identifiants multiples et vous offre la possibilité de vous intégrer à vos processus de ressources humaines (RH).

> **Considération relative à la conception**
>
> Utilisez un IdP externe si cette option est disponible pour votre entreprise. Si votre IdP prend en charge le système de gestion des identités interdomaines (SCIM), profitez de la fonctionnalité SCIM d'IAM Identity Center pour automatiser le provisionnement des utilisateurs, des groupes et des autorisations (synchronisation). Cela permet à AWS l'accès de rester synchronisé avec le flux de travail de votre entreprise pour les nouvelles recrues, les employés qui passent à une autre équipe et les employés qui quittent l'entreprise. À tout moment, vous ne pouvez avoir qu'un seul annuaire ou un seul fournisseur d'identité SAML 2.0 connecté à IAM Identity Center. Vous pouvez toutefois passer à un autre fournisseur d'identité.

Conseiller d'accès IAM

Le conseiller d'accès IAM fournit des données de traçabilité sous la forme d'informations de dernier accès au service pour votre Comptes AWS et OUs. Utilisez ce contrôle de détective pour contribuer à la stratégie du moindre privilège. Pour les responsables IAM, vous pouvez consulter deux types

d'informations auxquelles vous avez accédé pour la dernière fois : les informations autorisées et Service AWS les informations relatives aux actions autorisées. Les informations comprennent la date et l'heure de la tentative.

L'accès IAM au sein du compte de gestion de l'organisation vous permet de consulter les données du dernier accès au service pour le compte de gestion de l'organisation, l'unité d'organisation, le compte membre ou la politique IAM de votre AWS organisation. Ces informations sont disponibles dans la console IAM du compte de gestion et peuvent également être obtenues par programmation en utilisant le conseiller APIs d'accès IAM AWS CLI ou un client programmatique. Les informations indiquent quels principaux d'une organisation ou d'un compte ont tenté pour la dernière fois d'accéder au service et quand. Les dernières informations consultées fournissent des informations sur l'utilisation réelle des services (voir des exemples de scénarios), ce qui vous permet de limiter les autorisations IAM aux seuls services réellement utilisés.

AWS Systems Manager

Configuration rapide et explorateur, qui sont des fonctionnalités de AWS Systems Manager, prennent en charge AWS Organizations et fonctionnent à partir du compte Org Management.

Quick Setup est une fonctionnalité d'automatisation de Systems Manager. Il permet au compte Org Management de définir facilement des configurations permettant à Systems Manager de s'engager en votre nom sur tous les comptes de votre AWS organisation. Vous pouvez activer la configuration rapide dans l'ensemble de votre AWS organisation ou choisir une option spécifique OUs. Quick Setup peut programmer AWS Systems Manager l'agent (agent SSM) pour exécuter des mises à jour bihebdomadaires sur vos instances EC2 et peut configurer une analyse quotidienne de ces instances afin d'identifier les correctifs manquants.

Explorer est un tableau de bord des opérations personnalisable qui fournit des informations sur vos AWS ressources. Explorer affiche une vue agrégée des données d'exploitation pour vos AWS comptes et pour l'ensemble de ceux-ci Régions AWS. Cela inclut les données relatives à vos instances EC2 et les détails de conformité des correctifs. Une fois que vous avez terminé la configuration intégrée (qui inclut également Systems Manager OpsCenter) AWS Organizations, vous pouvez agréger les données dans Explorer par unité d'organisation ou pour AWS l'ensemble d'une organisation. Systems Manager agrège les données dans le compte AWS Org Management avant de les afficher dans Explorer.

La section Workloads OU située plus loin dans ce guide décrit l'utilisation de l'agent SSM sur les instances EC2 du compte d'application.

AWS Control Tower

AWS Control Towerfournit un moyen simple de configurer et de gérer un AWS environnement multi-comptes sécurisé, appelé zone d'atterrissage. AWS Control Tower crée votre zone de landing zone en utilisant AWS Organizations et fournit une gestion et une gouvernance continues des comptes ainsi que les meilleures pratiques de mise en œuvre. Vous pouvez l'utiliser AWS Control Tower pour provisionner de nouveaux comptes en quelques étapes tout en vous assurant que les comptes sont conformes aux politiques de votre organisation. Vous pouvez même ajouter des comptes existants à un nouvel AWS Control Tower environnement.

AWS Control Tower dispose d'un ensemble de fonctionnalités large et flexible. L'une de ses fonctionnalités clés est sa capacité à orchestrer les capacités de plusieurs autres Services AWS, notamment AWS Organizations AWS Service Catalog, et d'IAM Identity Center, pour créer une zone d'atterrissage. Par exemple, par défaut, AWS Control Tower utilise AWS CloudFormation pour établir une base de référence, des politiques de contrôle des AWS Organizations services (SCPs) pour empêcher les modifications de configuration et des AWS Config Rules règles pour détecter en permanence les non-conformités. AWS Control Tower utilise des plans qui vous aident à aligner rapidement votre AWS environnement multi-comptes sur les principes de conception fondamentaux de AWS Well Architected en matière de sécurité. Parmi les fonctionnalités de gouvernance, elle AWS Control Tower propose des garde-fous qui empêchent le déploiement de ressources non conformes aux politiques sélectionnées.

Vous pouvez commencer à mettre en œuvre les directives AWS SRA avec AWS Control Tower. Par exemple, AWS Control Tower établit une AWS organisation avec l'architecture multi-comptes recommandée. Il fournit des plans pour assurer la gestion des identités, fournir un accès fédéré aux comptes, centraliser la journalisation, établir des audits de sécurité entre comptes, définir un flux de travail pour le provisionnement de nouveaux comptes et implémenter des lignes de base de comptes avec des configurations réseau.

Dans la AWS SRA, AWS Control Tower se trouve dans le compte de gestion de l'organisation, car il AWS Control Tower utilise ce compte pour configurer automatiquement une AWS organisation et désigne ce compte comme compte de gestion. Ce compte est utilisé pour la facturation au sein de votre AWS organisation. Il est également utilisé pour le provisionnement des comptes par Account Factory, pour gérer OUs et pour gérer les garde-fous. Si vous vous lancez AWS Control Tower dans une AWS organisation existante, vous pouvez utiliser le compte de gestion existant. AWS Control Tower utilisera ce compte comme compte de gestion désigné.

Considération relative à la conception

Si vous souhaitez définir une base de référence supplémentaire pour les contrôles et les configurations de vos comptes, vous pouvez utiliser les personnalisations pour AWS Control Tower (CfCT). Avec CfCT, vous pouvez personnaliser votre zone AWS Control Tower d'atterrissage à l'aide d'un CloudFormation modèle et SCPs. Vous pouvez déployer le modèle et les politiques personnalisés sur des comptes individuels et OUs au sein de votre organisation. CfCT s'intègre aux événements AWS Control Tower du cycle de vie pour garantir que les déploiements de ressources restent synchronisés avec votre zone d'atterrissage.

AWS Artifact

AWS Artifactfournit un accès à la demande aux rapports AWS de sécurité et de conformité et à certains accords en ligne. Les rapports disponibles AWS Artifact incluent des rapports sur les contrôles du système et de l'organisation (SOC), des rapports sur le secteur des cartes de paiement (PCI) et des certifications d'organismes d'accréditation de différentes zones géographiques et secteurs de conformité qui valident la mise en œuvre et l'efficacité opérationnelle des contrôles de AWS sécurité. AWS Artifact vous aide à effectuer votre due diligence AWS avec une transparence accrue dans notre environnement de contrôle de sécurité. Il vous permet également de surveiller en permanence la sécurité et la conformité AWS avec un accès immédiat aux nouveaux rapports.

AWS Artifact Les accords vous permettent de consulter, d'accepter et de suivre le statut des AWS accords tels que le Business Associate Addendum (BAA) pour un compte individuel et pour les comptes faisant partie de votre organisation. AWS Organizations

Vous pouvez fournir les artefacts AWS d'audit à vos auditeurs ou régulateurs comme preuve des contrôles de AWS sécurité. Vous pouvez également utiliser les conseils de responsabilité fournis par certains artefacts AWS d'audit pour concevoir votre architecture cloud. Ce guide permet de déterminer les contrôles de sécurité supplémentaires que vous pouvez mettre en place pour répondre aux cas d'utilisation spécifiques de votre système.

AWS Artifact est hébergé dans le compte Org Management afin de fournir un emplacement central où vous pouvez consulter, accepter et gérer les accords avec AWS. Cela est dû au fait que les accords acceptés sur le compte de gestion sont transférés vers les comptes des membres.

Considération relative à la conception

Les utilisateurs du compte Org Management doivent être limités à l'utilisation de la fonctionnalité Contrats de AWS Artifact et à rien d'autre. Pour mettre en œuvre la séparation des tâches, AWS Artifact il est également hébergé dans le compte Security Tooling, où vous pouvez déléguer des autorisations à vos parties prenantes chargées de la conformité et à des auditeurs externes pour accéder aux artefacts d'audit. Vous pouvez implémenter cette séparation en définissant des politiques d'autorisation IAM précises. Pour des exemples, consultez la section Exemples de politiques IAM dans la AWS documentation.

Garde-corps de service de sécurité distribués et centralisés

Dans le AWS SRA, Amazon AWS Security Hub AWS Security Hub CSPM, IAM Access Analyzer GuardDuty AWS Config, les traces d' AWS CloudTrail organisation, et souvent Amazon Macie, sont déployées avec un ensemble de garde-fous délégués approprié entre les comptes et fournissent également une surveillance, une gestion et une gouvernance centralisées au sein de votre organisation. AWS Vous trouverez ce groupe de services dans tous les types de comptes représentés dans la AWS SRA. Ils doivent faire partie de ceux Services AWS qui doivent être fournis dans le cadre du processus d'intégration et de définition de base de votre compte. Le référentiel de GitHub code fournit un exemple de mise en œuvre de services AWS axés sur la sécurité sur vos comptes, y compris le compte AWS Org Management.

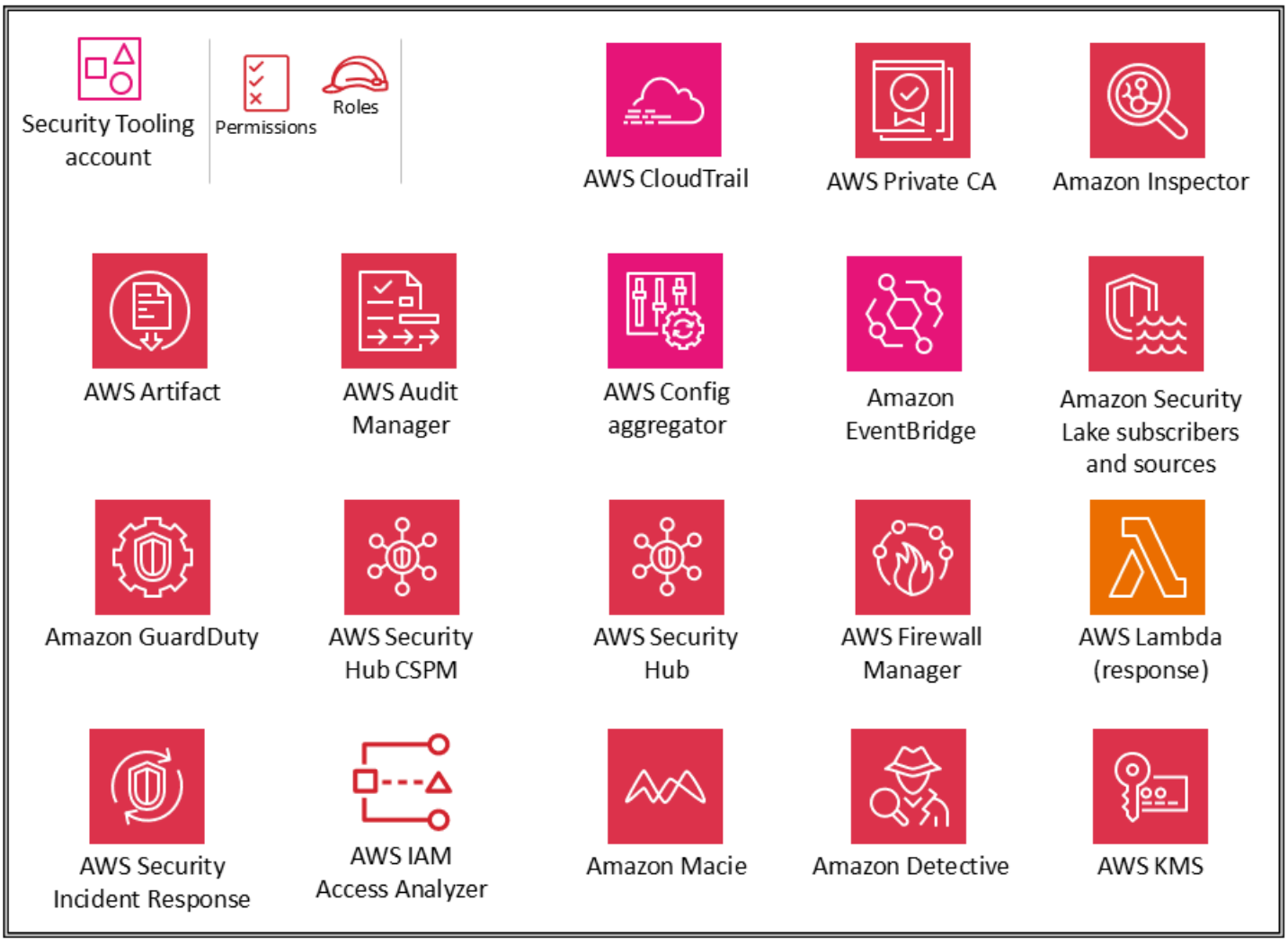
Outre ces services, AWS SRA inclut deux services axés sur la sécurité, Amazon Detective et AWS Audit Manager, qui prennent en charge l'intégration et les fonctionnalités d'administration déléguée dans. AWS Organizations Toutefois, ils ne sont pas inclus dans les services recommandés pour l'établissement des bases de référence des comptes. Nous avons constaté que ces services sont mieux utilisés dans les scénarios suivants :

- Vous disposez d'une équipe ou d'un groupe de ressources dédié qui exécute ces fonctions de criminalistique numérique et d'audit informatique. Detective est la solution idéale pour les équipes d'analystes de sécurité, et Audit Manager est utile à vos équipes d'audit interne ou de conformité.
- Vous souhaitez vous concentrer sur un ensemble d'outils de base tels qu' AWS Config Amazon GuardDuty et AWS Security Hub CSPM au début de votre projet, puis vous appuyer sur ceux-ci en utilisant des services offrant des fonctionnalités supplémentaires. AWS Security Hub

Security OU — Compte Security Tooling

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le schéma suivant illustre les services AWS de sécurité configurés dans le compte Security Tooling.



Le compte Security Tooling est dédié à l'exploitation des services de sécurité, à la surveillance Comptes AWS et à l'automatisation des alertes et réponses de sécurité. Les objectifs de sécurité sont notamment les suivants :

- Fournissez un compte dédié avec un accès contrôlé pour gérer l'accès aux garde-fous de sécurité, à la surveillance et à la réponse.

- Maintenez l'infrastructure de sécurité centralisée appropriée pour surveiller les données relatives aux opérations de sécurité et garantir la traçabilité. La détection, l'investigation et la réponse sont des éléments essentiels du cycle de vie de la sécurité et peuvent être utilisées pour soutenir un processus de qualité, une obligation légale ou de conformité, ainsi que pour l'identification des menaces et les efforts de réponse.
- Soutenez davantage la stratégie de defense-in-depth l'entreprise en maintenant un niveau de contrôle supplémentaire sur la configuration et les opérations de sécurité appropriées, telles que les clés de chiffrement et les paramètres des groupes de sécurité. Il s'agit d'un compte sur lequel travaillent les opérateurs de sécurité. Les rôles en lecture seule/d'audit permettant de consulter les informations à AWS l'échelle de l'organisation sont typiques, tandis que les write/modify rôles sont limités en nombre, étroitement contrôlés, surveillés et enregistrés.

Considérations relatives à la conception

- AWS Control Tower nomme le compte sous l'unité d'organisation de sécurité le compte d'audit par défaut. Vous pouvez renommer le compte lors de la AWS Control Tower configuration.
- Il peut être approprié de disposer de plusieurs comptes Security Tooling. Par exemple, la surveillance et la réponse aux événements de sécurité sont souvent confiées à une équipe dédiée. La sécurité du réseau peut justifier son propre compte et ses propres rôles en collaboration avec l'infrastructure cloud ou l'équipe réseau. Ces divisions conservent l'objectif de séparer les enclaves de sécurité centralisées et mettent davantage l'accent sur la séparation des tâches, le moindre privilège et la simplicité potentielle des affectations des équipes. Si vous en utilisez AWS Control Tower, cela limite la création d'éléments supplémentaires dans le Comptes AWS cadre de l'unité d'organisation de sécurité.

Administrateur délégué pour les services de sécurité

Le compte Security Tooling sert de compte administrateur pour les services de sécurité gérés dans une administrator/member structure intégrée à l'ensemble du Comptes AWS. Comme indiqué précédemment, cela est géré par le biais de la fonctionnalité d'administrateur AWS Organizations délégué. Les services de la AWS SRA qui prennent actuellement en charge l'administrateur délégué incluent la gestion centralisée IAM de l'accès root, AWS Config,, AWS Firewall Manager Amazon GuardDuty, IAM Access Analyzer, Amazon Macie,, AWS Security Hub, Amazon

Detective, AWS Security Hub CSPM AWS Audit Manager Amazon Inspector et. AWS CloudTrail AWS Systems Manager Votre équipe de sécurité gère les fonctionnalités de sécurité de ces services et surveille tous les événements ou découvertes spécifiques à la sécurité.

AWS IAM Identity Center prend en charge l'administration déléguée d'un compte membre. AWS SRA utilise le compte Shared Services comme compte d'administrateur délégué pour IAM Identity Center, comme expliqué plus loin dans la section IAM Identity Center du compte Shared Services.

Accès root centralisé

Le compte Security Tooling est le compte d'administrateur délégué pour la gestion centralisée IAM de la capacité d'accès root. Cette fonctionnalité doit être activée au niveau de l'organisation en activant la gestion des informations d'identification et l'action root privilégiée dans les comptes des membres. Les administrateurs délégués doivent disposer d'`sts:AssumeRoot`autorisations explicites pour pouvoir effectuer des actions root privilégiées au nom des comptes membres. Cette autorisation n'est disponible qu'une fois que l'action root privilégiée sur un compte membre est activée dans le compte de gestion de l'organisation ou dans le compte d'administrateur délégué. Avec cette autorisation, les utilisateurs peuvent effectuer des tâches d'utilisateur root privilégié sur les comptes membres, de manière centralisée depuis le compte Security Tooling. Après avoir lancé une session privilégiée, vous pouvez supprimer une politique de compartiment S3 mal configurée, supprimer une politique de file d'attente SQS mal configurée, supprimer les informations d'identification de l'utilisateur root pour un compte membre et réactiver les informations d'identification de l'utilisateur root pour un compte membre. Vous pouvez effectuer ces actions depuis la console, en utilisant le AWS Command Line Interface (AWS CLI) ou via APIs.

AWS CloudTrail

AWS CloudTrailest un service qui prend en charge la gouvernance, la conformité et l'audit des activités de votre entreprise Compte AWS. Vous pouvez ainsi enregistrer, surveiller en permanence et conserver l'activité du compte liée aux actions menées au sein de votre AWS infrastructure. CloudTrail CloudTrail est intégré à AWS Organizations, et cette intégration peut être utilisée pour créer un suivi unique qui enregistre tous les événements pour tous les comptes de l' AWS organisation. Cet élément est appelé journal de suivi d'une organisation. Vous pouvez créer et gérer un journal d'organisation uniquement depuis le compte de gestion de l'organisation ou depuis un compte d'administrateur délégué. Lorsque vous créez un journal d'organisation, un suivi portant le nom que vous spécifiez est créé dans chaque Compte AWS journal appartenant à votre AWS organisation. Le journal enregistre l'activité de tous les comptes, y compris le compte de gestion, de l' AWS organisation et stocke les journaux dans un seul compartiment S3. En raison de la sensibilité

de ce compartiment S3, vous devez le sécuriser en suivant les meilleures pratiques décrites dans la section Amazon S3 en tant que magasin de journaux central plus loin dans ce guide. Tous les comptes de l' AWS organisation peuvent voir le parcours de l'organisation dans leur liste de sentiers. Toutefois, les membres Comptes AWS ont un accès en lecture seule à cette randonnée. Par défaut, lorsque vous créez un parcours d'organisation dans la CloudTrail console, il s'agit d'un parcours multirégional. Pour plus d'informations sur les meilleures pratiques en matière de sécurité, consultez la CloudTraildocumentation.

Dans le AWS SRA, le compte Security Tooling est le compte d'administrateur délégué pour la gestion. CloudTrail Le compartiment S3 correspondant pour stocker les journaux de suivi de l'organisation est créé dans le compte Log Archive. Il s'agit de séparer la gestion et l'utilisation des privilèges de CloudTrail journalisation. Pour plus d'informations sur la création ou la mise à jour d'un compartiment S3 pour stocker les fichiers journaux d'un journal d'entreprise, consultez la CloudTrail documentation. En matière de sécurité, il est recommandé d'ajouter la clé de `aws:SourceArn` condition du journal de l'organisation à la politique de ressources du compartiment S3 (et à toute autre ressource telle que les clés KMS ou les rubriques SNS). Cela garantit que le compartiment S3 accepte uniquement les données associées au parcours spécifique. Le journal est configuré avec la validation du fichier journal pour la validation de l'intégrité du fichier journal. Les fichiers log et digest sont chiffrés à l'aide de SSE-KMS. Le journal de l'organisation est également intégré à un groupe de CloudWatch journaux dans Logs pour envoyer des événements à conserver à long terme.

> **Note**
>
> Vous pouvez créer et gérer des traces d'organisation à partir de comptes de gestion et d'administrateur délégué. Toutefois, il est recommandé de limiter l'accès au compte de gestion et d'utiliser la fonctionnalité d'administrateur délégué lorsqu'elle est disponible.

> **Considérations relatives à la conception**
>
> - CloudTrail n'enregistre pas les événements liés aux données par défaut, car il s'agit souvent d'activités à volume élevé. Cependant, vous devez capturer les événements de données pour des AWS ressources critiques spécifiques telles que les compartiments S3, les fonctions Lambda, les événements de journal provenant de AWS l'extérieur qui sont envoyés au lac et CloudTrail les rubriques SNS. Pour ce faire, configurez le journal de votre organisation pour inclure les événements de données provenant de ressources spécifiques en spécifiant les ressources individuelles ARNs de chaque ressource.

- Si un compte membre a besoin d'accéder aux fichiers CloudTrail journaux pour son propre compte, vous pouvez partager de manière sélective les fichiers CloudTrail journaux de l'organisation à partir du compartiment S3 central. Toutefois, si les comptes membres nécessitent des groupes de CloudWatch journaux Amazon locaux pour les CloudTrail journaux de leur compte ou souhaitent configurer la gestion des journaux et les événements de données (lecture seule, écriture seule, événements de gestion, événements de données) différemment du journal de l'organisation, ils peuvent créer un journal local avec les contrôles appropriés. Les sentiers spécifiques au compte local entraînent des frais supplémentaires.

AWS Security Hub CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM), anciennement connu sous le nom de Cloud Security Posture Management () AWS Security Hub, vous fournit une vue complète de votre posture de sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub CSPM collecte des données de sécurité provenant de services AWS intégrés, de produits tiers pris en charge et d'autres produits de sécurité personnalisés que vous pourriez utiliser. Il vous aide à surveiller et à analyser en permanence les tendances en matière de sécurité et à identifier les problèmes de sécurité prioritaires. Outre les sources ingérées, Security Hub CSPM génère ses propres résultats, qui sont représentés par des contrôles de sécurité correspondant à une ou plusieurs normes de sécurité. Ces normes incluent les meilleures pratiques de sécurité AWS fondamentales (FSBP), le Center for Internet Security (CIS) AWS Foundations Benchmark v1.20 et v1.4.0, le National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5, la norme de sécurité des données du secteur des cartes de paiement (PCI DSS) et les normes de gestion des services. Pour obtenir une liste des normes de sécurité actuelles et des informations sur les contrôles de sécurité spécifiques, consultez la référence aux normes pour Security Hub CSPM dans la documentation de Security Hub CSPM.

Security Hub CSPM s'intègre AWS Organizations pour simplifier la gestion du niveau de sécurité de tous les comptes existants et futurs de votre AWS organisation. Vous pouvez utiliser la fonctionnalité de configuration centrale du Security Hub CSPM depuis le compte administrateur délégué (dans ce cas, Security Tooling) pour spécifier comment le service Security Hub CSPM, les normes de sécurité et les contrôles de sécurité sont configurés dans les comptes et les unités organisationnelles () de votre organisation dans toutes les régions. OUs Vous pouvez configurer ces paramètres en quelques étapes à partir d'une région principale, appelée région d'origine. Si vous n'utilisez pas

la configuration centralisée, vous devez configurer Security Hub CSPM séparément dans chaque compte et région. L'administrateur délégué peut désigner des OUs comptes autogérés, où le membre peut configurer les paramètres séparément dans chaque région, ou des comptes gérés de manière centralisée, où l'administrateur délégué peut configurer le compte du membre ou l'unité d'organisation dans toutes les régions. Vous pouvez désigner tous les OUs comptes de votre organisation comme étant gérés de manière centralisée, tous autogérés ou une combinaison des deux. Cela simplifie l'application d'une configuration cohérente tout en offrant la flexibilité de la modifier pour chaque unité d'organisation et chaque compte.

Le compte administrateur délégué CSPM de Security Hub peut également consulter les résultats, consulter les informations et contrôler les détails de tous les comptes membres. Vous pouvez également désigner une région d'agrégation au sein du compte administrateur délégué afin de centraliser vos résultats entre vos comptes et les régions associées. Vos résultats sont synchronisés de manière continue et bidirectionnelle entre la région agrégatrice et toutes les autres régions.

Security Hub CSPM prend en charge les intégrations avec plusieurs. Services AWS Amazon GuardDuty AWS Config, Amazon Macie, IAM Access Analyzer, Amazon AWS Firewall Manager Inspector, Amazon Route 53 Resolver DNS Firewall et AWS Systems Manager Patch Manager peuvent transmettre les résultats à Security Hub CSPM. Security Hub CSPM traite les résultats en utilisant un format standard appelé AWS Security Finding Format (ASFF). Security Hub CSPM met en corrélation les résultats des produits intégrés afin de prioriser les plus importants. Vous pouvez enrichir les métadonnées des résultats du Security Hub CSPM pour mieux contextualiser, hiérarchiser et prendre les mesures nécessaires en fonction des résultats de sécurité. Cet enrichissement ajoute des balises de ressource, une nouvelle balise d' AWS application et des informations de nom de compte à chaque découverte ingérée dans Security Hub CSPM. Cela vous permet d'affiner les résultats pour les règles d'automatisation, de rechercher ou de filtrer les résultats et les informations, et d'évaluer l'état du niveau de sécurité par application. En outre, vous pouvez utiliser des règles d'automatisation pour mettre à jour automatiquement les résultats. Lorsque Security Hub CSPM ingère des résultats, il peut appliquer diverses règles, telles que la suppression des résultats, la modification de leur gravité et l'ajout de notes aux résultats. Ces actions de règle prennent effet lorsque les résultats correspondent aux critères que vous avez spécifiés, tels que la ressource ou IDs le compte auquel le résultat est associé, ou son titre. Vous pouvez utiliser des règles d'automatisation pour mettre à jour certains champs de recherche dans l'ASFF. Les règles s'appliquent à la fois aux nouvelles découvertes et aux mises à jour.

Au cours de l'enquête sur un événement de sécurité, vous pouvez accéder de Security Hub CSPM à Amazon Detective pour rechercher un GuardDuty résultat. Security Hub CSPM recommande

d'aligner les comptes d'administrateur délégué pour des services tels que Detective (lorsqu'ils existent) pour une intégration plus fluide. Par exemple, si vous n'alignez pas les comptes d'administrateur entre Detective et Security Hub CSPM, la navigation entre les résultats et Detective ne fonctionnera pas. Pour obtenir une liste complète, consultez la section Présentation des Service AWS intégrations avec Security Hub CSPM dans la documentation de Security Hub CSPM.

Vous pouvez utiliser Security Hub CSPM avec la fonctionnalité Network Access Analyzer d'Amazon VPC pour surveiller en permanence la conformité de votre configuration réseau. AWS Cela vous aidera à bloquer les accès indésirables au réseau et à empêcher l'accès externe à vos ressources critiques. Pour plus de détails sur l'architecture et la mise en œuvre, consultez le billet de AWS blog Vérification continue de la conformité du réseau à l'aide d'Amazon VPC Network Access Analyzer et. AWS Security Hub CSPM

Outre ses fonctionnalités de surveillance, Security Hub CSPM prend en charge l'intégration avec Amazon EventBridge afin d'automatiser la correction de résultats spécifiques. Vous pouvez définir des actions personnalisées à effectuer lors de la réception d'un résultat. Vous pouvez, par exemple, configurer des actions personnalisées, pour envoyer des conclusions à un système de tickets ou à un système de correction automatique. Pour des discussions et des exemples supplémentaires, consultez les articles de AWS blog Réponse et correction automatisées avec AWS Security Hub CSPM et Comment déployer la AWS solution pour la réponse et la correction automatisées de Security Hub CSPM.

Security Hub CSPM utilise des liens de service AWS Config Rules pour effectuer la plupart de ses contrôles de sécurité. Pour prendre en charge ces contrôles, AWS Config ils doivent être activés sur tous les comptes, y compris le compte administrateur (ou administrateur délégué) et les comptes membres, dans chacun des comptes où le Security Région AWS Hub CSPM est activé.

Considérations relatives à la conception

- Si une norme de conformité, telle que PCI-DSS, est déjà présente dans Security Hub CSPM, le service Security Hub CSPM entièrement géré est le moyen le plus simple de la rendre opérationnelle. Toutefois, si vous souhaitez élaborer votre propre norme de conformité ou de sécurité, qui peut inclure des contrôles de sécurité, d'exploitation ou d'optimisation des coûts, les packs de AWS Config conformité proposent un processus de personnalisation simplifié. (Pour plus d'informations sur les packs de conformité AWS Config et les packs de conformité, consultez la AWS Configsection.)
- Les cas d'utilisation courants de Security Hub CSPM sont les suivants :

- En tant que tableau de bord offrant aux propriétaires d'applications une visibilité sur le niveau de sécurité et de conformité de leurs AWS ressources
- En tant que vue centrale des résultats de sécurité utilisés par les opérations de sécurité, les intervenants en cas d'incident et les chasseurs de menaces pour trier les résultats de AWS sécurité et de conformité et prendre des mesures en conséquence dans les différentes régions Comptes AWS
- Pour agréger et acheminer les résultats de sécurité et de conformité provenant de différentes Comptes AWS régions, vers un système centralisé de gestion des informations et des événements de sécurité (SIEM) ou un autre système d'orchestration de sécurité

Pour obtenir des conseils supplémentaires sur ces cas d'utilisation, notamment sur la manière de les configurer, consultez le billet de blog Three Recurrent Security Hub CSPM use patterns and how to deploy them.

Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation de Security Hub CSPM. Cela inclut l'activation automatique du service, l'administration déléguée à un compte membre (Security Tooling) et la configuration pour activer Security Hub CSPM pour tous les comptes existants et futurs de l'organisation. AWS

AWS Security Hub

AWS Security Hubest une solution de sécurité cloud unifiée qui hiérarchise vos menaces de sécurité critiques et vous aide à y répondre à grande échelle. Security Hub détecte les problèmes de sécurité en temps quasi réel en corrélant et en enrichissant automatiquement les signaux de sécurité provenant de sources multiples, telles que la gestion de la posture (AWS Security Hub CSPM), la gestion des vulnérabilités (Amazon Inspector), les données sensibles (Amazon Macie) et la détection des menaces (Amazon). GuardDuty Cela permet aux équipes de sécurité de hiérarchiser les risques actifs dans leurs environnements cloud grâce à des analyses automatisées et à des informations contextuelles. Security Hub fournit une représentation visuelle de la trajectoire d'attaque potentielle que les attaquants peuvent exploiter pour accéder aux ressources associées à une découverte

d'exposition. Cela transforme les signaux de sécurité complexes en informations exploitables, afin que vous puissiez prendre rapidement des décisions éclairées concernant votre sécurité.

Security Hub a été repensé de manière stratégique afin de simplifier l'activation des éléments constitutifs des services de sécurité associés afin d'obtenir des résultats en matière de sécurité. En corrélant les résultats de sécurité dans une matrice de menaces entre différents signaux de sécurité en temps quasi réel, vous pouvez d'abord hiérarchiser les risques les plus critiques. Les résultats sont corrélés afin de détecter l'exposition associée aux AWS ressources. Les expositions représentent des faiblesses plus générales en matière de contrôles de sécurité, de mauvaises configurations ou d'autres domaines susceptibles d'être exploités par des menaces actives. Par exemple, une exposition peut être une instance EC2 accessible depuis Internet et présentant des vulnérabilités logicielles présentant une forte probabilité d'exploitation.

Security Hub et Security Hub CSPM sont des services complémentaires. Security Hub CSPM fournit une vue complète de votre niveau de sécurité et vous aide à évaluer votre environnement cloud par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub fournit une expérience unifiée qui vous aide à hiérarchiser les problèmes de sécurité critiques et à y répondre. Les résultats du Security Hub CSPM sont automatiquement acheminés vers Security Hub, où ils sont corrélés aux résultats d'autres services de sécurité, tels qu'Amazon Inspector, afin de générer des risques. Cela vous permet d'identifier les risques les plus critiques de votre environnement.

Security Hub fournit également un résumé des ressources de votre AWS environnement par type et les résultats associés. Les ressources sont hiérarchisées en fonction des expositions et des séquences d'attaque. Lorsque vous choisissez un type de ressource, vous pouvez consulter toutes les ressources associées à ce type de ressource.

Pour une expérience optimale, nous recommandons d'activer Security Hub et Security Hub CSPM, ainsi que les autres services de sécurité suivants : Amazon GuardDuty, Amazon Inspector et Amazon Macie. Vous pouvez savoir si ces services et fonctionnalités sont activés de manière uniforme sur tous les comptes membres de votre organisation en utilisant les résultats de Security Hub Coverage.

Dans le AWS SRA, le compte Security Tooling agit en tant qu'administrateur délégué pour Security Hub, Security Hub CSPM et d'autres services de sécurité. AWS Dans le compte Security Tooling, vous pouvez consulter toutes les ressources associées aux comptes des membres. Vous pouvez également consulter toutes les ressources de votre maison Région AWS à partir de liens Régions AWS.

Note de mise en œuvre

L'activation de Security Hub nécessite trois étapes, notamment des procédures permettant de déterminer si vous avez déjà activé Security Hub CSPM. Security Hub est intégré de manière native AWS Organizations, ce qui simplifie le processus de configuration et de mise en œuvre, centralise et regroupe tous les résultats en un seul endroit. Conformément aux bonnes pratiques de la AWS SRA, utilisez le compte Security Tooling comme compte d'administrateur délégué pour gérer et configurer Security Hub. Utilisez les paramètres de configuration du Security Hub pour activer automatiquement toutes les régions et tous les comptes, y compris les futures régions et comptes. OUs Vous devez également configurer l'agrégation entre régions pour regrouper les résultats, les ressources et les tendances provenant de plusieurs régions Régions AWS dans une seule région d'origine. Lors de la configuration, vous pouvez également activer toutes les intégrations natives telles que Jira Cloud ou. ServiceNow

Considérations relatives à la conception

- Les résultats du Security Hub sont formatés dans le cadre de l'Open Cybersecurity Schema Framework (OCSF). Security Hub génère des résultats dans OCSF et reçoit les résultats dans OCSF de Security Hub CSPM et d'autres entités. Services AWS Ces résultats de l'OCSF peuvent être envoyés via Amazon à des EventBridge fins d'automatisation ou stockés dans un compte d'agrégation de journaux central pour effectuer une analyse et une conservation des journaux de sécurité.
- Le compte AWS Org Management ne peut pas se désigner comme administrateur délégué dans Security Hub. Cela correspond à la meilleure pratique de la AWS SRA qui consiste à désigner le compte Security Tooling en tant qu'administrateur délégué. Notez également :
  - Le compte administrateur désigné pour Security Hub CSPM devient automatiquement l'administrateur désigné pour Security Hub.
  - La suppression de l'administration déléguée via Security Hub supprime également l'administration déléguée pour Security Hub CSPM. De même, la suppression de l'administration déléguée via Security Hub CSPM la supprime également pour Security Hub.

- Security Hub inclut des fonctionnalités qui modifient automatiquement les résultats et prennent des mesures en fonction de vos spécifications. Security Hub prend en charge les types d'automatisations suivants :
  - Règles d'automatisation, qui mettent automatiquement à jour les résultats, suppriment les résultats et envoient les résultats aux outils de billetterie en temps quasi réel sur la base de critères définis.
  - Réponse et correction automatisées, qui créent des EventBridge règles personnalisées qui définissent les actions automatiques à entreprendre en fonction de résultats et d'informations spécifiques.
- Security Hub peut configurer Amazon Inspector pour tous les comptes membres et régions par le biais de politiques, et peut configurer GuardDuty le CSPM de Security Hub pendant le déploiement. Les politiques génèrent des AWS Organizations politiques pour les comptes et les régions. Les déploiements sont des actions ponctuelles qui activent une fonctionnalité de sécurité sur des comptes et des régions sélectionnés. Les déploiements ne s'appliquent pas aux comptes nouvellement activés. Vous pouvez également activer automatiquement les fonctionnalités pour les nouveaux comptes membres dans GuardDuty Security Hub CSPM.

Amazon GuardDuty

Amazon GuardDuty est un service de détection des menaces qui surveille en permanence les activités malveillantes et les comportements non autorisés afin de protéger votre charge de travail Comptes AWS et celle de vos charges de travail. Vous devez toujours capturer et stocker les journaux appropriés à des fins de surveillance et d'audit, mais vous devez GuardDuty extraire des flux de données indépendants directement à partir AWS CloudTrail des journaux de flux Amazon VPC et des journaux AWS DNS. Vous n'avez pas à gérer les politiques relatives aux compartiments Amazon S3 ni à modifier la façon dont vous collectez et stockez vos journaux. GuardDutyles autorisations sont gérées comme des rôles liés à un service que vous pouvez révoquer à tout moment en les désactivant. GuardDuty Cela facilite l'activation du service sans configuration complexe et élimine le risque qu'une modification des autorisations IAM ou une modification de la politique du compartiment S3 affecte le fonctionnement du service.

En plus de fournir des sources de données de base, GuardDuty fournit des fonctionnalités facultatives pour identifier les résultats de sécurité. Il s'agit notamment de la protection EKS, de la protection RDS, de la protection S3, de la protection contre les logiciels malveillants et de la

protection Lambda. Pour les nouveaux détecteurs, ces fonctionnalités optionnelles sont activées par défaut, à l'exception de la protection EKS, qui doit être activée manuellement.

- Avec GuardDuty S3 Protection, GuardDuty surveille les événements liés aux données Amazon S3 CloudTrail en plus des événements de CloudTrail gestion par défaut. La surveillance des événements liés aux données permet GuardDuty de surveiller les opérations d'API au niveau des objets afin de détecter les risques de sécurité potentiels pour les données de vos compartiments S3.
- GuardDuty Malware Protection détecte la présence de malwares sur les instances Amazon EC2 ou les charges de travail des conteneurs en lançant des scans sans agent sur les volumes Amazon Elastic Block Store (Amazon EBS) connectés. GuardDuty détecte également les malwares potentiels dans les compartiments S3 en scannant les objets récemment chargés ou les nouvelles versions d'objets existants.
- GuardDuty La protection RDS est conçue pour profiler et surveiller les activités d'accès aux bases de données Amazon Aurora sans affecter les performances des bases de données.
- GuardDuty La protection EKS inclut la surveillance du journal d'audit EKS et la surveillance du temps d'exécution EKS. Avec EKS Audit Log Monitoring, GuardDuty surveille les journaux d'audit Kubernetes des clusters Amazon EKS et les analyse pour détecter toute activité potentiellement malveillante et suspecte. EKS Runtime Monitoring utilise l'agent de GuardDuty sécurité (qui est un module complémentaire Amazon EKS) pour fournir une visibilité de l'exécution sur les charges de travail Amazon EKS individuelles. L'agent GuardDuty de sécurité aide à identifier les conteneurs spécifiques au sein de vos clusters Amazon EKS qui sont potentiellement compromis. Il peut également détecter les tentatives d'augmentation des privilèges d'un conteneur individuel vers l'hôte Amazon EC2 sous-jacent ou vers un environnement plus large. AWS

GuardDuty fournit également une fonctionnalité connue sous le nom de détection étendue des menaces qui détecte automatiquement les attaques en plusieurs étapes couvrant des sources de données, plusieurs types de AWS ressources et le temps passé au cours d'un Compte AWS. GuardDutymet en corrélation ces événements, appelés signaux, afin d'identifier les scénarios qui se présentent comme des menaces potentielles pour votre AWS environnement, puis génère une recherche de séquence d'attaque. Cela couvre les scénarios de menace impliquant une compromission liée à une utilisation abusive des AWS informations d'identification et des tentatives de compromission des données dans votre entreprise Comptes AWS. GuardDuty considère tous les types de recherche de séquences d'attaque comme critiques. Cette fonctionnalité est activée par défaut et aucun coût supplémentaire n'y est associé.

Dans le AWS SRA, GuardDuty il est activé dans tous les comptes via le compte administrateur GuardDuty délégué (dans ce cas AWS Organizations, le compte Security Tooling), et toutes les conclusions sont consultables et exploitables par les équipes de sécurité appropriées. GuardDuty les résultats actifs sont exportés vers un compartiment S3 central dans le compte Log Archive, afin que vous puissiez conserver les résultats au-delà de 90 jours. Les résultats sont exportés depuis le compte d'administrateur délégué et incluent également tous les résultats des comptes de membres associés dans la même région. Les résultats contenus dans le compartiment S3 sont chiffrés à l'aide d'une clé gérée par le AWS KMS client. La politique du compartiment S3 et la politique des clés KMS sont configurées GuardDuty pour autoriser uniquement l'utilisation des ressources.

Lorsque cette option AWS Security Hub CSPM est activée, GuardDuty les résultats sont automatiquement transmis à Security Hub CSPM et Security Hub. Lorsque Amazon Detective est activé, GuardDuty les résultats sont inclus dans le processus d'ingestion du journal Detective. GuardDuty et Detective prennent en charge les flux de travail utilisateur multiservices, où GuardDuty vous trouverez des liens depuis la console qui vous redirigent depuis une découverte sélectionnée vers une page Detective contenant un ensemble de visualisations sélectionnées pour étudier cette constatation. Par exemple, vous pouvez également intégrer GuardDuty Amazon EventBridge pour automatiser les meilleures pratiques GuardDuty, telles que l'automatisation des réponses aux nouvelles GuardDuty découvertes.

> **Exemple de mise en œuvre**
>
> La bibliothèque de code AWS SRA fournit un exemple d'implémentation de GuardDuty. Il inclut la configuration chiffrée du compartiment S3, l'administration déléguée et l' GuardDuty activation de tous les comptes existants et futurs de l' AWS organisation.

AWS Config

AWS Configest un service qui vous permet d'évaluer, d'auditer et d'évaluer les configurations des AWS ressources prises en charge dans votre Comptes AWS. AWS Config surveille et enregistre en permanence les configurations AWS des ressources, et évalue automatiquement les configurations enregistrées par rapport aux configurations souhaitées. Vous pouvez également intégrer AWS Config d'autres services pour effectuer le gros du travail dans les pipelines d'audit et de surveillance automatisés. Par exemple, AWS Config peut surveiller les modifications apportées à des secrets individuels dans AWS Secrets Manager.

Vous pouvez évaluer les paramètres de configuration de vos AWS ressources en utilisant AWS Config Rules. AWS Config fournit une bibliothèque de règles prédéfinies personnalisables appelées règles gérées, ou vous pouvez écrire vos propres règles personnalisées. Vous pouvez exécuter AWS Config Rules en mode proactif (avant le déploiement des ressources) ou en mode détective (après le déploiement des ressources). Les ressources peuvent être évaluées lors de changements de configuration, selon un calendrier périodique, ou les deux.

Un pack de conformité est un ensemble de AWS Config règles et d'actions correctives qui peuvent être déployées en tant qu'entité unique dans un compte et une région, ou au sein d'une organisation dans. AWS Organizations Les packs de conformité sont créés en créant un modèle YAML qui contient la liste des règles AWS Config gérées ou personnalisées et des actions correctives. Pour commencer à évaluer votre AWS environnement, utilisez l'un des exemples de modèles de pack de conformité.

AWS Config s'intègre AWS Security Hub CSPM à Security Hub CSPM pour envoyer les résultats des évaluations de règles AWS Config gérées et personnalisées sous forme de conclusions.

AWS Config Rules peut être utilisé conjointement avec AWS Systems Manager pour remédier efficacement aux ressources non conformes. Vous utilisez Systems Manager Explorer pour recueillir l'état de conformité des AWS Config règles de votre Comptes AWS cross, Régions AWS puis vous utilisez les documents d'automatisation de Systems Manager (runbooks) pour résoudre vos règles non conformes AWS Config . Pour plus de détails sur la mise en œuvre, consultez le billet de blog Corriger les AWS Config règles non conformes avec les runbooks AWS Systems Manager d'automatisation.

L' AWS Config agrégateur collecte les données de configuration et de conformité sur plusieurs comptes, régions et organisations au sein AWS Organizations de. Le tableau de bord de l'agrégateur affiche les données de configuration des ressources agrégées. Les tableaux de bord d'inventaire et de conformité fournissent des informations essentielles et actuelles sur la configuration de vos AWS ressources et l'état de conformité au sein d'une AWS organisation Comptes AWS, au sein de Régions AWS celle-ci ou au sein de celle-ci. Ils vous permettent de visualiser et d'évaluer votre inventaire de AWS ressources sans avoir à rédiger de requêtes AWS Config avancées. Vous pouvez obtenir des informations essentielles, telles qu'un résumé de la conformité par ressources, les 10 principaux comptes dont les ressources ne sont pas conformes, une comparaison des instances EC2 en cours d'exécution et arrêtées par type, et des volumes EBS par type et taille de volume.

Si vous l'utilisez AWS Control Tower pour gérer votre AWS organisation, celle-ci déploiera un ensemble de AWS Config règles servant de garde-fous (classées comme obligatoires, fortement

recommandées ou facultatives). Ces garde-fous vous aident à gérer vos ressources et à contrôler la conformité des comptes de votre AWS organisation. Ces AWS Config règles utiliseront automatiquement une `aws-control-tower` balise dont la valeur est de`managed-by-control-tower`.

AWS Config doit être activé pour chaque compte membre de l' AWS organisation et Région AWS contenant les ressources que vous souhaitez protéger. Vous pouvez gérer de manière centralisée (par exemple, créer, mettre à jour et supprimer) les AWS Config règles de tous les comptes de votre AWS organisation. À partir du compte d'administrateur AWS Config délégué, vous pouvez déployer un ensemble commun de AWS Config règles pour tous les comptes et spécifier les comptes pour lesquels AWS Config les règles ne doivent pas être créées. Le compte d'administrateur AWS Config délégué peut également agréger les données de configuration et de conformité des ressources provenant de tous les comptes membres afin de fournir une vue unique. Utilisez le compte APIs de l'administrateur délégué pour renforcer la gouvernance en vous assurant que les AWS Config règles sous-jacentes ne peuvent pas être modifiées par les comptes des membres de votre AWS organisation. AWS Config est intégré de manière native pour envoyer les résultats AWS Security Hub CSPM, si Security Hub CSPM est activé et qu'au moins une règle personnalisée ou AWS Config gérée existe.

Dans le AWS SRA, le compte d'administrateur AWS Config délégué est le compte Security Tooling. Le canal AWS Config de diffusion est configuré pour fournir des instantanés de configuration des ressources dans un compartiment S3 centralisé du compte Log Archive. Le compte Log Archive étant le magasin central du référentiel de journaux, il est utilisé pour stocker la configuration des ressources.

Considérations relatives à la conception

- AWS Config envoie des notifications de modification de configuration et de conformité à Amazon EventBridge. Cela signifie que vous pouvez utiliser les fonctionnalités de filtrage natives EventBridge pour filtrer les AWS Config événements afin de pouvoir acheminer des types spécifiques de notifications vers des cibles spécifiques. Par exemple, vous pouvez envoyer des notifications de conformité pour des règles ou des types de ressources spécifiques à des adresses e-mail spécifiques, ou acheminer les notifications de modification de configuration vers un outil externe de gestion des services informatiques (ITSM) ou de base de données de gestion des configurations (CMDB). Pour plus d'informations, consultez le billet de blog consacré aux AWS Config meilleures pratiques.

- Outre l'évaluation AWS Config proactive des règles, vous pouvez utiliser AWS CloudFormation Guardun outil d' policy-as-codeévaluation qui vérifie de manière proactive la conformité de la configuration des ressources. L'interface de ligne de AWS CloudFormation Guard commande (CLI) fournit un langage déclaratif spécifique au domaine (DSL) que vous pouvez utiliser pour exprimer la politique sous forme de code. En outre, vous pouvez utiliser des AWS CLI commandes pour valider des données structurées au format JSON ou YAML, telles que des ensembles de CloudFormation modifications, des fichiers de configuration Terraform basés sur JSON ou des configurations Kubernetes. Vous pouvez exécuter les évaluations localement en utilisant la AWS CloudFormation Guard CLI dans le cadre de votre processus de création ou dans le cadre de votre pipeline de déploiement. Si vous avez des AWS Cloud Development Kit (AWS CDK)applications, vous pouvez utiliser cdk-nag pour vérifier de manière proactive les meilleures pratiques.

Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation qui déploie des packs de AWS Config conformité dans toutes les régions d'une organisation Comptes AWS et dans toutes les régions. AWS Le module AWS Config Aggregator vous aide à configurer un AWS Config agrégateur en déléguant l'administration à un compte membre (Security Tooling) dans le compte Org Management, puis en configurant AWS Config Aggregator dans le compte administrateur délégué pour tous les comptes existants et futurs de l'organisation. AWS Vous pouvez utiliser le module AWS Config Control Tower Management Account pour l'activer AWS Config dans le compte Org Management ; il n'est pas activé par. AWS Control Tower

Amazon Security Lake

Amazon Security Lake est un service de lac de données de sécurité entièrement géré. Vous pouvez utiliser Security Lake pour centraliser automatiquement les données de sécurité provenant des AWS environnements, des fournisseurs de logiciels en tant que service (SaaS), des sites locaux et de sources tierces. Security Lake vous aide à créer une source de données normalisée qui simplifie l'utilisation des outils d'analyse par rapport aux données de sécurité, afin que vous puissiez mieux comprendre votre posture de sécurité dans l'ensemble de l'entreprise. Le lac de données est soutenu par des compartiments Amazon Simple Storage Service (Amazon S3), et vous restez propriétaire

de vos données. Security Lake collecte automatiquement les journaux Services AWS, notamment pour Amazon VPC AWS CloudTrail, Amazon Route 53, Amazon S3, les journaux d'audit, les AWS Security Hub CSPM résultats et AWS WAF les journaux d' AWS Lambda Amazon EKS.

AWS La SRA vous recommande d'utiliser le compte Log Archive comme compte d'administrateur délégué pour Security Lake. Pour plus d'informations sur la configuration du compte administrateur délégué, consultez Amazon Security Lake dans la section Security OU – Compte Log Archive. Les équipes de sécurité qui souhaitent accéder aux données de Security Lake ou qui ont besoin de pouvoir écrire des journaux non natifs dans les compartiments Security Lake à l'aide de fonctions personnalisées d'extraction, de transformation et de chargement (ETL) doivent opérer dans le compte Security Tooling.

Security Lake peut collecter des journaux provenant de différents fournisseurs de cloud, des journaux provenant de solutions tierces ou d'autres journaux personnalisés. Nous vous recommandons d'utiliser le compte Security Tooling pour exécuter les fonctions ETL afin de convertir les journaux au format Open Cybersecurity Schema Framework (OCSF) et de générer un fichier au format Apache Parquet. Security Lake crée le rôle multi-comptes avec les autorisations appropriées pour le compte Security Tooling et la source personnalisée soutenue par des fonctions Lambda ou des robots d' AWS Glue exploration, afin d'écrire des données dans les compartiments S3 pour Security Lake.

L'administrateur de Security Lake doit configurer les équipes de sécurité qui utilisent le compte Security Tooling et qui ont besoin d'accéder aux journaux que Security Lake collecte en tant qu'abonnés. Security Lake prend en charge deux types d'accès pour les abonnés :

- Accès aux données — Les abonnés peuvent accéder directement aux objets Amazon S3 pour Security Lake. Security Lake gère l'infrastructure et les autorisations. Lorsque vous configurez le compte Security Tooling en tant qu'abonné à l'accès aux données de Security Lake, le compte est informé de la présence de nouveaux objets dans les compartiments Security Lake via Amazon Simple Queue Service (Amazon SQS), et Security Lake crée les autorisations nécessaires pour accéder à ces nouveaux objets.
- Accès aux requêtes : les abonnés peuvent interroger les données sources à partir AWS Lake Formation des tables de votre compartiment S3 en utilisant des services tels qu'Amazon Athena. L'accès entre comptes est automatiquement configuré pour l'accès aux requêtes à l'aide de Lake Formation. Lorsque vous configurez le compte Security Tooling en tant qu'abonné à l'accès aux requêtes Security Lake, le compte bénéficie d'un accès en lecture seule aux journaux du compte Security Lake. Lorsque vous utilisez ce type d'abonné, l'Athena et les AWS Glue tables sont partagées entre le compte Security Lake Log Archive et le compte Security Tooling via AWS

Resource Access Manager ().AWS RAM Pour activer cette fonctionnalité, vous devez mettre à jour les paramètres de partage de données entre comptes vers la version 3.

Pour plus d'informations sur la création d'abonnés, consultez la section Gestion des abonnés dans la documentation de Security Lake.

Pour connaître les meilleures pratiques en matière d'ingestion de sources personnalisées, consultez la section Collecte de données à partir de sources personnalisées dans la documentation de Security Lake.

Vous pouvez utiliser Amazon Quick Sight, Amazon OpenSearch Service et Amazon SageMaker pour configurer des analyses par rapport aux données de sécurité que vous stockez dans Security Lake.

> **Considération relative à la conception**
>
> Si une équipe d'application a besoin d'un accès par requête aux données de Security Lake pour répondre à une exigence commerciale, l'administrateur de Security Lake doit configurer ce compte d'application en tant qu'abonné.

Amazon Macie

Amazon Macie est un service de sécurité et de confidentialité des données entièrement géré qui utilise l'apprentissage automatique et la correspondance de modèles pour découvrir et protéger vos données sensibles dans. AWS Vous devez identifier le type et la classification des données traitées par votre charge de travail afin de garantir l'application des contrôles appropriés. Vous pouvez utiliser Macie pour automatiser la découverte et le reporting des données sensibles de deux manières : en effectuant une découverte automatique des données sensibles et en créant et en exécutant des tâches de découverte de données sensibles. Grâce à la découverte automatique des données sensibles, Macie évalue quotidiennement votre inventaire de compartiments S3 et utilise des techniques d'échantillonnage pour identifier et sélectionner des objets S3 représentatifs de vos compartiments. Macie récupère et analyse ensuite les objets sélectionnés, en les inspectant pour détecter la présence de données sensibles. Les tâches de découverte de données sensibles permettent une analyse plus approfondie et plus ciblée. Avec cette option, vous définissez l'étendue et la profondeur de l'analyse, y compris les compartiments S3 à analyser, la profondeur d'échantillonnage et les critères personnalisés dérivés des propriétés des objets S3. Si Macie détecte un problème potentiel lié à la sécurité ou à la confidentialité d'un bucket, il crée une politique pour

vous. La découverte automatique des données est activée par défaut pour tous les nouveaux clients Macie, et les clients Macie existants peuvent l'activer en un clic.

Macie est activé dans tous les comptes via AWS Organizations. Les administrateurs disposant des autorisations appropriées sur le compte d'administrateur délégué (dans ce cas, le compte Security Tooling) peuvent activer ou suspendre Macie sur n'importe quel compte, créer des tâches de découverte de données sensibles pour les buckets appartenant à des comptes membres et consulter toutes les conclusions relatives aux politiques relatives à tous les comptes membres. Les résultats de données sensibles ne peuvent être consultés que par le compte qui a créé la tâche de résultats sensibles. Pour plus d'informations, consultez la section Gestion de plusieurs comptes Macie en tant qu'organisation dans la documentation Macie.

Les résultats de Macie sont transmis à des AWS Security Hub CSPM fins d'examen et d'analyse. Macie s'intègre également EventBridge à Amazon pour faciliter les réponses automatisées aux résultats tels que les alertes, les flux vers les systèmes de gestion des informations et des événements de sécurité (SIEM) et les mesures correctives automatisées.

Considérations relatives à la conception

- Si les objets S3 sont chiffrés avec une clé AWS Key Management Service (AWS KMS) que vous gérez, vous pouvez ajouter le rôle lié au service Macie en tant qu'utilisateur clé à cette clé KMS pour permettre à Macie de scanner les données.
- Macie est optimisé pour scanner des objets dans Amazon S3. Par conséquent, tout type d'objet compatible MacIE pouvant être placé dans Amazon S3 (de façon permanente ou temporaire) peut être scanné pour détecter la présence de données sensibles. Cela signifie que les données provenant d'autres sources, par exemple les exportations instantanées périodiques de bases de données Amazon Relational Database Service (Amazon RDS) ou Amazon Aurora, les tables Amazon DynamoDB exportées ou les fichiers texte extraits d'applications natives ou tierces, peuvent être déplacées vers Amazon S3 et évaluées par Macie.

Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation d'Amazon Macie. Cela inclut la délégation de l'administration à un compte membre et la configuration de Macie dans le compte administrateur délégué pour tous les comptes existants et futurs de l' AWS

organisation. Macie est également configuré pour envoyer les résultats à un compartiment S3 central crypté à l'aide d'une clé gérée par le client. AWS KMS

Analyseur d’accès IAM

Alors que vous accélérez votre processus d' AWS Cloud adoption et que vous continuez à innover, il est essentiel de contrôler étroitement les accès précis (autorisations), de contenir la prolifération des accès et de garantir une utilisation efficace des autorisations. L'accès excessif et non utilisé pose des problèmes de sécurité et complique l'application du principe du moindre privilège par les entreprises. Ce principe est un pilier important de l'architecture de sécurité qui implique de dimensionner en permanence les autorisations IAM afin de trouver un équilibre entre les exigences de sécurité et les exigences opérationnelles et de développement d'applications. Cet effort implique de nombreuses parties prenantes, notamment des équipes de sécurité centrale et du centre d'excellence cloud (CCoE) ainsi que des équipes de développement décentralisées.

Gestion des identités et des accès AWS Access Analyzer fournit des outils permettant de définir efficacement des autorisations précises, de vérifier les autorisations prévues et d'affiner les autorisations en supprimant les accès non utilisés afin de vous aider à respecter les normes de sécurité de votre entreprise. Il vous donne une visibilité sur l'accès externe et interne aux AWS ressources et sur les résultats d'accès non utilisés via des tableaux de bord et AWS Security Hub CSPM. En outre, il prend en charge Amazon EventBridge pour les flux de travail personnalisés de notification et de correction basés sur les événements.

La fonction de résultats de l'analyseur d'accès externe d'IAM Access Analyzer vous aide à identifier les ressources de votre AWS organisation et les comptes, tels que les compartiments Amazon S3 ou les rôles IAM, qui sont partagés avec une entité externe. L' AWS organisation ou le compte que vous choisissez est connu sous le nom de zone de confiance. L'analyseur utilise un raisonnement automatique pour analyser toutes les ressources prises en charge dans la zone de confiance et génère des résultats pour les principaux qui peuvent accéder aux ressources depuis l'extérieur de la zone de confiance. Ces résultats permettent d'identifier les ressources partagées avec une entité externe et de prévisualiser l'impact de votre politique sur l'accès public et multicompte à votre ressource avant de déployer les autorisations relatives aux ressources. Ceci est disponible sans frais supplémentaires.

De même, la fonction de recherche de l'analyseur d'accès interne d'IAM Access Analyzer vous aide à identifier les ressources de votre AWS organisation et les comptes partagés avec les

principaux en interne au sein de votre organisation ou de votre compte. Cette analyse soutient le principe du moindre privilège en garantissant que les ressources que vous avez spécifiées ne sont accessibles qu'aux principaux responsables concernés au sein de votre organisation. Il s'agit d'une fonctionnalité payante qui nécessite une configuration explicite des ressources à inspecter. Utilisez cette fonctionnalité judicieusement pour surveiller des ressources sensibles spécifiques qui, de par leur conception, doivent être verrouillées même en interne.

Les résultats d'IAM Access Analyzer vous aident également à identifier les accès non utilisés accordés dans vos AWS organisations et comptes, notamment :

- Rôles IAM non utilisés : rôles n'ayant aucune activité d'accès dans la fenêtre d'utilisation spécifiée.
- Utilisateurs, informations d'identification et clés d'accès IAM non utilisés : informations d'identification appartenant aux utilisateurs IAM et utilisées pour accéder aux ressources Services AWS .
- Politiques et autorisations IAM non utilisées : autorisations au niveau du service et au niveau de l'action qui n'ont pas été utilisées par un rôle dans une fenêtre d'utilisation spécifiée. IAM Access Analyzer utilise des politiques basées sur l'identité associées aux rôles pour déterminer les services et les actions auxquels ces rôles peuvent accéder. L'analyseur fournit un aperçu des autorisations non utilisées pour toutes les autorisations de niveau de service.

Vous pouvez utiliser les résultats générés par IAM Access Analyzer pour obtenir de la visibilité sur tout accès involontaire ou non utilisé et y remédier, conformément aux politiques et aux normes de sécurité de votre organisation. Après correction, ces résultats sont marqués comme résolus lors de la prochaine exécution de l'analyseur. Si le résultat est intentionnel, vous pouvez le marquer comme archivé dans IAM Access Analyzer et hiérarchiser les autres résultats présentant un risque de sécurité accru. En outre, vous pouvez configurer des règles d'archivage pour archiver automatiquement des résultats spécifiques. Par exemple, vous pouvez créer une règle d’archivage pour archiver automatiquement tous les résultats pour un compartiment Amazon S3 spécifique auquel vous accordez régulièrement l’accès.

En tant que créateur, vous pouvez utiliser IAM Access Analyzer pour effectuer des vérifications automatisées des politiques IAM plus tôt dans votre processus de développement et de déploiement (CI/CD) afin de respecter les normes de sécurité de votre entreprise. Vous pouvez intégrer les vérifications et révisions de politiques personnalisées d'IAM Access Analyzer AWS CloudFormation pour automatiser les révisions des politiques dans le cadre des pipelines de votre équipe de CI/CD développement. Cela inclut notamment les éléments suivants :

- Validation des politiques IAM — IAM Access Analyzer valide vos politiques par rapport à la grammaire des politiques IAM et aux meilleures pratiques. AWS Vous pouvez consulter les résultats des contrôles de validation des politiques, notamment les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions pour votre politique. Plus de 100 contrôles de validation des politiques sont actuellement disponibles et peuvent être automatisés à l'aide des AWS Command Line Interface touches (AWS CLI) et APIs.
- Contrôles de politique personnalisés IAM — Les contrôles de politique personnalisés d'IAM Access Analyzer valident vos politiques par rapport aux normes de sécurité que vous avez spécifiées. Les contrôles de politique personnalisés utilisent un raisonnement automatisé pour fournir un niveau d'assurance supérieur quant au respect des normes de sécurité de votre entreprise. Les types de vérifications de politiques personnalisées incluent :
  - Comparaison avec une politique de référence : lorsque vous modifiez une politique, vous pouvez la comparer à une stratégie de référence, telle qu'une version existante de la stratégie, pour vérifier si la mise à jour accorde un nouvel accès. L'CheckNoNewAccessAPI compare deux politiques (une politique mise à jour et une politique de référence) afin de déterminer si la politique mise à jour introduit un nouvel accès par rapport à la politique de référence, et renvoie une réponse positive ou négative.
  - Vérifiez par rapport à une liste d'actions IAM : vous pouvez utiliser l'CheckAccessNotGrantedAPI pour vous assurer qu'une politique n'autorise pas l'accès à une liste d'actions critiques définies dans votre norme de sécurité. Cette API utilise une politique et une liste de 100 actions IAM au maximum pour vérifier si la politique autorise au moins l'une des actions, et renvoie une réponse d'échec ou de réussite.

Les équipes de sécurité et les autres auteurs de politiques IAM peuvent utiliser IAM Access Analyzer pour créer des politiques conformes à la grammaire des politiques IAM et aux normes de sécurité. La création manuelle de politiques correctement dimensionnées peut être source d'erreurs et prendre beaucoup de temps. La fonction de génération de politiques IAM Access Analyzer aide à créer des politiques IAM basées sur l'activité d'accès d'un principal. IAM Access Analyzer examine AWS CloudTrail les journaux des services pris en charge et génère un modèle de politique contenant les autorisations utilisées par le principal dans la plage de dates spécifiée. Vous pouvez ensuite utiliser ce modèle pour créer une politique avec des autorisations détaillées qui n'accordent que les autorisations nécessaires.

- Un suivi doit être activé CloudTrail pour que votre compte puisse générer une politique basée sur l'activité d'accès.

- IAM Access Analyzer n'identifie pas l'activité au niveau de l'action pour les événements de données, tels que les événements de données Amazon S3, dans les politiques générées.
- L'`iam:PassRole`action n'est pas suivie CloudTrail et n'est pas incluse dans les politiques générées.

L'analyseur d'accès IAM est déployé dans le compte Security Tooling via la fonctionnalité d'administrateur délégué dans. AWS Organizations L'administrateur délégué est autorisé à créer et à gérer des analyseurs avec l' AWS organisation comme zone de confiance.

Considération relative à la conception

Pour obtenir des résultats spécifiques au compte (où le compte sert de limite fiable), vous devez créer un analyseur de l'étendue du compte dans chaque compte membre. Cela peut être fait dans le cadre du pipeline de comptes. Les résultats relatifs au compte sont transmis au Security Hub CSPM au niveau du compte membre. De là, ils sont transférés vers le compte d'administrateur délégué du Security Hub CSPM (Security Tooling).

Exemples d’implémentation

- La bibliothèque de code AWS SRA fournit un exemple d'implémentation d'IAM Access Analyzer. Il explique comment configurer un analyseur au niveau de l'organisation dans un compte d'administrateur délégué et un analyseur au niveau du compte dans chaque compte.
- Pour plus d'informations sur la manière dont vous pouvez intégrer des contrôles de politique personnalisés dans les flux de travail des créateurs, consultez le billet de AWS blog Présentation des contrôles de politique personnalisés d'IAM Access Analyzer.

AWS Firewall Manager

AWS Firewall Managercontribue à protéger votre réseau en simplifiant vos tâches d'administration et de maintenance pour les AWS WAF groupes AWS Network Firewall de sécurité Amazon VPC Amazon Route 53 Resolver et le pare-feu DNS sur plusieurs comptes et ressources. AWS Shield Advanced Avec Firewall Manager, vous ne configurez qu'une seule AWS WAF fois vos règles de pare-feu, les protections Shield Advanced, les groupes de sécurité Amazon VPC, les pare-feux

Network Firewall et les associations de groupes de règles de pare-feu DNS. Le service applique automatiquement les règles et les protections sur l'ensemble de vos comptes et de vos ressources, même celles qui sont ajoutées ultérieurement.

Firewall Manager est particulièrement utile lorsque vous souhaitez protéger AWS l'ensemble de votre organisation plutôt qu'un petit nombre de comptes et de ressources spécifiques, ou si vous ajoutez fréquemment de nouvelles ressources que vous souhaitez protéger. Firewall Manager utilise des politiques de sécurité pour vous permettre de définir un ensemble de configurations, notamment les règles, protections et actions pertinentes qui doivent être déployées, ainsi que les comptes et ressources (indiqués par des balises) à inclure ou à exclure. Vous pouvez créer des configurations granulaires et flexibles tout en étant en mesure d'étendre le contrôle à un grand nombre de comptes et VPCs. Ces politiques appliquent automatiquement et de manière cohérente les règles que vous configurez, même lorsque de nouveaux comptes et ressources sont créés. Firewall Manager est activé dans tous les comptes AWS Organizations, et la configuration et la gestion sont effectuées par les équipes de sécurité appropriées dans le compte d'administrateur délégué de Firewall Manager (dans ce cas, le compte Security Tooling).

Vous devez activer AWS Config chaque Région AWS élément contenant les ressources que vous souhaitez protéger. Si vous ne souhaitez pas l'activer AWS Config pour toutes les ressources, vous devez l'activer pour les ressources associées au type de politiques de Firewall Manager que vous utilisez. Lorsque vous utilisez à la fois Firewall Manager AWS Security Hub CSPM et Firewall Manager, Firewall Manager envoie automatiquement vos résultats à Security Hub CSPM. Firewall Manager crée des résultats pour les ressources non conformes et pour les attaques qu'il détecte, et envoie les résultats à Security Hub CSPM. Lorsque vous configurez une politique Firewall Manager pour AWS WAF, vous pouvez activer de manière centralisée la connexion aux listes de contrôle d'accès Web (Web ACLs) pour tous les comptes concernés et centraliser les journaux sous un seul compte.

Avec Firewall Manager, vous pouvez avoir un ou plusieurs administrateurs chargés de gérer les ressources de pare-feu de votre entreprise. Lorsque vous affectez plusieurs administrateurs, vous pouvez appliquer des conditions d'étendue administrative restrictives pour définir les ressources (comptes OUs, régions, types de politiques) que chaque administrateur peut gérer. Cela vous donne la flexibilité d'avoir différents rôles d'administrateur au sein de votre organisation et vous aide à conserver le principe de l'accès le moins privilégié. La AWS SRA utilise un administrateur dont l'intégralité de l'étendue administrative est déléguée au compte Security Tooling.

Considération relative à la conception

Les responsables de comptes des comptes membres individuels de l' AWS organisation peuvent configurer des contrôles supplémentaires (tels que des AWS WAF règles et des groupes de sécurité Amazon VPC) dans les services gérés de Firewall Manager en fonction de leurs besoins particuliers.

Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation de Firewall Manager. Il illustre l'administration déléguée (outils de sécurité), déploie un groupe de sécurité maximal autorisé, configure une politique de groupe de sécurité et configure plusieurs politiques. AWS WAF

Amazon EventBridge

Amazon EventBridge est un service de bus d'événements sans serveur qui permet de connecter facilement vos applications à des données provenant de diverses sources. Il est fréquemment utilisé dans l'automatisation de la sécurité. Vous pouvez configurer des règles de routage pour déterminer où envoyer vos données afin de créer des architectures d'applications qui réagissent en temps réel à toutes vos sources de données. Vous pouvez créer un bus d'événements personnalisé pour recevoir les événements de vos applications personnalisées, en plus d'utiliser le bus d'événements par défaut dans chaque compte. Vous pouvez créer un bus d'événements dans le compte Security Tooling qui peut recevoir des événements spécifiques à la sécurité provenant d'autres comptes de l'organisation. AWS Par exemple, en liant AWS Config Rules Amazon et AWS Security Hub CSPM avec GuardDuty EventBridge, vous créez un pipeline flexible et automatisé pour acheminer les données de sécurité, émettre des alertes et gérer les actions visant à résoudre les problèmes.

Considérations relatives à la conception

- EventBridge est capable d'acheminer des événements vers un certain nombre de cibles différentes. Un modèle intéressant pour automatiser les actions de sécurité consiste à relier des événements particuliers à des AWS Lambda intervenants individuels, qui prennent les mesures appropriées. Par exemple, dans certaines circonstances, vous souhaiterez peut-être l'utiliser EventBridge pour acheminer une recherche de compartiment S3 public

vers un répondeur Lambda qui corrige la politique du compartiment et supprime les autorisations publiques. Ces intervenants peuvent être intégrés à vos manuels d'enquête et à vos manuels d'exécution afin de coordonner les activités d'intervention.

- L'une des meilleures pratiques pour une équipe des opérations de sécurité efficace consiste à intégrer le flux des événements et des résultats de sécurité dans un système de notification et de flux de travail tel qu'un système de billetterie, un bug/issue système ou un autre système de gestion des informations et des événements de sécurité (SIEM). Cela permet de réduire le flux de travail lié aux e-mails et aux rapports statiques, et de vous aider à acheminer, à escalader et à gérer les événements ou les résultats. Les capacités de routage flexibles qu' EventBridge il contient constituent un puissant outil pour cette intégration.

Amazon Detective

Amazon Detective soutient votre stratégie de contrôle de sécurité réactive en simplifiant l'analyse, l'investigation et l'identification rapide de la cause première des découvertes de sécurité ou des activités suspectes pour vos analystes de sécurité. Detective extrait automatiquement les événements temporels tels que les tentatives de connexion, les appels d'API et le trafic réseau à partir AWS CloudTrail des journaux et des journaux de flux Amazon VPC. Detective utilise ces événements en utilisant des flux indépendants de CloudTrail journaux et des journaux de flux Amazon VPC. Vous pouvez utiliser Detective pour accéder à un an de données historiques sur les événements. Detective utilise l'apprentissage automatique et la visualisation pour créer une vue unifiée et interactive du comportement de vos ressources et des interactions entre elles au fil du temps. C'est ce que l'on appelle un graphe de comportement. Vous pouvez explorer le graphe de comportement pour examiner des actions disparates telles que des tentatives d'ouverture de session infructueuses ou des appels d'API suspects.

Detective s'intègre à Amazon Security Lake pour permettre aux analystes de sécurité d'interroger et de récupérer les journaux stockés dans Security Lake. Vous pouvez utiliser cette intégration pour obtenir des informations supplémentaires à partir CloudTrail des journaux et des journaux de flux Amazon VPC stockés dans Security Lake lorsque vous menez des enquêtes de sécurité dans Detective.

Detective ingère également les résultats détectés par Amazon GuardDuty, y compris les menaces détectées par GuardDuty Runtime Monitoring. Lorsqu'un compte active Detective, il devient le compte administrateur du graphe de comportement. Avant d'essayer d'activer Detective, assurez-

vous que votre compte est connecté GuardDuty depuis au moins 48 heures. Si vous ne répondez pas à cette exigence, vous ne pouvez pas l'activer DetectiveDetective.

Les sources de données facultatives supplémentaires pour Detective incluent les journaux d'audit Amazon EKS et AWS Security Hub CSPM. La source de données du journal d'audit Amazon EKS améliore les informations fournies sur les types d'entités suivants : clusters Amazon EKS, pods Kubernetes, images de conteneurs et sujets Kubernetes. La source de données Security Hub fait partie des résultats de AWS sécurité, où elle met en corrélation les résultats de différents produits dans Security Hub et les intègre dans Detective.

Detective regroupe automatiquement plusieurs résultats liés à un seul événement de compromission de sécurité dans des groupes de recherche. Les acteurs de la menace exécutent généralement une séquence d'actions qui aboutissent à de multiples constatations de sécurité réparties dans le temps et les ressources. Par conséquent, la recherche de groupes devrait être le point de départ des enquêtes impliquant plusieurs entités et conclusions. Detective fournit également des résumés de groupes de recherche en utilisant une IA générative qui analyse automatiquement les groupes de recherche et fournit des informations en langage naturel pour vous aider à accélérer les enquêtes de sécurité.

Detective s'intègre à AWS Organizations. Le compte Org Management délègue un compte membre en tant que compte administrateur Detective. Dans le AWS SRA, il s'agit du compte Security Tooling. Le compte administrateur Detective permet d'activer automatiquement tous les comptes membres actuels de l'organisation en tant que comptes de membre Detective, et d'ajouter de nouveaux comptes membres au fur et à mesure qu'ils sont ajoutés à l' AWS organisation. Les comptes d'administrateur Detective ont également la possibilité d'inviter des comptes membres qui ne résident pas actuellement dans l' AWS organisation, mais qui appartiennent à la même région, à fournir leurs données au graphique de comportement du compte principal. Lorsqu'un compte membre accepte l'invitation et est activé, Detective commence à ingérer et à extraire les données du compte membre dans ce graphique de comportement.

> **Considération relative à la conception**
>
> Vous pouvez accéder à Detective pour trouver des profils à partir des AWS Security Hub CSPM consoles GuardDuty et. Ces liens peuvent aider à rationaliser le processus d'enquête. Votre compte doit être le compte administratif de Detective et du service que vous quittez (GuardDutyou Security Hub CSPM). Si les comptes principaux sont les mêmes pour les services, les liens d'intégration fonctionnent parfaitement.

AWS Audit Manager

AWS Audit Managervous aide à auditer en permanence votre AWS utilisation afin de simplifier la gestion des audits et la conformité aux réglementations et aux normes du secteur. Elle vous permet de passer de la collecte, de l'examen et de la gestion manuels des preuves à une solution qui automatise la collecte des preuves, fournit un moyen simple de suivre la source des preuves d'audit, permet la collaboration en équipe et aide à gérer la sécurité et l'intégrité des preuves. Lorsqu'il est temps d'effectuer un audit, Audit Manager vous aide à gérer les examens de vos contrôles par les parties prenantes.

Avec Audit Manager, vous pouvez effectuer un audit par rapport à des frameworks prédéfinis tels que le benchmark du Center for Internet Security (CIS), le CIS AWS Foundations Benchmark, System and Organization Controls 2 (SOC 2) et le Payment Card Industry Data Security Standard (PCI DSS). Il vous donne également la possibilité de créer vos propres cadres avec des contrôles standard ou personnalisés en fonction de vos exigences spécifiques en matière d'audits internes.

Audit Manager collecte quatre types de preuves. Trois types de preuves sont automatisés : les preuves de contrôle de conformité provenant de AWS Config et AWS Security Hub CSPM, les preuves d'événements de AWS CloudTrail gestion et les preuves de configuration provenant d'appels d' AWS service-to-service API. Pour les preuves qui ne peuvent pas être automatisées, Audit Manager vous permet de télécharger des preuves manuelles.

Par défaut, vos données dans Audit Manager sont chiffrées à l'aide de clés AWS gérées. Le AWS SRA utilise une clé gérée par le client pour le chiffrement afin de mieux contrôler l'accès logique. Vous devez également configurer un compartiment S3 dans l' Région AWS endroit où Audit Manager publie le rapport d'évaluation. Ces compartiments doivent être chiffrés à l'aide d'une clé gérée par le client et avoir une politique de compartiment configurée pour autoriser uniquement Audit Manager à publier des rapports.

> **Note**
>
> Audit Manager aide à collecter des preuves pertinentes pour vérifier la conformité aux normes et réglementations de conformité spécifiques. Toutefois, il n'évalue pas votre conformité. Par conséquent, les preuves collectées par le biais d'Audit Manager peuvent ne pas inclure les détails de vos processus opérationnels nécessaires aux audits. Audit Manager ne remplace pas un conseiller juridique ou un expert en conformité. Nous vous recommandons de faire

appel aux services d'un évaluateur tiers certifié pour le ou les cadres de conformité par rapport auxquels vous êtes évalué.

Les évaluations d'Audit Manager peuvent être effectuées sur plusieurs comptes au sein de votre AWS organisation. Audit Manager collecte et consolide les preuves dans un compte d'administrateur délégué dans AWS Organizations. Cette fonctionnalité d'audit est principalement utilisée par les équipes de conformité et d'audit interne, et ne nécessite qu'un accès en lecture à votre Comptes AWS.

Considérations relatives à la conception

- Audit Manager complète d'autres services AWS de sécurité tels que AWS Security Hub CSPM AWS Security Hub, et AWS Config pour aider à mettre en œuvre un cadre de gestion des risques. Audit Manager fournit des fonctionnalités d'assurance des risques indépendantes, tandis que Security Hub CSPM vous aide à superviser vos risques et que les packs de AWS Config conformité vous aident à gérer vos risques. Les professionnels de l'audit qui connaissent le modèle à trois lignes développé par l'Institut des auditeurs internes (IIA) doivent noter que cette combinaison vous Services AWS permet de couvrir les trois lignes de défense. Pour plus d'informations, consultez la série de blogues en deux parties sur le blog AWS Cloud Operations & Migrations.
- Pour qu'Audit Manager puisse collecter les preuves du Security Hub CSPM, le compte d'administrateur délégué pour les deux services doit être le même. Compte AWS C'est pourquoi, dans la AWS SRA, le compte Security Tooling est l'administrateur délégué d'Audit Manager.

AWS Artifact

AWS Artifactest hébergé dans le compte Security Tooling afin de séparer la fonctionnalité de gestion des artefacts de conformité du compte de gestion de l' AWS organisation. Cette séparation des tâches est importante car nous vous recommandons d'éviter d'utiliser le compte AWS Org Management pour les déploiements, sauf en cas d'absolue nécessité. Transférez plutôt les déploiements aux comptes des membres. Étant donné que la gestion des artefacts d'audit peut être effectuée à partir d'un compte membre et que la fonction est étroitement liée à l'équipe de sécurité et de conformité, le compte Security Tooling est désigné comme compte administrateur pour. AWS

Artifact Vous pouvez utiliser AWS Artifact les rapports pour télécharger des documents AWS de sécurité et de conformité, tels que les certifications AWS ISO, les rapports PCI (Payment Card Industry) et les rapports SOC (System and Organization Controls).

AWS Artifact ne prend pas en charge la fonctionnalité d'administration déléguée. Au lieu de cela, vous pouvez limiter cette fonctionnalité aux seuls rôles IAM du compte Security Tooling relatifs à vos équipes d'audit et de conformité, afin qu'elles puissent télécharger, examiner et fournir ces rapports aux auditeurs externes selon les besoins. Vous pouvez également restreindre les rôles IAM spécifiques afin de n'avoir accès qu'à des AWS Artifact rapports spécifiques par le biais de politiques IAM. Pour des exemples de politiques IAM, consultez la AWS Artifact documentation.

> **Considération relative à la conception**
>
> Si vous choisissez d'avoir un compte dédié Compte AWS aux équipes d'audit et de conformité, vous pouvez l'héberger AWS Artifact dans un compte d'audit de sécurité, distinct du compte Security Tooling. AWS Artifact les rapports fournissent des preuves démontrant qu'une organisation suit un processus documenté ou répond à une exigence spécifique. Les artefacts d'audit sont collectés et archivés tout au long du cycle de développement du système et peuvent être utilisés comme preuves dans le cadre d'audits et d'évaluations internes ou externes.

AWS KMS

AWS Key Management Service(AWS KMS) vous aide à créer et à gérer des clés cryptographiques et à contrôler leur utilisation dans un large éventail d'applications Services AWS et dans celles-ci. AWS KMS est un service sécurisé et résilient qui utilise des modules de sécurité matériels pour protéger les clés cryptographiques. Il suit les processus de cycle de vie standard du secteur pour les éléments clés, tels que le stockage, la rotation et le contrôle d'accès des clés. AWS KMS peut aider à protéger vos données à l'aide de clés de chiffrement et de signature, et peut être utilisé à la fois pour le chiffrement côté serveur et le chiffrement côté client via le SDK de chiffrement.AWS Pour des raisons de protection et de flexibilité, AWS KMS prend en charge trois types de clés : les clés gérées par le client, les clés AWS gérées et les clés AWS détenues. Les clés gérées par le client sont des AWS KMS clés Compte AWS que vous créez, détenez et gérez. AWS les clés gérées sont des AWS KMS clés de votre compte créées, gérées et utilisées en votre nom par et intégrées à AWS KMS. Service AWS AWS les clés possédées sont un ensemble de AWS KMS clés qu'un Service AWS utilisateur possède et gère pour une utilisation multiple Comptes AWS. Pour plus d'informations

sur l'utilisation AWS KMS des clés, consultez la AWS KMS documentation et les détails AWS KMS cryptographiques.

L'une des options de déploiement consiste à centraliser la responsabilité de la gestion des AWS KMS clés sur un seul compte tout en déléguant la capacité d'utiliser les clés du compte d'application aux ressources de l'application en utilisant une combinaison de politiques clés et IAM. Cette approche est sûre et simple à gérer, mais elle peut se AWS KMS heurter à des obstacles en raison des limites de régulation, des limites de service des comptes et de l'inondation de l'équipe de sécurité par les tâches opérationnelles de gestion des clés. Une autre option de déploiement consiste à utiliser un modèle décentralisé dans lequel vous autorisez AWS KMS à résider dans plusieurs comptes, et vous autorisez les responsables de l'infrastructure et des charges de travail d'un compte spécifique à gérer leurs propres clés. Ce modèle donne à vos équipes chargées de la charge de travail plus de contrôle, de flexibilité et d'agilité en ce qui concerne l'utilisation des clés de chiffrement. Cela permet également d'éviter les limites d'API, de limiter l'étendue de l'impact à une Compte AWS seule et de simplifier les tâches de reporting, d'audit et autres tâches liées à la conformité. Dans un modèle décentralisé, il est important de déployer et d'appliquer des garde-fous afin que les clés décentralisées soient gérées de la même manière et que l'utilisation des AWS KMS clés soit auditée conformément aux meilleures pratiques et politiques établies. Pour plus d'informations, consultez le livre blanc AWS Key Management Service Meilleures pratiques. AWS La SRA recommande un modèle de gestion distribuée des clés dans lequel les AWS KMS clés résident localement dans le compte où elles sont utilisées. Nous vous recommandons d'éviter d'utiliser une seule clé dans un compte pour toutes les fonctions cryptographiques. Les clés peuvent être créées en fonction des exigences relatives à la fonction et à la protection des données, et pour appliquer le principe du moindre privilège. Dans certains cas, les autorisations de chiffrement seraient séparées des autorisations de déchiffrement, et les administrateurs géreraient les fonctions du cycle de vie mais ne seraient pas en mesure de chiffrer ou de déchiffrer les données avec les clés qu'ils gèrent.

Dans le compte Security Tooling, AWS KMS il est utilisé pour gérer le chiffrement des services de sécurité centralisés tels que le AWS CloudTrail journal de l'organisation géré par l' AWS organisation.

AWS CA privée

AWS Autorité de certification privée(AWS CA privée) est un service de CA privé géré qui vous aide à gérer en toute sécurité le cycle de vie de vos certificats TLS d'entité finale privée pour les instances EC2, les conteneurs, les appareils IoT et les ressources sur site. Il permet de chiffrer les communications TLS avec les applications en cours d'exécution. Vous pouvez ainsi créer votre propre hiérarchie d'autorités de certification (une autorité de certification racine, par le biais de certificats subordonnés CAs à l'entité finale) et émettre des certificats pour authentifier les utilisateurs

internes, les ordinateurs, les applications, les services, les serveurs et autres appareils, et pour signer le code informatique. AWS CA privée Les certificats émis par une autorité de certification privée ne sont fiables qu'au sein de votre AWS organisation, et non sur Internet.

Une infrastructure à clé publique (PKI) ou une équipe de sécurité peut être chargée de gérer l'ensemble de l'infrastructure PKI. Cela inclut la gestion et la création de l'autorité de certification privée. Cependant, il doit y avoir une disposition permettant aux équipes chargées de la charge de travail de répondre elles-mêmes à leurs exigences en matière de certificats. Le AWS SRA décrit une hiérarchie d'autorité de certification centralisée dans laquelle l'autorité de certification racine est hébergée dans le compte Security Tooling. Cela permet aux équipes de sécurité d'appliquer un contrôle de sécurité rigoureux, car l'autorité de certification racine est à la base de l'ensemble de l'infrastructure PKI. Cependant, la création de certificats privés à partir de l'autorité de certification privée est déléguée aux équipes de développement d'applications en partageant l'autorité de certification sur un compte d'application à l'aide de AWS Resource Access Manager (AWS RAM). AWS RAM gère les autorisations requises pour le partage entre comptes. Cela élimine le besoin d'une autorité de certification privée pour chaque compte et constitue un mode de déploiement plus rentable. Pour plus d'informations sur le flux de travail et la mise en œuvre, consultez le billet de blog Comment utiliser AWS RAM pour partager vos AWS CA privée comptes entre plusieurs comptes.

> **Note**
>
> AWS Certificate Manager (ACM) vous aide également à provisionner, gérer et déployer des certificats TLS publics à utiliser avec. Services AWS Pour prendre en charge cette fonctionnalité, ACM doit résider dans le pays Compte AWS qui utiliserait le certificat public. Cette question est abordée plus loin dans ce guide, dans la section Compte de l'application.

> **Considérations relatives à la conception**
>
> - Avec AWS CA privée, vous pouvez créer une hiérarchie d'autorités de certification comportant jusqu'à cinq niveaux. Vous pouvez également créer plusieurs hiérarchies, chacune ayant sa propre racine. La AWS CA privée hiérarchie doit être conforme à la conception de l'infrastructure PKI de votre organisation. Cependant, gardez à l'esprit que l'augmentation de la hiérarchie de l'autorité de certification augmente le nombre de certificats dans le parcours de certification, ce qui, à son tour, augmente le temps de validation d'un certificat d'entité finale. Une hiérarchie d'autorités de certification bien définie présente des avantages tels qu'un contrôle de sécurité granulaire adapté à chaque

autorité de certification, la délégation des autorités de certification subordonnées à une application différente, ce qui entraîne une division des tâches administratives, l'utilisation d'une autorité de certification avec une confiance révocable limitée, la possibilité de définir différentes périodes de validité et la capacité d'appliquer des limites de chemin. Idéalement, votre racine et votre subordonné CAs sont séparés Comptes AWS. Pour plus d'informations sur la planification d'une hiérarchie CA à l'aide de AWS CA privée, consultez la AWS CA privée documentation et le billet de blog Comment sécuriser une AWS CA privée hiérarchie à l'échelle de l'entreprise pour l'automobile et le secteur manufacturier.

- AWS CA privée peut s'intégrer à votre hiérarchie CA existante, ce qui vous permet d'utiliser les fonctionnalités d'automatisation et AWS d'intégration native d'ACM en conjonction avec la racine de confiance existante que vous utilisez aujourd'hui. Vous pouvez créer une autorité de certification subordonnée dans AWS CA privée soutenue par une autorité de certification parent sur site. Pour plus d'informations sur la mise en œuvre, consultez la section Installation d'un certificat d'autorité de certification subordonnée signé par une autorité de certification parent externe dans la AWS CA privée documentation.

Amazon Inspector

Amazon Inspector est un service de gestion automatique des vulnérabilités qui découvre et analyse automatiquement les instances Amazon EC2, les images de conteneurs dans Amazon Elastic Container Registry (Amazon ECR) AWS Lambda , les fonctions et les référentiels de code au sein de vos gestionnaires de code source pour détecter des vulnérabilités logicielles connues et une exposition involontaire au réseau.

Amazon Inspector évalue en permanence votre environnement tout au long du cycle de vie de vos ressources en analysant automatiquement les ressources chaque fois que vous y apportez des modifications. Les événements qui déclenchent la nouvelle analyse d'une ressource incluent l'installation d'un nouveau package sur une instance EC2, l'installation d'un correctif et la publication d'un nouveau rapport CVE (Common Vulnerabilities and Exposures) qui affecte la ressource. Amazon Inspector prend en charge les évaluations de référence du Center of Internet Security (CIS) pour les systèmes d'exploitation dans les instances EC2.

Amazon Inspector s'intègre à des outils de développement tels que Jenkins et TeamCity pour l'évaluation des images de conteneurs. Vous pouvez évaluer les vulnérabilités logicielles de vos images de conteneur dans le cadre de votre intégration continue et de votre livraison continue (tableau de bord de l'CI/CD) tools, and push security to an earlier point in the software development

lifecycle. Assessment findings are available in the CI/CDoutil), afin de pouvoir effectuer des actions automatisées en réponse à des problèmes de sécurité critiques tels que le blocage de builds ou le transfert d'images vers des registres de conteneurs. Si vous en avez un actif Compte AWS, vous pouvez installer le plugin Amazon Inspector depuis votre place de marché d' CI/CD outils et ajouter un scan Amazon Inspector à votre pipeline de génération sans avoir à activer le service Amazon Inspector. Cette fonctionnalité fonctionne avec des CI/CD outils hébergés n'importe où (sur site AWS, sur site ou dans des clouds hybrides) afin que vous puissiez toujours utiliser une solution unique dans tous vos pipelines de développement. Lorsqu'Amazon Inspector est activé, il découvre automatiquement toutes vos instances EC2, les images de conteneurs dans Amazon ECR et les CI/CD outils, ainsi que les fonctions Lambda à grande échelle, et les surveille en permanence pour détecter les vulnérabilités connues.

Les résultats d'Amazon Inspector relatifs à l'accessibilité du réseau évaluent l'accessibilité de vos instances EC2 vers ou depuis les périphériques VPC, tels que les passerelles Internet, les connexions d'appairage VPC ou les réseaux privés virtuels () via une passerelle virtuelle. VPNs Ces règles permettent d'automatiser la surveillance de vos AWS réseaux et d'identifier les endroits où l'accès réseau à vos instances EC2 peut être mal configuré en raison de groupes de sécurité mal gérés, de listes de contrôle d'accès (ACLs), de passerelles Internet, etc. Pour plus d'informations, consultez la documentation Amazon Inspector.

Lorsqu'Amazon Inspector identifie des vulnérabilités ou des chemins réseau ouverts, il produit un résultat que vous pouvez examiner. Le résultat inclut des informations complètes sur la vulnérabilité, notamment un score de risque, la ressource affectée et des recommandations de correction.
Le score de risque est spécifiquement adapté à votre environnement et est calculé en corrélant les informations up-to-date CVE avec des facteurs temporels et environnementaux tels que les informations d'accessibilité et d'exploitabilité du réseau afin de fournir une constatation contextuelle.

Amazon Inspector Code Security analyse le code source des applications propriétaires, les dépendances des applications tierces et l'infrastructure en tant que code (IaC) pour détecter les vulnérabilités. Après avoir activé Code Security, vous pouvez créer et appliquer une configuration de scan à votre référentiel de code afin de déterminer la fréquence, le type de scan et les référentiels à scanner. Code Security prend en charge les tests statiques de sécurité des applications (SAST), l'analyse de la composition logicielle (SCA) et l'analyse iAc. Pour configurer la fréquence, vous pouvez définir des scans à la demande, lors de modifications de code ou périodiquement. L'analyse du code capture des extraits de code pour mettre en évidence les vulnérabilités détectées.
Les extraits de code sont stockés chiffrés à l'aide de clés KMS. L'administrateur délégué d'une organisation ne peut pas consulter les extraits de code appartenant aux comptes des membres.

Une fois que vous avez intégré vos gestionnaires de code source (SCMs) à Code Security, tous les référentiels de code sont répertoriés en tant que projets dans la console Amazon Inspector. Code Security surveille uniquement la branche par défaut de chaque référentiel. Amazon Inspector rationalise les mesures de sécurité en fournissant des recommandations de correction de code spécifiques directement sur le lieu de travail des développeurs. L'intégration bidirectionnelle avec votre SCM suggère automatiquement des correctifs sous forme de commentaires dans les pull requests (PRs) et les demandes de fusion (MRs) pour les résultats critiques et élevés, et alerte les développeurs sur les vulnérabilités les plus importantes à corriger sans perturber leur flux de travail.

Pour détecter les vulnérabilités, les instances EC2 doivent être gérées à l'aide de AWS Systems Manager l' AWS Systems Manager agent (SSMagent). Aucun agent n'est requis pour l'accessibilité réseau des instances EC2 ou pour l'analyse des vulnérabilités des images de conteneurs dans les fonctions Amazon ECR ou Lambda.

Amazon Inspector est intégré AWS Organizations et prend en charge l'administration déléguée. Dans le AWS SRA, le compte Security Tooling devient le compte d'administrateur délégué d'Amazon Inspector. Le compte d'administrateur délégué Amazon Inspector peut gérer les données relatives aux résultats et certains paramètres pour les membres de l' AWS organisation. Cela inclut l'affichage des détails des résultats agrégés pour tous les comptes membres, l'activation ou la désactivation des scans des comptes membres et l'examen des ressources numérisées au sein de l' AWS organisation.

Considérations relatives à la conception

- Amazon Inspector s'intègre AWS Security Hub CSPM automatiquement à Security Hub lorsque les deux services sont activés. Vous pouvez utiliser cette intégration pour envoyer tous les résultats d'Amazon Inspector au Security Hub CSPM, qui les inclura ensuite dans son analyse de votre niveau de sécurité.
- Amazon Inspector exporte automatiquement les événements relatifs aux résultats, aux modifications de la couverture des ressources et aux analyses initiales des ressources individuelles vers Amazon et EventBridge, éventuellement, vers un bucket Amazon Simple Storage Service (Amazon S3). Pour exporter les résultats actifs vers un compartiment S3, vous avez besoin d'une AWS KMS clé qu'Amazon Inspector peut utiliser pour chiffrer les résultats, et d'un compartiment S3 avec des autorisations permettant à Amazon Inspector de télécharger des objets. EventBridgel'intégration vous permet de surveiller et de traiter les résultats en temps quasi réel dans le cadre de vos flux de travail existants en matière de sécurité et de conformité. EventBridge les événements sont publiés sur le compte administrateur délégué Amazon Inspector en plus du compte membre dont ils proviennent.

- Les intégrations d'Amazon Inspector Code Security avec le GitHub SaaS, GitHub Enterprise Cloud et GitHub Enterprise Server nécessitent un accès Internet public.

Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation d'Amazon Inspector. Il illustre l'administration déléguée (outils de sécurité) et configure Amazon Inspector pour tous les comptes existants et futurs de l' AWS organisation.

AWS Security Incident Response

AWS Security Incident Responseest un service qui vous aide à vous préparer aux incidents de sécurité dans votre AWS environnement et à y répondre. Il trie les résultats, intensifie les événements de sécurité et gère les cas qui nécessitent votre attention immédiate. En outre, il vous donne accès à l'équipe de réponse aux incidents AWS clients (CIRT), qui enquête sur les ressources concernées. AWS Security Incident Response fournit également des fonctionnalités de réponse et de correction automatisées par le biais de AWS Systems Manager documents (documents SSM), qui aident les équipes de sécurité à répondre aux incidents de sécurité et à s'en remettre plus efficacement. AWS Security Incident Response s'intègre à Amazon GuardDuty et AWS Security Hub CSPM pour recevoir les résultats de sécurité et orchestrer des réponses automatisées.

Dans le AWS SRA, AWS Security Incident Response est déployé dans le compte Security Tooling en tant que compte d'administrateur délégué. Le compte Security Tooling est sélectionné car il correspond à l'objectif du compte, qui est d'exploiter les services de sécurité et d'automatiser les alertes et les réponses de sécurité. Le compte Security Tooling fait également office de compte d'administrateur délégué pour Security Hub CSPM et contribue GuardDuty à simplifier la gestion des flux AWS Security Incident Response de travail. AWS Security Incident Response est configuré pour fonctionner avec AWS Organizations, afin que vous puissiez gérer les réponses aux incidents sur les comptes de votre organisation à partir du compte Security Tooling.

AWS Security Incident Response vous aide à mettre en œuvre les phases suivantes du cycle de vie de réponse aux incidents :

- Préparation : Créez et maintenez des plans de réponse et des documents SSM pour les actions de confinement.

- Détection et analyse : analysez automatiquement les résultats de sécurité et déterminez la gravité de l'incident.
- Détection et analyse : ouvrez un dossier pris en charge par le service et contactez le AWS CIRT pour obtenir une assistance supplémentaire. Le CIRT est un groupe de personnes qui fournissent un soutien lors d'événements de sécurité actifs.
- Confinement et éradication : exécutez des actions de confinement automatisées via des documents SSM.
- Activité après l'incident : documentez les détails de l'incident et effectuez une analyse après l'incident.

Vous pouvez également l'utiliser AWS Security Incident Response pour créer des dossiers autogérés. AWS Security Incident Response peut créer une notification sortante ou un cas lorsque vous devez être au courant d'un élément susceptible d'avoir un impact sur votre compte ou vos ressources ou agir en conséquence. Cette fonctionnalité n'est disponible que lorsque vous activez les flux de travail de réponse proactive et de triage des alertes dans le cadre de votre abonnement.

Considérations relatives à la conception

- Lors de la mise en œuvre AWS Security Incident Response, examinez attentivement et testez les actions de réponse automatisées avant de les activer en production. L'automatisation peut accélérer la réponse aux incidents, mais des actions automatisées mal configurées peuvent avoir un impact sur les charges de travail légitimes.
- Envisagez d'utiliser des documents SSM AWS Security Incident Response pour mettre en œuvre des procédures de confinement spécifiques à l'organisation tout en conservant les meilleures pratiques intégrées au service pour les types d'incidents courants.
- Si vous prévoyez de l'utiliser AWS Security Incident Response dans un VPC, assurez-vous que les points de terminaison VPC appropriés sont configurés pour Systems Manager et les autres services intégrés afin d'activer les actions de confinement dans les sous-réseaux privés.

Déployer des services de sécurité communs au sein de tous Comptes AWS

La section Appliquer les services de sécurité à l'ensemble de votre AWS organisation plus haut dans cette référence a mis en évidence les services de sécurité qui protègent un Compte AWS, et a noté

que bon nombre de ces services peuvent également être configurés et gérés au sein de l'entreprise AWS Organizations. Certains de ces services doivent être déployés dans tous les comptes, et vous les verrez dans le AWS SRA. Cela permet un ensemble cohérent de garde-fous et fournit une surveillance, une gestion et une gouvernance centralisées au sein de votre AWS organisation.

Security Hub CSPM,, GuardDuty AWS Config, IAM Access Analyzer et les traces d' CloudTrail organisation apparaissent dans tous les comptes. Les trois premiers prennent en charge la fonctionnalité d'administrateur délégué décrite précédemment dans la section Le compte de gestion, l'accès sécurisé et les administrateurs délégués. CloudTrail utilise actuellement un mécanisme d'agrégation différent.

Le référentiel de GitHub code AWS SRA fournit un exemple d'implémentation permettant d'activer Security Hub CSPM,, GuardDuty AWS Config AWS Firewall Manager, et les traces d' CloudTrail organisation sur tous vos comptes, y compris le compte AWS Org Management.

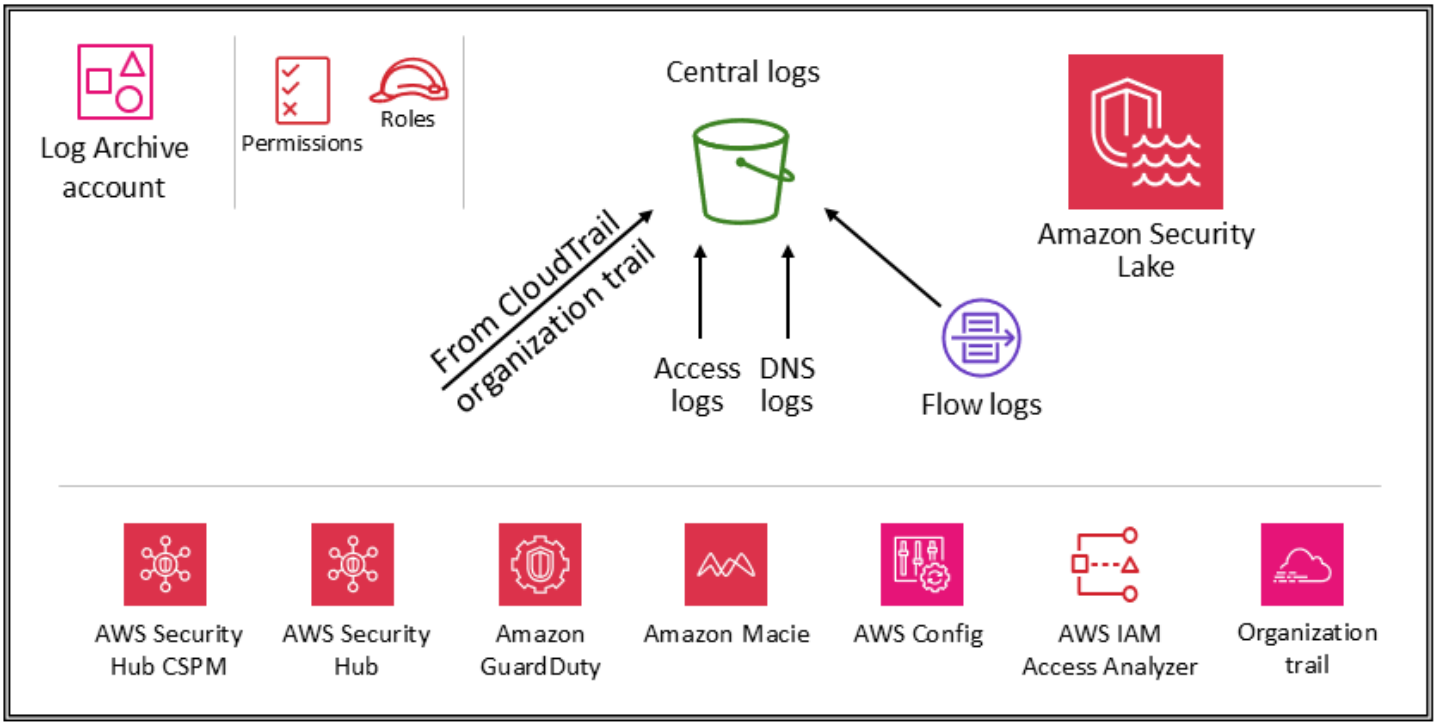
Considérations relatives à la conception

- Des configurations de compte spécifiques peuvent nécessiter des services de sécurité supplémentaires. Par exemple, les comptes qui gèrent les compartiments S3 (les comptes Application et Log Archive) devraient également inclure Amazon Macie et envisager d'activer CloudTrail la journalisation des événements de données S3 dans ces services de sécurité courants. (Macie prend en charge l'administration déléguée avec une configuration et une surveillance centralisées.) Un autre exemple est Amazon Inspector, qui s'applique uniquement aux comptes hébergeant des instances EC2 ou des images Amazon ECR.
- Outre les services décrits précédemment dans cette section, le AWS SRA inclut deux services axés sur la sécurité, Amazon Detective et Amazon Detective AWS Audit Manager, qui prennent en charge AWS Organizations l'intégration et la fonctionnalité d'administrateur délégué. Toutefois, ils ne sont pas inclus dans les services recommandés pour la définition de base des comptes, car nous avons constaté que ces services sont mieux utilisés dans les scénarios suivants :
  - Vous disposez d'une équipe ou d'un groupe de ressources dédié qui exécute ces fonctions. Detective est utilisé de préférence par les équipes d'analystes de sécurité et Audit Manager est utile à vos équipes d'audit interne ou de conformité.
  - Vous souhaitez vous concentrer sur un ensemble d'outils de base tels que GuardDuty Security Hub CSPM au début de votre projet, puis vous appuyer sur ceux-ci en utilisant des services offrant des fonctionnalités supplémentaires.

Security OU — Compte Log Archive

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le schéma suivant illustre les services AWS de sécurité configurés dans le compte Log Archive.



Le compte Log Archive est dédié à l'ingestion et à l'archivage de tous les journaux et sauvegardes liés à la sécurité. Avec les journaux centralisés en place, vous pouvez surveiller, auditer et émettre des alertes en cas d'accès aux objets Amazon S3, d'activité non autorisée par identité, de modification de la politique IAM et d'autres activités critiques effectuées sur des ressources sensibles. Les objectifs de sécurité sont simples : il doit s'agir d'un stockage immuable, accessible uniquement par des mécanismes contrôlés, automatisés et surveillés, et conçu dans un souci de durabilité (par exemple, en utilisant les processus de réplication et d'archivage appropriés). Des contrôles peuvent être mis en œuvre en profondeur pour protéger l'intégrité et la disponibilité des journaux et du processus de gestion des journaux. Outre les contrôles préventifs, tels que l'attribution des rôles les moins privilégiés à utiliser pour l'accès et le chiffrement des journaux à l'aide d'une AWS KMS clé contrôlée, utilisez des contrôles de détection permettant de AWS Config surveiller (d'alerter et de corriger) cet ensemble d'autorisations en cas de modifications inattendues.

> **Considération relative à la conception**
>
> Les données du journal opérationnel utilisées par vos équipes chargées de l'infrastructure, des opérations et de la charge de travail recoupent souvent les données du journal utilisées par les équipes chargées de la sécurité, de l'audit et de la conformité. Nous vous recommandons de consolider les données de vos journaux opérationnels dans le compte Log Archive. En fonction de vos exigences spécifiques en matière de sécurité et de gouvernance, vous devrez peut-être filtrer les données du journal opérationnel enregistrées sur ce compte. Vous devrez peut-être également spécifier qui a accès aux données du journal opérationnel dans le compte Log Archive.

Types de journaux

Les principaux journaux affichés dans le AWS SRA incluent AWS CloudTrail (suivi de l'organisation), les journaux de flux Amazon VPC, les journaux d'accès d' CloudFront Amazon AWS WAF et les journaux DNS d'Amazon Route 53. Ces journaux fournissent un audit des actions entreprises (ou tentées) par un utilisateur, un rôle ou une entité réseau (identifié, par exemple, par une adresse IP). Service AWS D'autres types de journaux (par exemple, les journaux d'applications ou les journaux de base de données) peuvent également être capturés et archivés. Pour plus d'informations sur les sources de journalisation et les meilleures pratiques de journalisation, consultez la documentation de sécurité de chaque service.

Amazon S3 en tant que magasin de journaux central

De nombreuses informations de Services AWS journalisation dans Amazon S3, soit par défaut, soit exclusivement. AWS CloudTrail, Amazon VPC Flow Logs, Elastic Load Balancing GuardDuty AWS Config, Amazon et AWS WAF voici quelques exemples de services qui enregistrent des informations dans Amazon S3. Cela signifie que l'intégrité des journaux est assurée par l'intégrité des objets S3 ; la confidentialité des journaux est assurée par les contrôles d'accès aux objets S3 ; et la disponibilité des journaux est assurée par le biais du verrouillage des objets S3, des versions des objets S3 et des règles de cycle de vie S3. En enregistrant les informations dans un compartiment S3 dédié et centralisé qui réside dans un compte dédié, vous pouvez gérer ces journaux dans quelques compartiments et appliquer des contrôles de sécurité stricts, un accès et une séparation des tâches.

Dans le AWS SRA, les principaux journaux stockés dans Amazon S3 proviennent CloudTrail. Cette section décrit donc comment protéger ces objets. Ce guide s'applique également à tout autre objet

S3 créé par vos propres applications ou par d'autres Services AWS. Appliquez ces modèles chaque fois que vous avez des données dans Amazon S3 qui nécessitent une intégrité élevée, un contrôle d'accès renforcé et une conservation ou une destruction automatisées.

Tous les nouveaux objets (y compris les CloudTrail journaux) chargés dans des compartiments S3 sont chiffrés par défaut à l'aide du chiffrement côté serveur Amazon avec des clés de chiffrement gérées par Amazon S3 (SSE-S3). Cela permet de protéger les données au repos, mais le contrôle d'accès est contrôlé exclusivement par les politiques IAM. Pour fournir une couche de sécurité gérée supplémentaire, vous pouvez utiliser le chiffrement côté serveur avec des AWS KMS clés que vous gérez (SSE-KMS) sur tous les compartiments de sécurité S3. Cela ajoute un deuxième niveau de contrôle d'accès. Pour lire les fichiers journaux, un utilisateur doit disposer à la fois des autorisations de lecture Amazon S3 pour l'objet S3 et d'une stratégie ou d'un rôle IAM lui permettant de déchiffrer selon la politique de clé associée.

Deux options vous permettent de protéger ou de vérifier l'intégrité des objets de CloudTrail journal stockés dans Amazon S3. CloudTrail fournit une validation de l'intégrité du fichier journal afin de déterminer si un fichier journal a été modifié ou supprimé après CloudTrail sa livraison. L'autre option est S3 Object Lock.

Outre la protection du compartiment S3 lui-même, vous pouvez respecter le principe du moindre privilège pour les services de journalisation (par exemple CloudTrail) et le compte Log Archive. Par exemple, les utilisateurs disposant d'autorisations accordées par la politique IAM AWS gérée `AWSCloudTrail_FullAccess` peuvent désactiver ou reconfigurer les fonctions d'audit les plus sensibles et les plus importantes de leur compte. Comptes AWS Limitez l'application de cette politique IAM au moins de personnes possible.

Utilisez des contrôles de détection, tels que ceux fournis par AWS Config IAM Access Analyzer, pour surveiller (et alerter et corriger) cet ensemble plus large de contrôles préventifs en cas de changements inattendus.

Pour en savoir plus sur les meilleures pratiques de sécurité pour les compartiments S3, consultez la documentation Amazon S3, les conférences techniques en ligne et le billet de blog Les 10 meilleures pratiques de sécurité pour sécuriser les données dans Amazon S3.

Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation de l'accès public aux comptes de blocs Amazon S3. Ce module bloque l'accès public à Amazon S3 pour tous les comptes existants et futurs de l' AWS organisation.

Amazon Security Lake

AWS La SRA vous recommande d'utiliser le compte Log Archive comme compte d'administrateur délégué pour Amazon Security Lake. Dans ce cas, Security Lake collecte les journaux pris en charge dans des compartiments S3 dédiés sur le même compte que les autres journaux de sécurité recommandés par la SRA.

Pour protéger la disponibilité des journaux et le processus de gestion des journaux, les compartiments S3 pour Security Lake ne doivent être accessibles que par le service Security Lake ou par les rôles IAM gérés par Security Lake pour les sources ou les abonnés. Outre l'utilisation de contrôles préventifs, tels que l'attribution de rôles dotés de privilèges d'accès minimaux et le chiffrement des journaux à l'aide d'une AWS KMS clé contrôlée, utilisez des contrôles de détection permettant de surveiller (d'alerter et de corriger) cet AWS Config ensemble d'autorisations en cas de modifications inattendues.

L'administrateur de Security Lake peut activer la collecte de journaux au sein de votre AWS organisation. Ces journaux sont stockés dans des compartiments S3 régionaux du compte Log Archive. En outre, pour centraliser les journaux et faciliter le stockage et l'analyse, l'administrateur de Security Lake peut choisir une ou plusieurs régions cumulatives dans lesquelles les journaux de tous les compartiments S3 régionaux sont consolidés et stockés. Les journaux pris en charge Services AWS sont automatiquement convertis en un schéma open source standardisé appelé Open Cybersecurity Schema Framework (OCSF) et enregistrés au format Apache Parquet dans des compartiments Security Lake S3. Grâce au support OCSF, Security Lake normalise et consolide efficacement les données de sécurité provenant AWS d'autres sources de sécurité de l'entreprise afin de créer un référentiel unifié et fiable d'informations relatives à la sécurité.

Security Lake peut collecter des journaux associés aux événements AWS CloudTrail de gestion et aux événements de CloudTrail données pour Amazon S3 et AWS Lambda. Pour collecter les événements CloudTrail de gestion dans Security Lake, vous devez disposer d'au moins un journal d'organisation CloudTrail multirégional qui collecte les événements de CloudTrail gestion en lecture

et en écriture. La journalisation doit être activée pour le parcours. Un suivi multirégional fournit les fichiers journaux de plusieurs régions vers un seul compartiment S3 pour une seule Compte AWS. Si les régions se trouvent dans des pays différents, tenez compte des exigences en matière d'exportation de données pour déterminer si les sentiers multirégionaux peuvent être activés.

AWS Security Hub CSPM est une source de données native prise en charge dans Security Lake, et vous devez ajouter les résultats du Security Hub CSPM à Security Lake. Security Hub CSPM génère des résultats à partir de nombreuses intégrations différentes Services AWS et tierces. Ces résultats vous permettent d'avoir une vue d'ensemble de votre niveau de conformité et de savoir si vous suivez les recommandations AWS et les AWS Partner solutions de sécurité.

Pour obtenir de la visibilité et des informations exploitables à partir des journaux et des événements, vous pouvez interroger les données à l'aide d'outils tels qu'Amazon Athena, Amazon Service, OpenSearch Amazon Quick et de solutions tierces. Les utilisateurs qui ont besoin d'accéder aux données du journal Security Lake ne doivent pas accéder directement au compte Log Archive. Ils ne doivent accéder aux données qu'à partir du compte Security Tooling. Ils peuvent également utiliser d'autres sites Comptes AWS ou des sites sur site qui fournissent des outils d'analyse tels que OpenSearch Service, Quick, ou des outils tiers tels que des outils de gestion des informations et des événements de sécurité (SIEM). Pour donner accès aux données, l'administrateur doit configurer les abonnés Security Lake dans le compte Log Archive et configurer le compte qui a besoin d'accéder aux données en tant qu'abonné à accès aux requêtes. Pour plus d'informations, consultez Amazon Security Lake dans la section Security OU – Compte Security Tooling de ce guide.

Security Lake fournit une politique AWS gérée pour vous aider à gérer l'accès des administrateurs au service. Pour plus d'informations, consultez le guide de l'utilisateur de Security Lake. Il est recommandé de restreindre la configuration de Security Lake via les pipelines de développement et d'empêcher les modifications de configuration via les AWS consoles ou le AWS Command Line Interface (AWS CLI). En outre, vous devez définir des politiques IAM et des politiques de contrôle des services (SCPs) strictes afin de fournir uniquement les autorisations nécessaires à la gestion de Security Lake. Vous pouvez configurer les notifications pour détecter tout accès direct à ces compartiments S3.

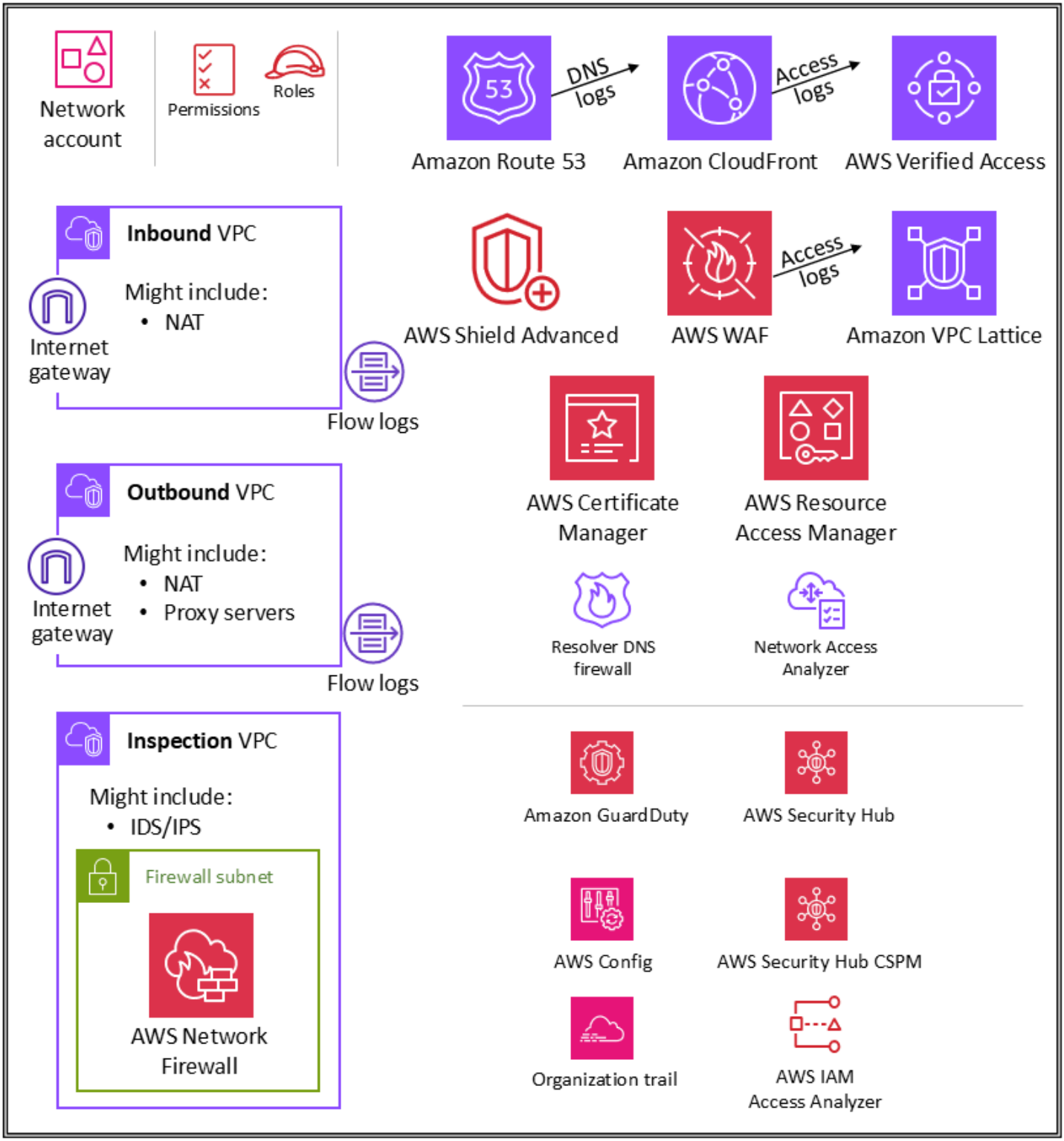
> **Considération relative à la conception**
>
> Lorsque vous activez CloudTrail des événements de gestion dans Security Lake, ils entraînent des frais pour Security Lake. La collecte des événements de CloudTrail gestion dans Security Lake nécessite un suivi organisationnel CloudTrail multirégional qui collecte les événements de CloudTrail gestion en lecture et en écriture. Ce premier sentier est disponible

sans frais pour vous. CloudTrail les événements de gestion ne représentent généralement qu'un faible pourcentage (environ 5 %) du total des CloudTrail événements. Cela s'applique aux clients qui utilisent AWS Control Tower ou disposent de CloudTrail journaux centralisés dans un compte Log Archive.

Infrastructure UO – Compte réseau

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le schéma suivant illustre les services de AWS sécurité configurés dans le compte réseau.



Le compte réseau gère la passerelle entre votre application et Internet en général. Il est important de protéger cette interface bidirectionnelle. Le compte Réseau isole les services, la configuration et le fonctionnement du réseau des charges de travail des applications individuelles, de la sécurité

et des autres infrastructures. Cette disposition permet non seulement de limiter la connectivité, les autorisations et le flux de données, mais aussi de favoriser la séparation des tâches et le moindre privilège pour les équipes qui ont besoin d'opérer sur ces comptes. En divisant le flux réseau en clouds privés virtuels entrants et sortants distincts (VPCs), vous pouvez protéger l'infrastructure et le trafic sensibles contre les accès indésirables. Le réseau entrant est généralement considéré comme présentant un risque plus élevé et doit faire l'objet d'un routage, d'une surveillance et d'une atténuation des problèmes potentiels appropriés. Ces comptes d'infrastructure hériteront des barrières de protection d'autorisation du compte de gestion de l'organisation et de l'UO de l'infrastructure. Les équipes de mise en réseau (et de sécurité) gèrent la majorité de l'infrastructure de ce compte.

Architecture réseau

Bien que la conception et les spécificités du réseau dépassent le cadre de ce document, nous recommandons les trois options suivantes pour la connectivité réseau entre les différents comptes : peering VPC, AWS PrivateLink et. AWS Transit Gateway Les normes opérationnelles, les budgets et les besoins spécifiques en matière de bande passante sont des éléments importants à prendre en compte lors du choix de l'un d'entre eux.

- Peering VPC – Le moyen le plus simple d'en connecter deux VPCs est d'utiliser l'appairage VPC. Une connexion permet une connectivité bidirectionnelle complète entre les VPCs. VPCs qui se trouvent dans des comptes séparés et Régions AWS peuvent également être comparés entre eux. À grande échelle, lorsque vous en avez des dizaines, voire des centaines VPCs, leur interconnexion par le biais du peering se traduit par un maillage de centaines, voire de milliers de connexions d'appairage, ce qui peut être difficile à gérer et à faire évoluer. Il est préférable d'utiliser l'appairage VPC lorsque les ressources d'un VPC doivent communiquer avec les ressources d'un autre VPC, que l'environnement des deux VPCs est contrôlé et sécurisé et que le nombre de personnes à connecter est inférieur VPCs à 10 (pour permettre la gestion individuelle de chaque connexion).
- AWS PrivateLink– PrivateLink fournit une connectivité privée entre VPCs les services et les applications. Vous pouvez créer votre propre application dans votre VPC et la configurer en tant que service PrivateLink alimenté (appelé service de point de terminaison). Les autres AWS principaux peuvent créer une connexion entre leur VPC et votre service de point de terminaison en utilisant un point de terminaison VPC d'interface ou un point de terminaison Gateway Load Balancer, selon le type de service. Lorsque vous l'utilisez PrivateLink, le trafic de service ne passe pas par un réseau routable publiquement. À utiliser PrivateLink lorsque vous disposez d'une configuration client-serveur dans laquelle vous souhaitez accorder à un ou plusieurs

consommateurs un accès VPCs unidirectionnel à un service ou à un ensemble d'instances spécifique dans le VPC du fournisseur de services. C'est également une bonne option lorsque les adresses IP des clients et des serveurs VPCs se chevauchent, car elle PrivateLink utilise des interfaces réseau élastiques au sein du VPC client afin d'éviter tout conflit d'IP avec le fournisseur de services.

- AWS Transit Gateway– Transit Gateway fournit une hub-and-spoke conception pour la connexion VPCs et les réseaux sur site en tant que service entièrement géré sans que vous ayez à provisionner des dispositifs virtuels. AWS gère la haute disponibilité et l'évolutivité. Une passerelle de transport en commun est une ressource régionale qui peut relier des VPCs milliers de personnes Région AWS. Vous pouvez associer votre connectivité hybride (VPN et AWS Direct Connect connexions) à une passerelle de transit unique, consolidant et contrôlant ainsi l'ensemble de la configuration de routage de votre AWS entreprise en un seul endroit. Une passerelle de transit résout la complexité liée à la création et à la gestion de plusieurs connexions d’appairage de VPC à grande échelle. Il s’agit de la solution par défaut pour la plupart des architectures de réseau, mais des besoins spécifiques en matière de coût, de bande passante et de latence peuvent faire de l’appairage VPC une solution mieux adaptée à vos besoins.

VPC entrant (d’entrée)

Le VPC entrant est destiné à accepter, inspecter et acheminer les connexions réseau initiées depuis l'extérieur de l'application. En fonction des spécificités de l’application, vous pouvez vous attendre à voir une traduction d’adresses réseau (NAT) dans ce VPC. Les journaux de flux de ce VPC sont capturés et stockés dans le compte d’archivage des journaux.

VPC sortant (de sortie)

Le VPC sortant est destiné à gérer les connexions réseau initiées depuis l’application. En fonction des spécificités de l'application, vous pouvez vous attendre à voir du trafic NAT, des points de Service AWS terminaison VPC spécifiques et l'hébergement de points de terminaison d'API externes dans ce VPC. Les journaux de flux de ce VPC sont capturés et stockés dans le compte d’archivage des journaux.

VPC d’inspection

Un VPC d'inspection dédié fournit une approche simplifiée et centralisée pour gérer les inspections entre VPCs (dans le même ou dans des environnements différents Régions AWS), Internet et les

réseaux sur site. Pour le AWS SRA, assurez-vous que tout le trafic entre les deux VPCs passe par le VPC d'inspection et évitez d'utiliser le VPC d'inspection pour toute autre charge de travail.

AWS Network Firewall

AWS Network Firewallest un service de pare-feu réseau géré à haute disponibilité pour votre VPC. Il vous permet de déployer et de gérer sans effort l'inspection dynamique, la prévention et la détection des intrusions, ainsi que le filtrage Web pour protéger vos réseaux virtuels sur. AWS Vous pouvez utiliser Network Firewall pour déchiffrer les sessions TLS et inspecter le trafic entrant et sortant. Pour plus d'informations sur la configuration de Network Firewall, consultez le billet de blog AWS Network Firewall — New Managed Firewall Service in VPC.

Vous utilisez un pare-feu par zone de disponibilité dans votre VPC. Pour chaque zone de disponibilité, vous choisissez un sous-réseau pour héberger le point de terminaison du pare-feu qui filtre votre trafic. Le point de terminaison du pare-feu d'une zone de disponibilité peut protéger tous les sous-réseaux de la zone, à l'exception du sous-réseau dans lequel il se trouve. Selon le cas d'utilisation et le modèle de déploiement, le sous-réseau du pare-feu peut être public ou privé. Le pare-feu est totalement transparent au flux de trafic et n'effectue pas de traduction d'adresses réseau (NAT). Il préserve l'adresse de la source et de la destination. Dans cette architecture de référence, les points de terminaison du pare-feu sont hébergés dans un VPC d'inspection. Tout le trafic en provenance du VPC entrant et à destination du VPC sortant est acheminé via ce sous-réseau de pare-feu pour être inspecté.

Network Firewall rend l'activité du pare-feu visible en temps réel grâce aux CloudWatch métriques Amazon et offre une visibilité accrue du trafic réseau en envoyant des journaux à Amazon Simple Storage Service (Amazon S3) CloudWatch et à Amazon Data Firehose. Network Firewall est interopérable avec votre approche de sécurité existante, y compris les technologies des AWS partenaires. Vous pouvez également importer des ensembles de règles Suricata existants, qui peuvent avoir été rédigés en interne ou provenir de fournisseurs tiers ou de plateformes open source.

Dans le AWS SRA, Network Firewall est utilisé dans le compte réseau car les fonctionnalités du service axées sur le contrôle du réseau correspondent à l'intention du compte.

Considérations relatives à la conception

- AWS Firewall Manager prend en charge le Network Firewall, ce qui vous permet de configurer et de déployer de manière centralisée les règles du Network Firewall au sein de votre organisation. (Pour plus de détails, consultez la section Utilisation des AWS

Network Firewall politiques dans Firewall Manager dans la AWS documentation.) Lorsque vous configurez Firewall Manager, celui-ci crée automatiquement un pare-feu avec des ensembles de règles VPCs que vous spécifiez dans les comptes. Il déploie également un point de terminaison dans un sous-réseau dédié pour chaque zone de disponibilité contenant des sous-réseaux publics. Dans le même temps, toute modification apportée à l'ensemble de règles configuré de manière centralisée est automatiquement mise à jour en aval sur les pare-feux Network Firewall déployés.

- Plusieurs modèles de déploiement sont disponibles avec Network Firewall. Le bon modèle dépend de votre cas d'utilisation et de vos besoins. Voici quelques exemples :
  - Modèle de déploiement distribué dans lequel Network Firewall est déployé de manière individuelle VPCs.
  - Modèle de déploiement centralisé dans lequel Network Firewall est déployé dans un VPC centralisé pour le trafic est-ouest (VPC à VPC) ou nord-sud (entrée et sortie Internet, sur site).
  - Modèle de déploiement combiné dans lequel Network Firewall est déployé dans un VPC centralisé pour le trafic est-ouest et un sous-ensemble du trafic nord-sud.
- En guise de bonne pratique, n'utilisez pas le sous-réseau Network Firewall pour déployer d'autres services. En effet, Network Firewall ne peut pas inspecter le trafic provenant de sources ou de destinations situées dans le sous-réseau du pare-feu.

Analyseur d'accès réseau

L'analyseur d'accès réseau est une fonctionnalité d'Amazon VPC qui identifie les accès réseau non intentionnels à vos ressources. Vous pouvez utiliser l'analyseur d'accès réseau pour valider la segmentation du réseau, identifier les ressources accessibles depuis Internet ou accessibles uniquement à partir de plages d'adresses IP fiables, et vérifier que vous disposez des contrôles réseau appropriés sur tous les chemins réseau.

Network Access Analyzer utilise des algorithmes de raisonnement automatisés pour analyser les chemins réseau qu'un paquet peut emprunter entre les ressources d'un AWS réseau et produit des résultats pour les chemins correspondant à l'étendue d'accès réseau que vous avez définie. L'analyseur d'accès réseau effectue une analyse statique de la configuration d'un réseau, ce qui signifie qu'aucun paquet n'est transmis sur le réseau dans le cadre de cette analyse.

Les règles d’accessibilité du réseau Amazon Inspector fournissent une fonctionnalité connexe. Les résultats générés par ces règles sont utilisés dans le compte de l’application. Network Access Analyzer et Network Reachability utilisent tous deux les dernières technologies issues d'une initiative de sécuritéAWS éprouvée, et ils appliquent cette technologie dans différents domaines d'intérêt. Le package Network Reachability se concentre spécifiquement sur les EC2 instances et leur accessibilité à Internet.

Le compte réseau définit l'infrastructure réseau critique qui contrôle le trafic entrant et sortant de votre AWS environnement. Ce trafic doit être étroitement surveillé. Dans le AWS SRA, l'analyseur d'accès réseau est utilisé dans le compte réseau pour aider à identifier les accès réseau non intentionnels, à identifier les ressources accessibles à Internet via des passerelles Internet et à vérifier que les contrôles réseau appropriés tels que les pare-feux réseau et les passerelles NAT sont présents sur tous les chemins réseau entre les ressources et les passerelles Internet.

> Considération relative à la conception
>
> Network Access Analyzer est une fonctionnalité d'Amazon VPC, et il peut être utilisé dans Compte AWS tous ceux dotés d'un VPC. Les administrateurs réseau peuvent obtenir des rôles IAM multicomptes bien définis afin de vérifier que les chemins réseau approuvés sont appliqués au sein de chacun d'entre eux. Compte AWS

AWS RAM

AWS Resource Access Manager(AWS RAM) vous permet de partager en toute sécurité les AWS ressources que vous créez dans l'un Compte AWS avec l'autre Comptes AWS.AWS RAM fournit un emplacement central pour gérer le partage des ressources et pour standardiser cette expérience entre les comptes. Cela simplifie la gestion des ressources tout en tirant parti de l’isolation administrative et de la facturation, et réduit la portée des avantages en matière de limitation de l’impact offerts par une stratégie de plusieurs comptes. Si votre compte est géré par AWS Organizations, vous AWS RAM permet de partager des ressources avec tous les comptes de l'organisation, ou uniquement avec les comptes d'une ou de plusieurs unités organisationnelles spécifiées (OUs). Vous pouvez également partager avec un utilisateur spécifique Comptes AWS par identifiant de compte, que le compte fasse partie ou non d'une organisation. Vous pouvez également partager certains types de ressources pris en charge avec des rôles et des utilisateurs IAM spécifiques.

AWS RAM vous permet de partager des ressources qui ne prennent pas en charge les politiques basées sur les ressources IAM, telles que les sous-réseaux VPC et les règles Route 53. De plus AWS RAM, les propriétaires d'une ressource peuvent voir quels principaux ont accès aux ressources individuelles qu'ils ont partagées. Les responsables IAM peuvent récupérer directement la liste des ressources partagées avec eux, ce qu'ils ne peuvent pas faire avec les ressources partagées par les politiques de ressources IAM. S'il AWS RAM est utilisé pour partager des ressources en dehors de votre AWS organisation, un processus d'invitation est lancé. Le destinataire doit accepter l'invitation avant que l'accès aux ressources ne soit accordé. Cela fournit des freins et contrepoids supplémentaires.

AWS RAM est invoqué et géré par le propriétaire de la ressource, dans le compte sur lequel la ressource partagée est déployée. Un cas d'utilisation courant AWS RAM illustré dans le AWS SRA est que les administrateurs réseau partagent des sous-réseaux VPC et des passerelles de transit avec l'ensemble de l'organisation. AWS Cela permet de découpler les fonctions de gestion du réseau Compte AWS et contribue à la séparation des tâches. Pour plus d'informations sur le partage VPC, consultez le AWS billet de blog Partage VPC : une nouvelle approche de la gestion des comptes multiples et des VPC et le livre blanc sur l'infrastructure réseau.AWS

Considération relative à la conception

Bien AWS RAM qu'un service soit déployé uniquement dans le compte réseau de la AWS SRA, il est généralement déployé sur plusieurs comptes. Par exemple, vous pouvez centraliser la gestion de votre lac de données sur un seul compte de lac de données, puis partager les ressources du catalogue de AWS Lake Formation données (bases de données et tables) avec d'autres comptes de votre AWS organisation. Pour plus d'informations, consultez la AWS Lake Formation documentation et le billet de AWS blog Partagez vos données en toute sécurité entre Comptes AWS utilisateurs AWS Lake Formation. En outre, les administrateurs de sécurité peuvent AWS RAM suivre les meilleures pratiques lorsqu'ils créent une AWS Autorité de certification privée hiérarchie. CAs peuvent être partagés avec des tiers externes, qui peuvent émettre des certificats sans avoir accès à la hiérarchie de l'autorité de certification. Cela permet aux organisations d’origine de limiter et de révoquer l’accès des tiers.

Accès vérifié par AWS

Accès vérifié par AWSfournit un accès sécurisé aux applications et aux ressources de l'entreprise sans VPN. Il améliore le niveau de sécurité et permet d'appliquer un accès Zero Trust en évaluant chaque demande d'accès en temps réel par rapport à des exigences prédéfinies. Vous pouvez définir une stratégie d'accès unique pour chaque application avec des conditions basées sur les données d'identité et la position de l'appareil. Verified Access fournit un accès sécurisé aux applications HTTP (S), telles que les applications basées sur un navigateur, et aux applications non HTTP (S) via les protocoles TCP, SSH et RDP pour des applications telles que les référentiels Git, les bases de données et les groupes d'instances. EC2 Ils sont accessibles à l'aide d'un terminal de ligne de commande ou d'une application de bureau. L'accès vérifié simplifie également les opérations de sécurité en aidant les administrateurs à définir et à surveiller efficacement les stratégies d'accès. Cela libère du temps pour mettre à jour les stratégies, répondre aux incidents de sécurité et de connectivité, et effectuer des audits de conformité. Verified Access prend également en charge l'intégration AWS WAF pour vous aider à filtrer les menaces courantes telles que l'injection SQL et les scripts intersites (XSS). Verified Access est parfaitement intégré AWS IAM Identity Center, ce qui permet aux utilisateurs de s'authentifier auprès de fournisseurs d'identité tiers basés sur le protocole SAML (). IdPs Si vous disposez déjà d'une solution IdP personnalisée compatible avec OpenID Connect (OIDC), l'accès vérifié peut également authentifier les utilisateurs en se connectant directement à votre IdP. L'accès vérifié enregistre chaque tentative d'accès afin que vous puissiez répondre rapidement aux incidents de sécurité et aux demandes d'audit. Verified Access prend en charge la livraison de ces journaux à Amazon Simple Storage Service (Amazon S3), Amazon Logs et CloudWatch Amazon Data Firehose.

L'accès vérifié prend en charge deux modèles d'applications d'entreprise courants : internes et orientées vers Internet. L'accès vérifié s'intègre aux applications à l'aide d'Application Load Balancer ou d'interfaces réseau élastiques. Si vous utilisez un Application Load Balancer, Verified Access nécessite un équilibreur de charge interne. Comme Verified Access est compatible AWS WAF au niveau de l'instance, une application existante intégrée à un Application Load Balancer peut déplacer les politiques de l'équilibreur de charge vers l'instance Verified Access. AWS WAF Une application d'entreprise est représentée sous la forme d'un point de terminaison d'accès vérifié. Chaque point de terminaison est associé à un groupe d'accès vérifié et hérite de la stratégie d'accès du groupe. Un groupe d'accès vérifié est un ensemble de points de terminaison d'accès vérifié et une stratégie d'accès vérifié au niveau du groupe. Les groupes simplifient la gestion des stratégies et permettent aux administrateurs informatiques de définir des critères de base. Les propriétaires d'applications peuvent en outre définir des stratégies détaillées en fonction de la sensibilité de l'application.

Dans le AWS SRA, l'accès vérifié est hébergé dans le compte réseau. L'équipe informatique centrale met en place des configurations gérées de manière centralisée. Par exemple, les membres de l'équipe peuvent connecter des fournisseurs de confiance tels que des fournisseurs d'identité (par exemple, Okta) et des fournisseurs de confiance d'appareils (par exemple, Jamf), créer des groupes et déterminer la stratégie au niveau du groupe. Ces configurations peuvent ensuite être partagées avec des dizaines, des centaines ou des milliers de comptes de charge de travail en utilisant AWS RAM. Cela permet aux équipes chargées des applications de gérer les points de terminaison sous-jacents qui gèrent leurs applications sans avoir à surcharger les autres équipes. AWS RAM fournit un moyen évolutif de tirer parti de l'accès vérifié pour les applications d'entreprise hébergées sur différents comptes de charge de travail.

> Considération relative à la conception
>
> Vous pouvez regrouper les points de terminaison des applications qui ont des exigences de sécurité similaires afin de simplifier l'administration des stratégies, puis partager le groupe avec les comptes d'application. Toutes les applications du groupe partagent la même stratégie de groupe. Si une application du groupe nécessite une stratégie spécifique en raison d'un cas particulier, vous pouvez appliquer une stratégie au niveau de l'application pour cette application.

Amazon VPC Lattice

Amazon VPC Lattice est un service de mise en réseau d'applications qui connecte, surveille et sécurise les communications. service-to-service Un service, souvent appelé microservice, est une unité logicielle déployable indépendamment qui exécute une tâche spécifique. VPC Lattice gère automatiquement la connectivité réseau et le routage au niveau de la couche applicative entre les services à travers VPCs et Comptes AWS sans que vous ayez à gérer la connectivité réseau sous-jacente, les équilibreurs de charge frontaux ou les proxys annexes. Il s'agit d'un proxy entièrement géré au niveau de l'application qui fournit un routage au niveau de l'application basé sur les caractéristiques de la demande telles que les chemins et les en-têtes. Le VPC Lattice est intégré à l'infrastructure VPC. Il fournit donc une approche cohérente pour un large éventail de types de calcul tels qu'Amazon Elastic Compute Cloud (Amazon), Amazon Elastic Kubernetes Service (Amazon EKS EC2) et. AWS Lambda VPC Lattice prend également en charge le routage pondéré pour les déploiements de type blue/green canary. Vous pouvez utiliser VPC Lattice pour créer un réseau de services avec une limite logique qui implémente automatiquement la découverte et la

connectivité des services. VPC Lattice s'intègre à IAM pour l'authentification et l'autorisation à l'aide de service-to-service politiques d'authentification.

VPC Lattice s'intègre AWS RAM pour permettre le partage de services et de réseaux de services. AWS SRA décrit une architecture distribuée dans laquelle les développeurs ou les propriétaires de services créent des services VPC Lattice dans leur compte d'application. Les propriétaires de services définissent les écouteurs, les règles de routage et les groupes cibles ainsi que les stratégies d'authentification. Ils partagent ensuite les services avec d'autres comptes et les associent aux réseaux de services VPC Lattice. Ces réseaux sont créés par les administrateurs réseau dans le compte réseau et partagés avec le compte d'application. Les administrateurs réseau configurent les stratégies d'authentification au niveau du réseau de services et la surveillance. Les administrateurs associent VPCs les services VPC Lattice à un ou plusieurs réseaux de services. Pour une présentation détaillée de cette architecture distribuée, consultez le billet de AWS blog Créez une connectivité multi-comptes multi-VPC sécurisée pour vos applications avec Amazon VPC Lattice

Considérations relatives à la conception

- En fonction du modèle opérationnel de votre organisation en matière de services ou de visibilité du réseau de services, les administrateurs réseau peuvent partager leurs réseaux de services et donner aux propriétaires de services le contrôle nécessaire pour associer leurs services et VPCs à ces réseaux de services. Les propriétaires de services peuvent également partager leurs services et les administrateurs de réseaux peuvent associer les services à des réseaux de services.
- Un client peut envoyer des demandes à des services associés à un réseau de services uniquement s'il se trouve dans un VPC associé au même réseau de services. Le trafic client qui traverse une connexion d'appairage de VPC ou une passerelle de transit est refusé.

Sécurit à la périphérie

La sécurité périphérique implique généralement trois types de protection : la diffusion sécurisée du contenu, la protection du réseau et de la couche applicative, et l'atténuation des attaques par déni de service (DDoS) distribué. Les contenus tels que les données, les vidéos, les applications APIs doivent être diffusés rapidement et en toute sécurité, en utilisant la version recommandée de TLS pour chiffrer les communications entre les points de terminaison. Le contenu doit également être soumis à des restrictions d'accès via des cookies signés et une authentification par jeton. URLs

La sécurité au niveau des applications doit être conçue pour contrôler le trafic des robots, bloquer les modèles d'attaque courants tels que l'injection SQL ou les scripts inter-site (XSS) et fournir une visibilité sur le trafic Web. À la périphérie, l'atténuation DDo S fournit une couche de défense importante qui garantit la disponibilité continue des opérations et services commerciaux critiques. Les applications APIs doivent également être protégées contre les inondations SYN, les inondations UDP ou autres attaques par réflexion, et bénéficier d'une atténuation intégrée pour mettre fin aux attaques de base au niveau de la couche réseau.

AWS propose plusieurs services destinés à fournir un environnement sécurisé, du cloud central à la périphérie du AWS réseau. Amazon CloudFront AWS Certificate Manager (ACM), AWS Shield AWS WAF, et Amazon Route 53 travaillent ensemble pour créer un périmètre de sécurité flexible à plusieurs niveaux. Avec CloudFront APIs, le contenu ou les applications peuvent être diffusés via HTTPS en utilisant TLSv1 .3 pour crypter et sécuriser les communications entre les clients spectateurs et CloudFront. Vous pouvez utiliser ACM pour créer un certificat SSL personnalisé et le déployer gratuitement sur une CloudFront distribution. ACM gère automatiquement le renouvellement des certificats. Shield est un service de protection DDo S géré qui permet de protéger les applications qui s'exécutent sur AWS. Il fournit une détection dynamique et des mesures d'atténuation automatiques en ligne qui minimisent les temps d'arrêt et la latence des applications. AWS WAF vous permet de créer des règles pour filtrer le trafic Web en fonction de conditions spécifiques (adresses IP, en-têtes et corps HTTP, ou personnalisé URIs), des attaques Web courantes et des robots omniprésents. Route 53 est un service Web DNS hautement disponible et évolutif. Route 53 connecte les demandes des utilisateurs aux applications Internet exécutées sur site AWS ou sur site. La AWS SRA adopte une architecture d'entrée réseau centralisée en utilisant AWS Transit Gateway, hébergée dans le compte réseau, de sorte que l'infrastructure de sécurité périphérique est également centralisée dans ce compte.

Amazon CloudFront

Amazon CloudFront est un réseau de diffusion de contenu (CDN) sécurisé qui fournit une protection intrinsèque contre les tentatives communes de couche réseau et de transport DDo S. Vous pouvez diffuser votre contenu ou vos applications à l'aide de certificats TLS, et les fonctionnalités TLS avancées sont activées automatiquement. APIs Vous pouvez utiliser AWS Certificate Manager (ACM) pour créer un certificat TLS personnalisé et appliquer les communications HTTPS entre les utilisateurs et CloudFront, comme décrit plus loin dans la section ACM. Vous pouvez également exiger que les communications entre CloudFront et votre origine personnalisée mettent en œuvre end-to-end le chiffrement pendant le transit. Pour ce scénario, vous devez installer un certificat TLS sur votre serveur d'origine. Si votre origine est un équilibreur de charge élastique, vous pouvez

utiliser un certificat généré par ACM ou un certificat validé par une autorité de certification (CA) tierce et importé dans ACM. Si les points de terminaison du site Web du compartiment S3 servent d'origine à CloudFront, vous ne pouvez pas configurer CloudFront pour utiliser le protocole HTTPS avec votre origine, car Amazon S3 ne prend pas en charge le protocole HTTPS pour les points de terminaison de sites Web. (Toutefois, vous pouvez toujours exiger le protocole HTTPS entre les utilisateurs et CloudFront.) Pour toutes les autres origines qui prennent en charge l'installation de certificats HTTPS, vous devez utiliser un certificat signé par une autorité de certification tierce de confiance.

CloudFront propose plusieurs options pour sécuriser et restreindre l'accès à votre contenu. Par exemple, il peut restreindre l'accès à votre origine Amazon S3 en utilisant des cookies signés URLs et signés. Pour plus d'informations, voir Configurer l'accès sécurisé et restreindre l'accès au contenu dans la CloudFront documentation.

Le AWS SRA illustre les CloudFront distributions centralisées dans le compte réseau, car elles s'alignent sur le modèle de réseau centralisé mis en œuvre à l'aide AWS Transit Gateway de. En déployant et en gérant les CloudFront distributions dans le compte réseau, vous bénéficiez des avantages des contrôles centralisés. Vous pouvez gérer toutes les CloudFront distributions en un seul endroit, ce qui facilite le contrôle d'accès, la configuration des paramètres et le suivi de l'utilisation sur tous les comptes. En outre, vous pouvez gérer les certificats ACM, les enregistrements DNS et la CloudFront journalisation à partir d'un compte centralisé.

Le tableau CloudFront de bord de sécurité fournit de la AWS WAF visibilité et des contrôles directement dans votre CloudFront distribution. Vous bénéficiez d'une visibilité sur les principales tendances en matière de sécurité de votre application, le trafic autorisé et bloqué et l'activité des robots. Vous pouvez utiliser des outils d'investigation tels que des analyseurs visuels de journaux et des contrôles de blocage intégrés pour isoler les modèles de trafic et bloquer le trafic sans interroger les journaux ni écrire de règles de sécurité.

Considérations relatives à la conception

- Vous pouvez également effectuer le déploiement dans le CloudFront cadre de l'application dans le compte d'application. Dans ce scénario, l'équipe chargée de l'application prend des décisions telles que la manière dont les CloudFront distributions sont déployées, détermine les politiques de cache appropriées et assume la responsabilité de la gouvernance, de l'audit et de la surveillance des CloudFront distributions. En répartissant les CloudFront distributions sur plusieurs comptes, vous pouvez bénéficier de quotas de service supplémentaires. Autre avantage, vous pouvez utiliser la configuration inhérente et

automatisée CloudFront de l'identité d'accès à l'origine (OAI) et du contrôle d'accès aux origines (OAC) pour restreindre l'accès aux origines Amazon S3.

- Lorsque vous diffusez du contenu Web via un CDN tel que celui-ci CloudFront, vous devez empêcher les spectateurs de contourner le CDN et d'accéder directement à votre contenu d'origine. Pour obtenir cette restriction d'accès à l'origine, vous pouvez utiliser CloudFront et AWS WAF ajouter des en-têtes personnalisés et vérifier les en-têtes avant de transférer les demandes à votre origine personnalisée. Pour une explication détaillée de cette solution, consultez le billet de blog sur la AWS sécurité How to enhance Amazon CloudFront Origin Security with AWS WAF and AWS Secrets Manager. Une autre méthode consiste à limiter uniquement la liste de CloudFront préfixes dans le groupe de sécurité associé à l'Application Load Balancer. Cela permettra de garantir que seule une CloudFront distribution peut accéder à l'équilibreur de charge.

AWS WAF

AWS WAFest un pare-feu pour applications Web qui aide à protéger vos applications Web contre les exploits Web tels que les vulnérabilités courantes et les robots susceptibles d'affecter la disponibilité des applications, de compromettre la sécurité ou de consommer des ressources excessives. Il peut être intégré à une CloudFront distribution Amazon, à une API REST Amazon API Gateway, à un Application Load Balancer, à une API AWS AppSync GraphQL, à un groupe d'utilisateurs Amazon Cognito et au service. AWS App Runner

AWS WAF utilise des listes de contrôle d'accès Web (ACLs) pour protéger un ensemble de AWS ressources. Une ACL Web est un ensemble de règles qui définit les critères d'inspection et une action associée à effectuer (bloquer, autoriser, compter ou exécuter un contrôle par bot) si une requête Web répond aux critères. AWS WAF fournit un ensemble de règles gérées qui fournissent une protection contre les vulnérabilités courantes des applications. Ces règles sont élaborées et gérées par AWS AWS nos partenaires. AWS WAF propose également un langage de règles puissant pour créer des règles personnalisées. Vous pouvez utiliser des règles personnalisées pour définir des critères d’inspection adaptés à vos besoins particuliers. Il peut s’agir par exemple de restrictions IP, de restrictions géographiques ou de versions personnalisées de règles gérées qui s’adaptent mieux au comportement de votre application spécifique.

AWS WAF fournit un ensemble de règles intelligentes gérées par niveaux pour les bots courants et ciblés et la protection contre le piratage de compte (ATP). Des frais d’abonnement et des frais d’inspection du trafic vous sont facturés lorsque vous utilisez le contrôle des bots et les groupes de

règles ATP. C'est pourquoi nous vous recommandons de surveiller d'abord votre trafic et de décider ensuite de ce que vous allez utiliser. Vous pouvez utiliser les tableaux de bord de gestion des bots et de prise de contrôle de compte disponibles gratuitement sur la AWS WAF console pour surveiller ces activités, puis décider si vous avez besoin d'un groupe de AWS WAF règles de niveau intelligent.

Dans le AWS SRA, AWS WAF est intégré CloudFront au compte réseau. Dans cette configuration, le traitement des AWS WAF règles s'effectue aux emplacements périphériques plutôt qu'au sein du VPC. Cela permet de filtrer le trafic malveillant plus près de l'utilisateur final qui a demandé le contenu, et d'empêcher le trafic malveillant d'entrer dans votre réseau principal.

Vous pouvez envoyer AWS WAF des journaux complets vers un compartiment S3 du compte Log Archive en configurant l'accès entre comptes au compartiment S3. Pour plus d'informations, consultez l'article AWS Re:Post à ce sujet.

Considérations relatives à la conception

- Comme alternative au déploiement AWS WAF centralisé dans le compte réseau, certains cas d'utilisation sont mieux satisfaits AWS WAF en déployant dans le compte d'application. Par exemple, vous pouvez choisir cette option lorsque vous déployez vos CloudFront distributions dans votre compte d'application ou que vous utilisez des équilibreurs de charge d'application destinés au public, ou si vous utilisez API Gateway devant vos applications Web. Si vous décidez de déployer AWS WAF dans chaque compte d'application, utilisez-le AWS Firewall Manager pour gérer les AWS WAF règles de ces comptes à partir du compte Security Tooling centralisé.
- Vous pouvez également ajouter des AWS WAF règles générales au niveau de la CloudFront couche et des AWS WAF règles supplémentaires spécifiques à l'application dans une ressource régionale telle que l'Application Load Balancer ou la passerelle API.

AWS Shield

AWS Shieldest un service de protection DDo S géré qui protège les applications qui s'exécutent sur AWS. Il existe deux niveaux de Shield : Shield Standard et Shield Advanced. Shield Standard fournit à tous les AWS clients une protection contre les événements d'infrastructure les plus courants (couches 3 et 4) sans frais supplémentaires. Shield Advanced fournit des mesures d'atténuation automatiques plus sophistiquées pour les événements non autorisés qui ciblent les applications sur les zones hébergées Amazon EC2, Elastic Load Balancing (Elastic Load Balancing) et Route

53 protégées. CloudFront AWS Global Accelerator Si vous possédez des sites Web très visibles ou si vous êtes sujet à de fréquentes attaques DDo S, vous pouvez envisager les fonctionnalités supplémentaires proposées par Shield Advanced.

Vous pouvez utiliser la fonction d'atténuation automatique de la couche DDo S de Shield Advanced pour configurer Shield Advanced afin de réagir automatiquement afin d'atténuer les attaques de la couche application (couche 7) contre vos CloudFront distributions protégées, les équilibreurs de charge Elastic Load Balancing (Elastic Load Balancing) (Application, Network et Classic), les zones hébergées Amazon Route 53, les adresses IP Amazon EC2 Elastic et les accélérateurs AWS Global Accelerator standard. Lorsque vous activez cette fonctionnalité, Shield Advanced génère automatiquement des AWS WAF règles personnalisées pour atténuer les attaques DDo S. Shield Advanced vous donne également accès à la AWS Shield Response Team (SRT). Vous pouvez contacter SRT à tout moment pour créer et gérer des mesures d'atténuation personnalisées pour votre application ou lors d'une attaque DDo S active. Si vous souhaitez que SRT surveille de manière proactive vos ressources protégées et vous contacte lors d'une tentative DDo S, pensez à activer la fonctionnalité d'engagement proactif.

Considérations relatives à la conception

- Si vos charges de travail sont dirigées par des ressources connectées à Internet dans le compte de l'application, telles qu'un Application Load Balancer ou un Network Load Balancer CloudFront, configurez Shield Advanced dans le compte Application et ajoutez ces ressources à la protection Shield. Vous pouvez l'utiliser AWS Firewall Manager pour configurer ces options à grande échelle.
- Si le flux de données comporte plusieurs ressources, par exemple une CloudFront distribution devant un Application Load Balancer, utilisez uniquement la ressource du point d'entrée comme ressource protégée. Cela vous évitera de payer deux fois les frais de transfert de données en sortie (DTO) pour deux ressources.
- Shield Advanced enregistre les statistiques que vous pouvez surveiller sur Amazon CloudWatch. (Pour plus d'informations, consultez la section Surveillance avec Amazon CloudWatch dans la AWS documentation.) Configurez des CloudWatch alarmes pour recevoir des notifications SNS à votre centre de sécurité lorsqu'un événement DDo S est détecté. En cas de suspicion d'événement DDo S, contactez l'équipe de support aux AWS entreprises en déposant un ticket d'assistance et en lui attribuant la priorité la plus élevée. L'équipe Enterprise Support inclura l'équipe Shield Response Team (SRT) lors de

la gestion de l'événement. En outre, vous pouvez préconfigurer la fonction Lambda d' AWS Shield engagement pour créer un ticket d'assistance et envoyer un e-mail à l'équipe SRT.

AWS Certificate Manager (ACM)

AWS Certificate Manager(ACM) vous permet de provisionner, de gérer et de déployer des certificats TLS publics et privés à utiliser avec Services AWS vos ressources internes connectées. Avec ACM, vous pouvez rapidement demander un certificat, le déployer sur des AWS ressources intégrées à ACM, telles que les équilibreurs de charge Elastic Load Balancing, les CloudFront distributions et sur Amazon API APIs Gateway, et laisser ACM gérer les renouvellements de certificats. Lorsque vous demandez des certificats publics ACM, il n'est pas nécessaire de générer une paire de clés ou une demande de signature de certificat (CSR), de soumettre un CSR à une autorité de certification (CA) ou de télécharger et d'installer le certificat lorsqu'il est reçu. ACM offre également la possibilité d'importer des certificats TLS émis par des tiers CAs et de les déployer avec les services intégrés ACM. Lorsque vous utilisez ACM pour gérer des certificats, les clés privées des certificats sont protégées et stockées de manière sécurisée grâce à un chiffrement renforcé et aux meilleures pratiques de gestion des clés. Avec ACM, aucuns frais supplémentaires ne sont facturés pour le provisionnement des certificats publics, et ACM gère le processus de renouvellement.

ACM est utilisé dans le compte réseau pour générer un certificat TLS public, qui, à son tour, est utilisé par les CloudFront distributions pour établir la connexion HTTPS entre les spectateurs et. CloudFront Pour plus d'informations, consultez la documentation CloudFront .

Considération relative à la conception

Pour les certificats externes, ACM doit résider dans le même compte que les ressources pour lesquelles il fournit des certificats. Les certificats ne peuvent pas être partagés entre plusieurs comptes.

Amazon Route 53

Amazon Route 53 est un service Web DNS hautement disponible et évolutif. Vous pouvez utiliser Route 53 pour effectuer trois fonctions importantes : l'enregistrement de domaine, le routage DNS et la surveillance de l'état.

Vous pouvez utiliser Route 53 en tant que service DNS pour mapper des noms de domaine à vos EC2 instances, compartiments S3, CloudFront distributions et autres AWS ressources. La nature distribuée des serveurs AWS DNS permet de garantir que vos utilisateurs finaux sont systématiquement routés vers votre application. Des fonctionnalités telles que le flux de trafic et le contrôle du routage de la Route 53 vous aident à améliorer la fiabilité. Si le point de terminaison principal de votre application devient indisponible, vous pouvez configurer votre basculement pour rediriger vos utilisateurs vers un autre emplacement. Route 53 Resolver fournit un DNS récursif pour votre VPC et vos réseaux locaux via un VPN géré ou géré. AWS Direct Connect AWS

En utilisant le service IAM avec Route 53, vous pouvez contrôler avec précision qui peut mettre à jour vos données DNS. Vous pouvez activer la signature DNSSEC (DNS Security Extensions) pour permettre aux résolveurs DNS de valider qu'une réponse DNS provient de Route 53 et qu'elle n'a pas été altérée.

Le pare-feu DNS Route 53 Resolver protège les requêtes DNS sortantes provenant de votre. VPCs Ces demandes passent par Route 53 Resolver pour la résolution du nom de domaine. Une utilisation principale des protections de pare-feu DNS consiste à empêcher l'exfiltration DNS de vos données. Avec le pare-feu DNS, vous pouvez surveiller et contrôler les domaines que vos applications peuvent interroger. Vous pouvez refuser l'accès aux domaines malveillants et autoriser le passage de toutes les autres requêtes. Vous pouvez également refuser l'accès à tous les domaines, sauf ceux que vous approuvez explicitement. Vous pouvez également utiliser le pare-feu DNS pour bloquer les demandes de résolution aux ressources dans des zones hébergées privées (partagées ou locales), y compris les noms de points de terminaison d'un VPC. Il peut également bloquer les demandes de noms d' EC2 instances publics ou privés.

Les résolveurs Route 53 sont créés par défaut dans le cadre de chaque VPC. Dans le AWS SRA, la Route 53 est utilisée dans le compte réseau principalement pour la fonctionnalité de pare-feu DNS.

> **Considération relative à la conception**
>
> Le pare-feu DNS et AWS Network Firewall les deux proposent un filtrage des noms de domaine, mais pour différents types de trafic. Vous pouvez utiliser DNS Firewall et Network Firewall ensemble pour configurer le filtrage basé sur le domaine pour le trafic de la couche application sur deux chemins réseau différents :
>
> - Le pare-feu DNS permet de filtrer les requêtes DNS sortantes qui transitent par le résolveur Route 53 à partir d'applications internes à votre compte. VPCs Vous pouvez également

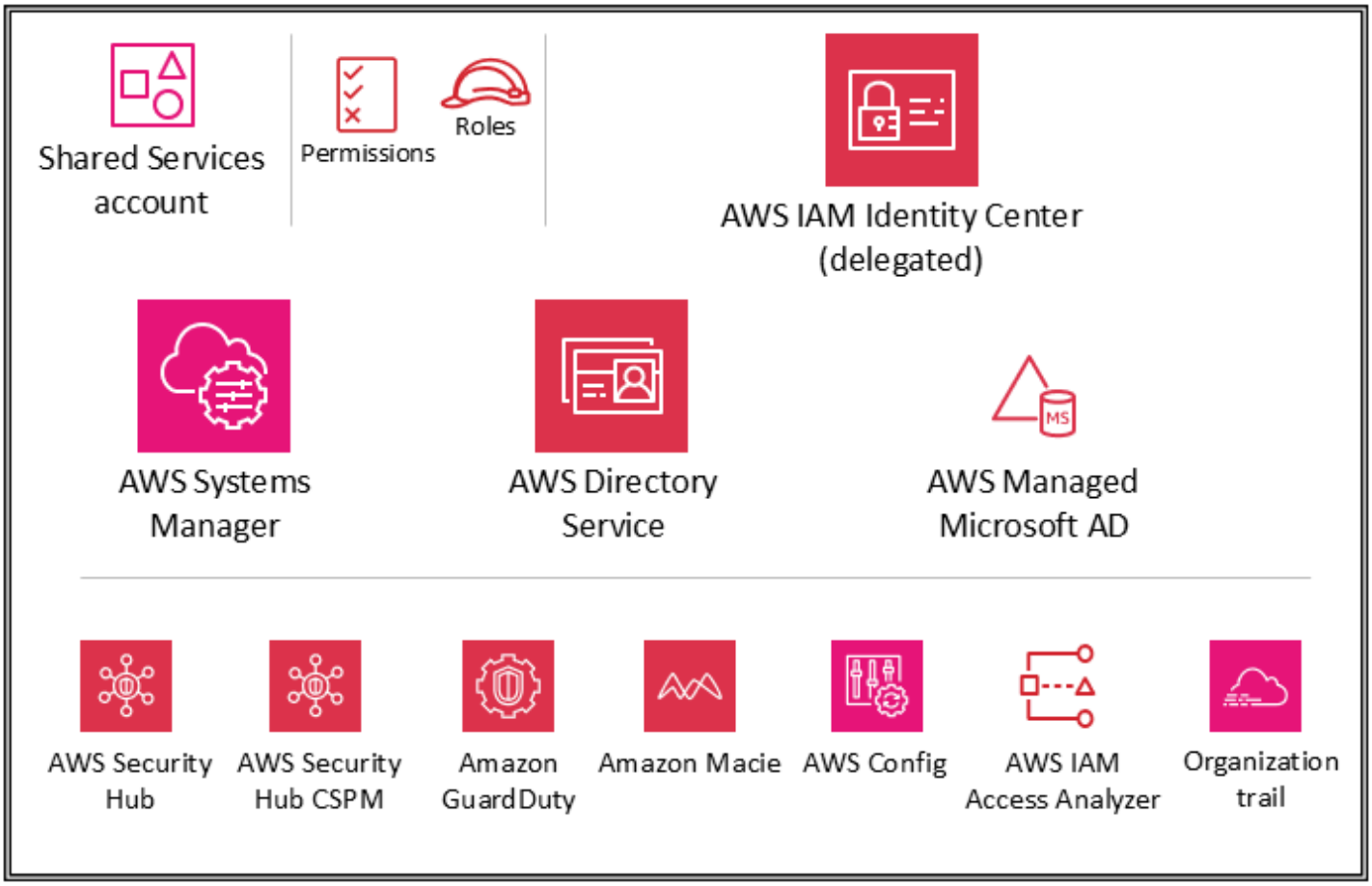
configurer le pare-feu DNS pour envoyer des réponses personnalisées pour les requêtes adressées à des noms de domaine bloqués.

- Network Firewall fournit un filtrage pour le trafic de la couche réseau et d'application, mais n'a pas de visibilité sur les requêtes effectuées par Route 53 Resolver.

Infrastructure OU — Compte Shared Services

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le schéma suivant illustre les services AWS de sécurité configurés dans le compte Shared Services.



Le compte Shared Services fait partie de l'unité d'organisation de l'infrastructure et son objectif est de prendre en charge les services utilisés par de nombreuses applications et équipes pour obtenir

leurs résultats. Par exemple, les services d'annuaire (Active Directory), les services de messagerie et les services de métadonnées entrent dans cette catégorie. La AWS SRA met en avant les services partagés qui prennent en charge les contrôles de sécurité. Bien que les comptes réseau fassent également partie de l'unité d'organisation d'infrastructure, ils sont supprimés du compte Shared Services pour faciliter la séparation des tâches. Les équipes chargées de gérer ces services n'ont pas besoin d'autorisations ni d'accès aux comptes du réseau.

AWS Systems Manager

AWS Systems Manager(qui est également inclus dans le compte de gestion de l'organisation et dans le compte de l'application) fournit un ensemble de fonctionnalités qui permettent la visibilité et le contrôle de vos AWS ressources. L'une de ces fonctionnalités, Systems Manager Explorer, est un tableau de bord des opérations personnalisable qui fournit des informations sur vos AWS ressources. Vous pouvez synchroniser les données d'exploitation de tous les comptes de votre AWS organisation à l'aide AWS Organizations de Systems Manager Explorer. Systems Manager est déployé dans le compte Shared Services via la fonctionnalité d'administrateur délégué dans AWS Organizations.

Systems Manager vous aide à maintenir la sécurité et la conformité en scannant vos instances gérées et en signalant (ou en prenant des mesures correctives) les violations des politiques détectées. En associant Systems Manager aux déploiements appropriés chez chaque membre Comptes AWS (par exemple, le compte d'application), vous pouvez coordonner la collecte des données d'inventaire des instances et centraliser les automatisations telles que l'application de correctifs et les mises à jour de sécurité.

AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, également connu sous le nom de AWS Managed Microsoft AD, permet à vos charges de travail et à vos AWS ressources sensibles aux annuaires d'utiliser Active Directory géré sur. AWS Vous pouvez associer des instances Amazon EC2 pour Windows Server, Amazon EC2 pour Linux et Amazon RDS for SQL Server à votre domaine, et AWS utiliser des services informatiques pour utilisateurs finaux (EUC), tels qu' WorkSpacesAmazon, avec des utilisateurs et des groupes Active Directory. AWS Managed Microsoft AD

AWS Managed Microsoft AD vous permet d'étendre votre Active Directory existant AWS et d'utiliser vos informations d'identification utilisateur locales existantes pour accéder aux ressources du cloud. Vous pouvez également administrer vos utilisateurs, groupes, applications et systèmes locaux sans la complexité liée à l'exécution et à la maintenance d'un Active Directory hautement disponible sur

site. Vous pouvez associer vos ordinateurs, ordinateurs portables et imprimantes existants à un AWS Managed Microsoft AD domaine.

AWS Managed Microsoft AD repose sur Microsoft Active Directory et ne vous oblige pas à synchroniser ou à répliquer les données de votre Active Directory existant vers le cloud. Vous pouvez utiliser les outils et fonctionnalités d'administration Active Directory habituels, tels que les objets de stratégie de groupe (GPOs), les approbations de domaine, les politiques de mot de passe détaillées, les comptes de services gérés de groupe (gMSAs), les extensions de schéma et l'authentification unique basée sur Kerberos. Vous pouvez également déléguer des tâches administratives et autoriser l'accès à l'aide des groupes de sécurité Active Directory.

La réplication multirégionale vous permet de déployer et d'utiliser un seul AWS Managed Microsoft AD répertoire sur plusieurs Régions AWS. Cela vous permet de déployer et de gérer plus facilement et à moindre coût vos charges de travail Microsoft Windows et Linux dans le monde entier. Lorsque vous utilisez la fonctionnalité de réplication multirégionale automatisée, vous bénéficiez d'une meilleure résilience tandis que vos applications utilisent un répertoire local pour des performances optimales.

AWS Managed Microsoft AD prend en charge le protocole LDAP (Lightweight Directory Access Protocol) sur SSL/TLS, également appelé LDAPS, dans les rôles client et serveur. Lorsqu'il agit en tant que serveur, AWS Managed Microsoft AD prend en charge le protocole LDAPS sur les ports 636 (SSL) et 389 (TLS). Vous activez les communications LDAPS côté serveur en installant un certificat sur vos contrôleurs de AWS Managed Microsoft AD domaine à partir d'une autorité AWS de certification (CA) Active Directory Certificate Services (AD CS). Lorsque vous agissez en tant que client, AWS Managed Microsoft AD prend en charge le protocole LDAPS sur les ports 636 (SSL). Vous pouvez activer les communications LDAPS côté client en enregistrant les certificats CA des émetteurs de certificats de votre serveur dans AWS, puis en activant LDAPS dans votre annuaire.

Dans le AWS SRA, Directory Service il est utilisé dans le compte Shared Services pour fournir des services de domaine pour les charges de travail compatibles avec Microsoft sur plusieurs comptes membres. AWS

> **Considération relative à la conception**
>
> Vous pouvez autoriser vos utilisateurs Active Directory locaux à se connecter à AWS Management Console et AWS Command Line Interface (AWS CLI) avec leurs informations d'identification Active Directory existantes en utilisant IAM Identity Center et en sélectionnant AWS Managed Microsoft AD comme source d'identité. Cela permet à vos utilisateurs

d'assumer l'un des rôles qui leur sont assignés lors de la connexion, d'accéder aux ressources et d'agir sur celles-ci conformément aux autorisations définies pour le rôle. Une autre option consiste à permettre AWS Managed Microsoft AD à vos utilisateurs d'assumer un rôle IAM.

IAM Identity Center

La AWS SRA utilise la fonctionnalité d'administrateur délégué prise en charge par AWS IAM Identity Center pour déléguer la majeure partie de l'administration d'IAM Identity Center au compte Shared Services. Cela permet de limiter le nombre d'utilisateurs qui ont besoin d'accéder au compte de gestion de l'organisation. IAM Identity Center doit toujours être activé dans le compte de gestion de l'organisation pour effectuer certaines tâches, notamment la gestion des ensembles d'autorisations fournis dans le compte de gestion de l'organisation.

La principale raison de l'utilisation du compte Shared Services en tant qu'administrateur délégué pour IAM Identity Center est l'emplacement Active Directory. Si vous envisagez d'utiliser Active Directory comme source d'identité IAM Identity Center, vous devez localiser le répertoire dans le compte membre que vous avez désigné comme compte d'administrateur délégué IAM Identity Center. Dans le AWS SRA, le compte Shared Services héberge AWS Managed Microsoft AD, de sorte que ce compte est désigné comme administrateur délégué d'IAM Identity Center.

IAM Identity Center prend en charge l'enregistrement d'un seul compte membre en tant qu'administrateur délégué à la fois. Vous ne pouvez créer un compte membre que lorsque vous vous connectez avec les informations d'identification du compte de gestion. Pour activer la délégation, vous devez prendre en compte les conditions requises répertoriées dans la documentation de l'IAM Identity Center. Le compte d'administrateur délégué peut effectuer la plupart des tâches de gestion d'IAM Identity Center, mais avec certaines restrictions, répertoriées dans la documentation d'IAM Identity Center. L'accès au compte d'administrateur délégué pour IAM Identity Center doit être étroitement contrôlé.

Considérations relatives à la conception

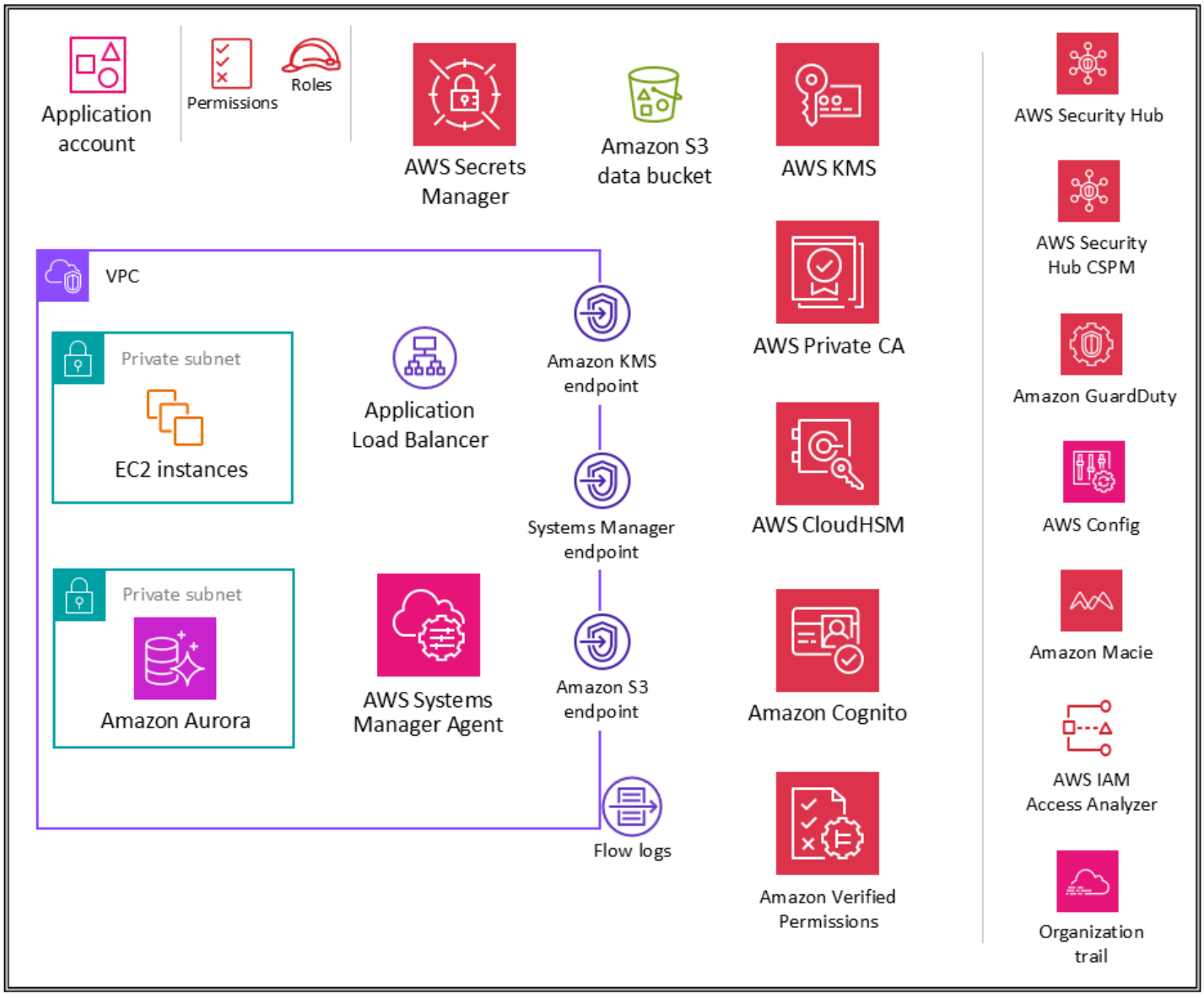
- Si vous décidez de remplacer la source d'identité IAM Identity Center d'une autre source par Active Directory, ou de la remplacer par une autre source, le répertoire doit résider (appartenir à) le compte membre administrateur délégué d'IAM Identity Center, s'il en existe un ; sinon, il doit se trouver dans le compte de gestion.

- Vous pouvez héberger AWS Managed Microsoft AD votre VPC dédié sur un autre compte, puis utiliser AWS Resource Access Manager (AWS RAM) pour partager des sous-réseaux de cet autre compte avec le compte administrateur délégué. Ainsi, l' AWS Managed Microsoft AD instance est contrôlée dans le compte administrateur délégué, mais du point de vue du réseau, elle agit comme si elle était déployée dans le VPC d'un autre compte. Cela est utile lorsque vous avez plusieurs AWS Managed Microsoft AD instances et que vous souhaitez les déployer localement là où votre charge de travail est exécutée, tout en les gérant de manière centralisée via un seul compte.
- Si vous disposez d'une équipe dédiée aux identités qui effectue des activités régulières de gestion des identités et des accès ou si vous avez des exigences de sécurité strictes pour séparer les fonctions de gestion des identités des autres fonctions de services partagés, vous pouvez héberger une équipe dédiée à la gestion Compte AWS des identités. Dans ce scénario, vous désignez ce compte comme administrateur délégué pour IAM Identity Center, et il héberge également votre AWS Managed Microsoft AD annuaire. Vous pouvez atteindre le même niveau d'isolation logique entre vos charges de travail de gestion des identités et les charges de travail des autres services partagés en utilisant des autorisations IAM précises au sein d'un seul compte de service partagé.
- IAM Identity Center ne fournit actuellement pas de support multirégional. (Pour activer IAM Identity Center dans une autre région, vous devez d'abord supprimer votre configuration IAM Identity Center actuelle.) En outre, il ne prend pas en charge l'utilisation de différentes sources d'identité pour différents ensembles de comptes et ne vous permet pas de déléguer la gestion des autorisations à différentes parties de votre organisation (c'est-à-dire plusieurs administrateurs délégués) ou à différents groupes d'administrateurs. Si vous avez besoin de l'une de ces fonctionnalités, vous pouvez utiliser la fédération IAM pour gérer vos identités d'utilisateur au sein d'un fournisseur d'identité (IdP) extérieur AWS et autoriser ces identités d'utilisateurs externes à AWS utiliser les ressources de votre compte. Les supports IAM sont IdPs compatibles avec OpenID Connect (OIDC) ou SAML 2.0. Il est recommandé d'utiliser la fédération SAML 2.0 avec des fournisseurs d'identité tiers tels qu'Active Directory Federation Service (AD FS), Okta, Azure Active Directory (Azure AD) ou Ping Identity pour fournir une fonctionnalité d'authentification unique permettant aux utilisateurs de se connecter AWS Management Console ou d'appeler AWS des opérations d'API. Pour plus d'informations sur la fédération IAM et les fournisseurs d'identité, consultez la section À propos de la fédération basée sur SAML 2.0 dans la documentation IAM.

Workloads OU — Compte d'application

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Le schéma suivant illustre les services AWS de sécurité configurés dans le compte d'application (ainsi que l'application elle-même).



Le compte Application héberge l'infrastructure et les services principaux permettant d'exécuter et de gérer une application d'entreprise. Le compte d'application et l'unité d'organisation Workloads

répondent à quelques objectifs de sécurité principaux. Tout d'abord, vous créez un compte distinct pour chaque application afin de définir des limites et des contrôles entre les charges de travail afin d'éviter les problèmes liés au mélange des rôles, des autorisations, des données et des clés de chiffrement. Vous souhaitez fournir un conteneur de comptes distinct dans lequel l'équipe chargée de l'application peut bénéficier de droits étendus pour gérer sa propre infrastructure sans affecter les autres. Ensuite, vous ajoutez une couche de protection en fournissant un mécanisme permettant à l'équipe des opérations de sécurité de surveiller et de collecter les données de sécurité. Utilisez un suivi organisationnel et des déploiements locaux de services de sécurité des comptes (Amazon GuardDuty, AWS Config, AWS Security Hub CSPM, Amazon EventBridge, IAM Access Analyzer), qui sont configurés et surveillés par l'équipe de sécurité. Enfin, vous permettez à votre entreprise de configurer les contrôles de manière centralisée. Vous alignez le compte d'application sur la structure de sécurité globale en le faisant membre de l'unité d'organisation Workloads, grâce à laquelle il hérite des autorisations de service, des contraintes et des garde-fous appropriés.

Considération relative à la conception

Dans votre organisation, il est probable que vous possédiez plusieurs applications métiers. L'UO Workloads est conçue pour héberger la plupart des charges de travail spécifiques à votre entreprise, y compris les environnements de production et de non-production. Ces charges de travail peuvent être une combinaison d'applications commerciales off-the-shelf (COTS) et d'applications personnalisées et de services de données développés en interne. Il existe peu de modèles d'organisation des différentes applications métiers ainsi que de leurs environnements de développement. L'un des modèles consiste à avoir plusieurs enfants en OUs fonction de votre environnement de développement, tel que la production, la mise en scène, les tests et le développement, et à utiliser des Comptes AWS enfants distincts pour ceux OUs qui concernent les différentes applications. Un autre schéma courant consiste à avoir un enfant distinct OUs par application, puis à utiliser un enfant distinct Comptes AWS pour chaque environnement de développement. La structure exacte de l'unité d'organisation et du compte dépend de la conception de votre application et des équipes qui gèrent ces applications. Réfléchissez aux contrôles de sécurité que vous souhaitez appliquer, qu'ils soient spécifiques à l'environnement ou à l'application, car il est plus facile de les mettre en œuvre dès que possible. SCPs OUs Pour plus d'informations sur l'organisation axée sur la charge de travail OUs, consultez la OUs section Applications du AWS livre blanc Organiser votre AWS environnement à l'aide de plusieurs comptes.

VPC d'application

Le cloud privé virtuel (VPC) du compte d'application nécessite à la fois un accès entrant (pour les services Web simples que vous modélisez) et un accès sortant (pour les besoins ou les besoins de l'application). Service AWS Par défaut, les ressources d'un VPC sont routables les unes vers les autres. Il existe deux sous-réseaux privés : l'un pour héberger les EC2 instances (couche application) et l'autre pour Amazon Aurora (couche base de données). La segmentation du réseau entre les différents niveaux, tels que le niveau application et le niveau base de données, est réalisée par le biais de groupes de sécurité VPC, qui limitent le trafic au niveau de l'instance. Pour des raisons de résilience, la charge de travail couvre au moins deux zones de disponibilité et utilise deux sous-réseaux par zone.

> Considération relative à la conception
>
> Vous pouvez utiliser Traffic Mirroring pour copier le trafic réseau à partir d'une interface réseau élastique d' EC2 instances. Vous pouvez ensuite envoyer le trafic vers des dispositifs de out-of-band sécurité et de surveillance à des fins d'inspection du contenu, de surveillance des menaces ou de résolution des problèmes. Par exemple, vous souhaiterez peut-être surveiller le trafic qui quitte votre VPC ou le trafic dont la source est extérieure à votre VPC. Dans ce cas, vous refléterez tout le trafic, à l'exception du trafic passant par votre VPC, et vous l'enverrez à une seule appliance de surveillance. Les journaux de flux Amazon VPC ne capturent pas le trafic en miroir ; ils capturent généralement les informations provenant uniquement des en-têtes de paquets. La mise en miroir du trafic fournit des informations plus approfondies sur le trafic réseau en vous permettant d'analyser le contenu réel du trafic, y compris la charge utile. Activez la mise en miroir du trafic uniquement pour l'interface elastic network des EC2 instances susceptibles de fonctionner dans le cadre de charges de travail sensibles ou pour lesquelles vous pensez avoir besoin de diagnostics détaillés en cas de problème.

Points de terminaison d’un VPC

Les points de terminaison VPC fournissent une couche supplémentaire de contrôle de sécurité, ainsi que d'évolutivité et de fiabilité. Utilisez-les pour connecter le VPC de votre application à un autre. Services AWS(Dans le compte d'application, le AWS SRA utilise des points de terminaison VPC AWS KMS pour AWS Systems Manager, et Amazon S3.) Les points de terminaison sont des périphériques virtuels. Il s'agit de composants VPC mis à l’à échelle horizontalement, redondants

et hautement disponibles. Ils permettent la communication entre des instances de votre VPC et de vos services sans imposer de risques de disponibilité ou de contraintes de bande passante sur votre trafic réseau. Vous pouvez utiliser un point de terminaison VPC pour connecter de manière privée votre VPC aux services de point de terminaison VPC pris en charge et Services AWS alimentés par celui-ci AWS PrivateLink sans avoir besoin d'une passerelle Internet, d'un périphérique NAT, d'une connexion VPN ou d'une connexion. AWS Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec d'autres instances. Services AWS Le trafic entre votre VPC et l'autre Service AWS ne quitte pas le réseau Amazon.

Un autre avantage de l'utilisation des points de terminaison VPC est de permettre la configuration des politiques des points de terminaison. Une stratégie de point de terminaison d'un VPC est une stratégie de ressource IAM que vous attachez à un point de terminaison lorsque vous le créez ou le modifiez. Si vous n'attachez pas de stratégie IAM lorsque vous créez un point de terminaison AWS , associez une stratégie IAM par défaut qui permet un accès complet au service. Une stratégie de point de terminaison n'annule pas et ne remplace pas les stratégies utilisateur IAM ou les stratégies propres à des services comme par exemple, les stratégies de compartiment S3. Il s'agit d'une politique IAM distincte pour contrôler l'accès du point de terminaison au service spécifié. De cette façon, il ajoute un niveau de contrôle supplémentaire sur les personnes AWS habilitées à communiquer avec les ressources ou les services.

Amazon EC2

Les EC2 instances Amazon qui composent notre application utilisent la version 2 du service de métadonnées d'instance (IMDSv2). IMDSv2 ajoute des protections contre quatre types de vulnérabilités qui pourraient être utilisées pour tenter d'accéder à l'IMDS : les pare-feux d'applications de sites Web, les proxys inverses ouverts, les vulnérabilités de falsification de requêtes côté serveur (SSRF), les pare-feux ouverts de couche 3 et. NATs Pour plus d'informations, consultez le billet de blog Ajoutez une défense approfondie contre les pare-feux ouverts, les proxys inverses et les vulnérabilités SSRF grâce aux améliorations apportées au service de métadonnées d' EC2 instance.

Utilisez des éléments séparés VPCs (en tant que sous-ensemble des limites de compte) pour isoler l'infrastructure par segments de charge de travail. Utilisez des sous-réseaux pour isoler les niveaux de votre application (par exemple, web, application et base de données) dans un VPC unique. Utilisez des sous-réseaux privés pour vos instances si elles ne doivent pas être accessibles directement à partir d'Internet. Pour appeler l' EC2API Amazon depuis votre sous-réseau privé sans passer par une passerelle Internet, utilisez AWS PrivateLink. Limitez l'accès à vos instances en utilisant des groupes de sécurité. Utilisez les journaux de flux VPC pour surveiller le trafic qui atteint vos instances. Utilisez le gestionnaire de session, une fonctionnalité de AWS Systems Manager,

pour accéder à vos instances à distance au lieu d'ouvrir les ports SSH entrants et de gérer les clés SSH. Utilisez des volumes Amazon Elastic Block Store (Amazon EBS) distincts pour le système d'exploitation et vos données. Vous pouvez configurer votre Compte AWS pour appliquer le chiffrement des nouveaux volumes EBS et des copies instantanées que vous créez.

> **Exemple de mise en œuvre**
>
> La bibliothèque de code AWS SRA fournit un exemple d'implémentation du chiffrement Amazon EBS par défaut dans Amazon. EC2 Il montre comment activer le chiffrement Amazon EBS par défaut au niveau du compte au sein de chaque compte Compte AWS et Région AWS au sein de l'organisation. AWS

AWS Enclaves Nitro

AWS Nitro Enclaves est EC2 une fonctionnalité d'Amazon qui vous permet de créer des environnements d'exécution isolés, appelés enclaves, à partir d'instances. EC2 Les enclaves sont des machines virtuelles distinctes, renforcées et soumises à de fortes contraintes. Le processeur et la mémoire d'une EC2 instance parent unique sont partitionnés en enclaves isolées. Chaque enclave exécute un noyau indépendant. Les enclaves fournissent uniquement une connectivité de socket locale sécurisée avec leur instance parent. Elles ne disposent pas de stockage persistant, d'accès interactif ou de réseau externe. Les utilisateurs ne peuvent pas accéder à une enclave par SSH, et les processus, les applications ou les utilisateurs (root ou administrateur) de l'instance parent ne peuvent pas accéder aux données et aux applications qu'elle contient. Vous pouvez sécuriser vos données les plus sensibles, telles que les informations personnelles identifiables (PII), les données médicales, financières et de propriété intellectuelle, en quelques EC2 instances. Nitro Enclaves vous permet de vous concentrer sur votre application au lieu de vous soucier de l'intégration avec des services externes. Nitro Enclaves inclut une attestation cryptographique pour votre logiciel afin que vous puissiez être sûr que seul le code autorisé est exécuté, et une intégration avec celle-ci AWS KMS afin que seules vos enclaves puissent accéder au matériel sensible. Cela permet de réduire la surface d'attaque de vos applications de traitement de données les plus sensibles. L'utilisation de Nitro Enclaves est gratuite.

L'attestation cryptographique est un processus utilisé pour prouver l'identité d'une enclave. Le processus d'attestation est effectué par l'intermédiaire de l'Hyperviseur Nitro, qui produit un document d'attestation signé pour que l'enclave prouve son identité à un autre tiers ou à un autre service. Les

documents d'attestation contiennent des informations clés sur l'enclave, telles que la clé publique de l'enclave, les hachages de l'image et des applications de l'enclave, etc.

Avec AWS Certificate Manager (ACM) pour Nitro Enclaves, vous pouvez utiliser des certificats publics et privés. SSL/TLS certificates with your web applications and web servers running on EC2 instances with Nitro Enclaves. SSL/TLS certificates are used to secure network communications and to establish the identity of websites over the internet and resources on private networks. ACM for Nitro Enclaves removes the time-consuming and error-prone manual process of purchasing, uploading, and renewing SSL/TLS ACM for Nitro Enclaves crée des clés privées sécurisées, distribue le certificat et sa clé privée à votre enclave et gère les renouvellements de certificats. Avec ACM pour Nitro Enclaves, la clé privée du certificat reste isolée dans l'enclave, ce qui empêche l'instance et ses utilisateurs d'y accéder. Pour plus d'informations, consultez la section consacrée AWS Certificate Manager aux enclaves Nitro dans la documentation relative aux enclaves Nitro.

Application Load Balancers

Les équilibreurs de charge des applications distribuent le trafic applicatif entrant sur plusieurs cibles, telles que EC2 les instances, dans plusieurs zones de disponibilité. Dans le AWS SRA, le groupe cible de l'équilibreur de charge est constitué des instances d'application EC2 . La AWS SRA utilise des écouteurs HTTPS pour s'assurer que le canal de communication est crypté. L'Application Load Balancer utilise un certificat de serveur pour mettre fin à la connexion frontale, puis pour déchiffrer les demandes des clients avant de les envoyer aux cibles.

AWS Certificate Manager (ACM) s'intègre nativement aux équilibreurs de charge d'application, et le AWS SRA utilise ACM pour générer et gérer les certificats publics X.509 (serveur TLS) nécessaires. Vous pouvez appliquer le protocole TLS 1.2 et des chiffrements forts pour les connexions frontales grâce à la politique de sécurité Application Load Balancer. Pour plus d’informations, consultez la documentation relative à Elastic Load Balancing.

Considérations relatives à la conception

- Pour les scénarios courants tels que les applications strictement internes qui nécessitent un certificat TLS privé sur l'Application Load Balancer, vous pouvez utiliser ACM dans ce compte pour générer un certificat privé à partir de. AWS CA privée Dans la AWS SRA, l'autorité de certification privée racine ACM est hébergée dans le compte Security Tooling et peut être partagée avec l'ensemble de l' AWS organisation ou avec des personnes spécifiques Comptes AWS pour émettre des certificats d'entité finale, comme décrit précédemment dans la section sur le compte Security Tooling.

- Pour les certificats publics, vous pouvez utiliser ACM pour générer ces certificats et les gérer, y compris la rotation automatique. Vous pouvez également générer vos propres certificats en utilisant des SSL/TLS outils pour créer une demande de signature de certificat (CSR), faire signer la CSR par une autorité de certification (CA) pour produire un certificat, puis importer le certificat dans ACM ou le télécharger sur IAM pour l'utiliser avec l'Application Load Balancer. Si vous importez un certificat dans ACM, vous devez surveiller sa date d'expiration et le renouveler avant son expiration.
- Pour des niveaux de défense supplémentaires, vous pouvez déployer des AWS WAF politiques pour protéger l'Application Load Balancer. Le fait de disposer de politiques périphériques, de politiques d'application et même de couches d'application des politiques privées ou internes améliore la visibilité des demandes de communication et permet une application unifiée des politiques. Pour plus d'informations, consultez le billet de blog Deploying defense in depth using AWS Managed Rules for AWS WAF.

AWS CA privée

AWS Autorité de certification privée(AWS CA privée) est utilisé dans le compte Application pour générer des certificats privés à utiliser avec un Application Load Balancer. Il est courant que les équilibreurs de charge d'application diffusent du contenu sécurisé via le protocole TLS. Cela nécessite l'installation de certificats TLS sur l'Application Load Balancer. Pour les applications strictement internes, les certificats TLS privés peuvent fournir le canal sécurisé.

Dans le AWS SRA, AWS CA privée est hébergé dans le compte Security Tooling et partagé avec le compte de l'application à l'aide de. AWS RAM Cela permet aux développeurs d'un compte d'application de demander un certificat à une autorité de certification privée partagée. Le partage CAs au sein de votre organisation ou entre plusieurs Comptes AWS entreprises permet de réduire les coûts et la complexité liés à la création et à la gestion des doublons CAs dans tous vos domaines Comptes AWS. Lorsque vous utilisez ACM pour émettre des certificats privés à partir d'une autorité de certification partagée, le certificat est généré localement dans le compte demandeur, et ACM assure la gestion complète du cycle de vie et le renouvellement.

Amazon Inspector

La AWS SRA utilise Amazon Inspector pour détecter et scanner automatiquement les EC2 instances et les images de conteneurs qui se trouvent dans l'Amazon Elastic Container Registry (Amazon ECR) afin de détecter des vulnérabilités logicielles et une exposition involontaire au réseau.

Amazon Inspector est placé dans le compte d'application, car il fournit des services de gestion des vulnérabilités aux EC2 instances de ce compte. En outre, Amazon Inspector signale les chemins réseau indésirables vers et depuis EC2 les instances.

Amazon Inspector dans les comptes membres est géré de manière centralisée par le compte d'administrateur délégué. Dans le AWS SRA, le compte Security Tooling est le compte d'administrateur délégué. Le compte d'administrateur délégué peut gérer les données des résultats et certains paramètres pour les membres de l'organisation. Cela inclut l'affichage des détails des résultats agrégés pour tous les comptes membres, l'activation ou la désactivation des scans des comptes membres et l'examen des ressources numérisées au sein de l' AWS organisation.

> Considération relative à la conception
>
> Vous pouvez utiliser Patch Manager, une fonctionnalité de AWS Systems Manager, pour déclencher l'application de correctifs à la demande afin de corriger les failles de sécurité « jour zéro » ou autres failles de sécurité critiques d'Amazon Inspector. Le gestionnaire de correctifs vous permet de corriger ces vulnérabilités sans avoir à attendre le calendrier normal d'application des correctifs. La correction est effectuée à l'aide du runbook Systems Manager Automation. Pour plus d'informations, consultez la série de blogs en deux parties Automatisez la gestion et la correction des vulnérabilités à l' AWS aide d'Amazon Inspector et. AWS Systems Manager

AWS Systems Manager

AWS Systems Managerest un outil Service AWS que vous pouvez utiliser pour visualiser les données opérationnelles de plusieurs sources Services AWS et automatiser les tâches opérationnelles sur l'ensemble de vos AWS ressources. Grâce aux flux de travail et aux runbooks d'approbation automatisés, vous pouvez travailler à réduire les erreurs humaines et à simplifier les tâches de maintenance et de déploiement sur les AWS ressources.

Outre ces fonctionnalités d'automatisation générales, Systems Manager prend en charge un certain nombre de fonctionnalités de sécurité préventives, détectives et réactives. AWS Systems Manager L'agent (agent SSM) est un logiciel Amazon qui peut être installé et configuré sur une EC2 instance, un serveur sur site ou une machine virtuelle (VM). SSM Agent permet à Systems Manager de mettre à jour, gérer et configurer ces ressources. Systems Manager vous aide à maintenir la sécurité et la conformité en scannant ces instances gérées et en signalant (ou en prenant des mesures correctives) les violations détectées dans vos correctifs, configurations et politiques personnalisées.

Le AWS SRA utilise le gestionnaire de session, une fonctionnalité de Systems Manager, pour fournir une expérience de shell et de CLI interactive basée sur un navigateur. Cela permet une gestion d'instance sécurisée et vérifiable sans qu'il soit nécessaire d'ouvrir les ports entrants, de gérer les hôtes Bastion ou de gérer les clés SSH. La AWS SRA utilise le Patch Manager, une fonctionnalité de Systems Manager, pour appliquer des correctifs aux EC2 instances des systèmes d'exploitation et des applications.

La AWS SRA utilise également l'automatisation, une fonctionnalité de Systems Manager, pour simplifier les tâches courantes de maintenance et de déploiement des EC2 instances Amazon et d'autres AWS ressources. L'automatisation peut simplifier les tâches informatiques courantes, telles que la modification de l'état d'un ou plusieurs nœuds (à l'aide d'une automatisation de l'approbation) et la gestion des états des nœuds en fonction d'un calendrier. Systems Manager inclut des fonctions qui vous permettent de cibler de grands groupes d'instances à l'aide de balises, et des contrôles de rapidité qui vous aident à déployer les modifications selon les limites que vous définissez. L'automatisation propose des automatisations en un clic pour simplifier des tâches complexes telles que la création d'Amazon Machine Images (AMIs) dorées et la restauration d'instances inaccessibles. EC2 En outre, vous pouvez améliorer la sécurité opérationnelle en donnant aux rôles IAM l'accès à des runbooks spécifiques pour exécuter certaines fonctions, sans accorder directement d'autorisations à ces rôles. Par exemple, si vous souhaitez qu'un rôle IAM soit autorisé à redémarrer des EC2 instances spécifiques après des mises à jour de correctifs, mais que vous ne souhaitez pas accorder l'autorisation directement à ce rôle, vous pouvez créer un runbook d'automatisation et autoriser le rôle à exécuter uniquement le runbook.

Considérations relatives à la conception

- Systems Manager s'appuie sur les métadonnées de l' EC2 instance pour fonctionner correctement. Systems Manager peut accéder aux métadonnées des instances en utilisant la version 1 ou la version 2 du service de métadonnées d'instance (IMDSv1 et IMDSv2).
- L'agent SSM doit communiquer avec différentes Services AWS ressources telles que les EC2 messages Amazon, Systems Manager et Amazon S3. Pour que cette communication ait lieu, le sous-réseau nécessite soit une connectivité Internet sortante, soit le provisionnement de points de terminaison VPC appropriés. Le AWS SRA utilise des points de terminaison VPC pour que l'agent SSM établisse des chemins réseau privés vers différents. Services AWS
- Automation vous permet de partager les bonnes pratiques avec le reste de votre organisation. Vous pouvez créer les meilleures pratiques pour la gestion des ressources

dans les runbooks et partager les runbooks entre Régions AWS et groupes. Vous pouvez également restreindre les valeurs autorisées pour les paramètres du runbook. Dans ces cas d'utilisation, vous devrez peut-être créer des runbooks d'automatisation dans un compte central tel que Security Tooling ou Shared Services et les partager avec le reste de l' AWS organisation. Les cas d'utilisation courants incluent la capacité de mettre en œuvre de manière centralisée les correctifs et les mises à jour de sécurité, de remédier aux dérives liées aux configurations VPC ou aux politiques relatives aux compartiments S3, et de gérer EC2 les instances à grande échelle. Pour plus de détails sur l'implémentation, consultez la documentation de Systems Manager.

Amazon Aurora

Dans le AWS SRA, Amazon Aurora et Amazon S3 constituent le niveau de données logique. Aurora est un moteur de base de données relationnelle entièrement géré compatible avec MySQL et PostgreSQL. Une application exécutée sur les EC2 instances communique avec Aurora et Amazon S3 selon les besoins. Aurora est configuré avec un cluster de base de données au sein d'un groupe de sous-réseaux de base de données.

Considération relative à la conception

Comme dans de nombreux services de base de données, la sécurité d'Aurora est gérée à trois niveaux. Pour contrôler qui peut effectuer des actions de gestion Amazon Relational Database Service (Amazon RDS) sur les clusters de bases de données et les instances de base de données Aurora, vous utilisez IAM. Pour contrôler quels appareils et EC2 instances peuvent ouvrir des connexions au point de terminaison du cluster et au port de l'instance de base de données pour les clusters de base de données Aurora dans un VPC, vous utilisez un groupe de sécurité VPC. Pour authentifier les connexions et les autorisations pour un cluster de base de données Aurora, vous pouvez adopter la même approche qu'avec une instance de base de données autonome de MySQL ou PostgreSQL, ou vous pouvez utiliser l'authentification de base de données IAM pour Aurora MySQL Compatible Edition. Avec cette dernière approche, vous vous authentifiez auprès de votre cluster de base de données compatible Aurora MySQL à l'aide d'un rôle IAM et d'un jeton d'authentification.

Amazon S3

Amazon S3 est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Il constitue l'épine dorsale de nombreuses applications AWS, et les autorisations et contrôles de sécurité appropriés sont essentiels pour protéger les données sensibles. Pour connaître les meilleures pratiques de sécurité recommandées pour Amazon S3, consultez la documentation, les conférences techniques en ligne et des informations plus détaillées dans les articles de blog. La meilleure pratique la plus importante consiste à bloquer l'accès trop permissif (en particulier l'accès public) aux compartiments S3.

AWS KMS

Le AWS SRA illustre le modèle de distribution recommandé pour la gestion des clés, dans lequel la ressource AWS KMS key réside dans la même ressource Compte AWS que la ressource à chiffrer. Pour cette raison, AWS KMS il est utilisé dans le compte Application en plus d'être inclus dans le compte Security Tooling. Dans le compte d'application, AWS KMS est utilisé pour gérer les clés spécifiques aux ressources de l'application. Vous pouvez mettre en œuvre une séparation des tâches en utilisant des politiques clés pour accorder des autorisations d'utilisation clés aux rôles d'application locaux et pour restreindre les autorisations de gestion et de surveillance à vos principaux dépositaires.

> **Considération relative à la conception**
>
> Dans un modèle distribué, la AWS KMS principale responsabilité de gestion incombe à l'équipe chargée de l'application. Toutefois, votre équipe de sécurité centrale peut être chargée de la gouvernance et de la surveillance d'événements cryptographiques importants tels que les suivants :
>
> - Les éléments de clé importés dans une clé KMS approchent de leur date d'expiration.
> - Les éléments de clé dans une clé KMS ont effectué automatiquement une rotation.
> - La clé AKMS a été supprimée.
> - Le taux d'échec du déchiffrement est élevé.

AWS CloudHSM

AWS CloudHSMfournit des modules de sécurité matérielle gérés (HSMs) dans le AWS Cloud. Il vous permet de générer et d'utiliser vos propres clés de chiffrement à l'aide de la AWS norme FIPS 140-2 validée de niveau 3 à HSMs laquelle vous contrôlez l'accès. Vous pouvez l'utiliser AWS CloudHSM pour décharger SSL/TLS le traitement de vos serveurs Web. Cela réduit la charge du serveur Web et fournit une sécurité supplémentaire en stockant la clé privée du serveur Web AWS CloudHSM. Vous pouvez également déployer un HSM depuis le VPC entrant AWS CloudHSM dans le compte réseau pour stocker vos clés privées et signer les demandes de certificat si vous devez agir en tant qu'autorité de certification émettrice.

> Considération relative à la conception
>
> Si vous avez une exigence stricte pour la norme FIPS 140-2 niveau 3, vous pouvez également choisir de configurer AWS KMS le AWS CloudHSM cluster comme magasin de clés personnalisé plutôt que d'utiliser le magasin de clés KMS natif. Ce faisant, vous bénéficiez de l'intégration entre AWS KMS et Services AWS qui cryptent vos données, tout en étant responsable de la HSMs protection de vos clés KMS. Cela combine un locataire unique HSMs sous votre contrôle à la facilité d'utilisation et d'intégration de AWS KMS. Pour gérer votre AWS CloudHSM infrastructure, vous devez utiliser une infrastructure à clé publique (PKI) et disposer d'une équipe expérimentée en gestion HSMs.

AWS Secrets Manager

AWS Secrets Managervous aide à protéger les informations d'identification (secrets) dont vous avez besoin pour accéder à vos applications, services et ressources informatiques. Le service vous permet de faire pivoter, de gérer et de récupérer efficacement les informations d'identification de base de données, les clés d'API et autres secrets tout au long de leur cycle de vie. Vous pouvez remplacer les informations d'identification codées en dur dans votre code par un appel d'API à Secrets Manager pour récupérer le secret par programmation. Cela permet de garantir que le secret ne peut pas être compromis par quelqu'un qui examine votre code, car le secret n'existe plus dans le code. Secrets Manager vous aide également à déplacer vos applications entre les environnements (développement, pré-production, production). Au lieu de modifier le code, vous pouvez vous assurer qu'un secret correctement nommé et référencé est disponible dans l'environnement. Cela favorise la cohérence et la réutilisabilité du code d'application dans différents environnements, tout en nécessitant moins de modifications et d'interactions humaines une fois le code testé.

Avec Secrets Manager, vous pouvez gérer l'accès aux secrets en utilisant des politiques IAM précises et des politiques basées sur les ressources. Vous pouvez contribuer à sécuriser les secrets en les chiffrant à l'aide de clés de chiffrement que vous gérez à l'aide AWS KMS de ces clés. Secrets Manager s'intègre également aux services de AWS journalisation et de surveillance pour un audit centralisé.

Secrets Manager utilise le chiffrement des enveloppes AWS KMS keys et des clés de données pour protéger chaque valeur secrète. Lorsque vous créez un secret, vous pouvez choisir n'importe quelle clé symétrique gérée par le client dans la région Compte AWS et, ou vous pouvez utiliser la clé AWS gérée pour Secrets Manager.

La meilleure pratique consiste à surveiller vos secrets pour enregistrer toute modification apportée à ceux-ci. Cela vous permet de vous assurer que toute utilisation ou modification imprévue peut être étudiée. Les modifications indésirables peuvent être annulées. Secrets Manager en propose actuellement deux Services AWS qui vous permettent de surveiller votre organisation et votre activité : AWS CloudTrail et AWS Config. CloudTrail capture tous les appels d'API pour Secrets Manager sous forme d'événements, y compris les appels provenant de la console Secrets Manager et les appels de code adressés au Secrets Manager APIs. En outre, CloudTrail capture d'autres événements connexes (non liés à l'API) susceptibles d'avoir un impact sur votre sécurité ou votre conformité Compte AWS ou de vous aider à résoudre des problèmes opérationnels. Il s'agit notamment de certains événements de rotation de secrets et de suppression de versions secrètes. AWS Config peut fournir des contrôles de détection en suivant et en surveillant les modifications apportées aux secrets dans Secrets Manager. Ces modifications incluent la description d'un secret, la configuration de rotation, les balises et la relation avec d'autres AWS sources telles que la clé de chiffrement KMS ou les AWS Lambda fonctions utilisées pour la rotation du secret. Vous pouvez également configurer Amazon EventBridge, qui reçoit des notifications de modification de configuration et de conformité AWS Config, pour acheminer des événements secrets particuliers à des fins de notification ou de mesures correctives.

Dans le AWS SRA, Secrets Manager est situé dans le compte de l'application pour prendre en charge les cas d'utilisation des applications locales et pour gérer les secrets proches de leur utilisation. Ici, un profil d'instance est attaché aux EC2 instances du compte d'application. Des secrets distincts peuvent ensuite être configurés dans Secrets Manager pour permettre à ce profil d'instance de récupérer des secrets, par exemple pour rejoindre le domaine Active Directory ou LDAP approprié et pour accéder à la base de données Aurora. Secrets Manager s'intègre à Amazon RDS pour gérer les informations d'identification des utilisateurs lorsque vous créez, modifiez ou restaurez une instance de base de données Amazon RDS ou un cluster de base de données multi-AZ. Cela vous

permet de gérer la création et la rotation des clés et de remplacer les informations d'identification codées en dur dans votre code par des appels d'API programmatiques à Secrets Manager.

> Considération relative à la conception
>
> En général, configurez et gérez Secrets Manager dans le compte le plus proche de l'endroit où les secrets seront utilisés. Cette approche tire parti de la connaissance locale du cas d'utilisation et apporte rapidité et flexibilité aux équipes de développement d'applications. Pour les informations étroitement contrôlées nécessitant un niveau de contrôle supplémentaire, les secrets peuvent être gérés de manière centralisée par Secrets Manager dans le compte Security Tooling.

Amazon Cognito

Amazon Cognito vous permet d'ajouter l'inscription, la connexion et le contrôle d'accès des utilisateurs à vos applications Web et mobiles rapidement et efficacement. Amazon Cognito s'adapte à des millions d'utilisateurs et prend en charge la connexion auprès de fournisseurs d'identité sociale, tels qu'Apple, Facebook, Google et Amazon, ainsi que de fournisseurs d'identité d'entreprise via SAML 2.0 et OpenID Connect. Les deux principaux composants d'Amazon Cognito sont les groupes d'utilisateurs et les groupes d'identités. Les groupes d'utilisateurs sont des annuaires d'utilisateurs qui fournissent des options d'inscription et de connexion aux utilisateurs de votre application. Les pools d'identités vous permettent d'accorder à vos utilisateurs l'accès à d'autres Services AWS. Vous pouvez utiliser des groupes d'identités et des groupes d'utilisateurs séparément ou conjointement. Pour les scénarios d'utilisation courants, consultez la documentation Amazon Cognito.

Amazon Cognito fournit une interface utilisateur intégrée et personnalisable pour l'inscription et la connexion des utilisateurs. Vous pouvez utiliser Android, iOS et Amazon Cognito JavaScript SDKs pour ajouter des pages d'inscription et de connexion utilisateur à vos applications. Amazon Cognito Sync est une Service AWS bibliothèque cliente qui permet la synchronisation entre appareils des données utilisateur relatives aux applications.

Amazon Cognito prend en charge l'authentification multifactorielle et le chiffrement des données au repos et des données en transit. Les groupes d'utilisateurs Amazon Cognito fournissent des fonctionnalités de sécurité avancées pour protéger l'accès aux comptes utilisateurs dans votre application. Ces fonctionnalités de sécurité avancées fournissent une authentification adaptative basée sur le risque et une protection contre l'utilisation d'informations d'identification compromises.

Considérations relatives à la conception

- Vous pouvez créer une AWS Lambda fonction, puis la déclencher lors d'opérations de groupe d'utilisateurs telles que l'inscription, la confirmation et la connexion (authentification) des utilisateurs à l'aide d'un déclencheur Lambda. Vous pouvez ajouter des stimulations d'authentification, migrer des utilisateurs et personnaliser les messages de vérification. Pour les opérations courantes et le flux d'utilisateurs, consultez la documentation Amazon Cognito. Amazon Cognito appelle les fonctions Lambda de manière synchrone.
- Vous pouvez utiliser les groupes d'utilisateurs Amazon Cognito pour sécuriser les petites applications multi-locataires. Un cas d'utilisation courant de la conception à locataires multiples consiste à exécuter des charges de travail pour prendre en charge le test de plusieurs versions d'une application. Une conception multilocataire est également utile pour tester une application unique avec différents jeux de données, ce qui vous permet d'utiliser pleinement vos ressources de cluster. Assurez-vous toutefois que le nombre de locataires et le volume attendu correspondent aux quotas de service Amazon Cognito correspondants. Ces quotas sont partagés entre tous les locataires au sein de votre application.

Amazon Verified Permissions

Amazon Verified Permissions est un service de gestion des autorisations évolutif et précis pour les applications que vous créez. Les développeurs et les administrateurs peuvent utiliser Cedar, un langage de politique open source spécialement conçu et axé sur la sécurité, avec des rôles et des attributs pour définir des contrôles d'accès plus granulaires, sensibles au contexte et basés sur des politiques. Les développeurs peuvent créer des applications plus sécurisées plus rapidement en externalisant les autorisations et en centralisant la gestion et l'administration des politiques. Les autorisations vérifiées incluent des définitions de schéma, la grammaire des déclarations de politique et un raisonnement automatique qui s'étend à des millions d'autorisations, afin que vous puissiez appliquer les principes du refus par défaut et du moindre privilège. Le service inclut également un outil de simulation d'évaluation pour vous aider à tester vos décisions d'autorisation et vos politiques d'auteur. Ces fonctionnalités facilitent le déploiement d'un modèle d'autorisation détaillé et précis pour soutenir vos objectifs de confiance zéro. Verified Permissions centralise les autorisations dans un magasin de politiques et aide les développeurs à utiliser ces autorisations pour autoriser les actions des utilisateurs dans leurs applications.

Vous pouvez connecter votre application au service via l'API pour autoriser les demandes d'accès des utilisateurs. Pour chaque demande d'autorisation, le service récupère les politiques pertinentes et évalue ces politiques afin de déterminer si un utilisateur est autorisé à effectuer une action sur une ressource, en fonction des entrées contextuelles telles que les utilisateurs, les rôles, l'appartenance à un groupe et les attributs. Vous pouvez configurer et connecter les autorisations vérifiées pour envoyer vos journaux de gestion des politiques et d'autorisation à AWS CloudTrail. Si vous utilisez Amazon Cognito comme banque d'identités, vous pouvez l'intégrer à Verified Permissions et utiliser l'identifiant et les jetons d'accès renvoyés par Amazon Cognito dans les décisions d'autorisation de vos applications. Vous fournissez des jetons Amazon Cognito à Verified Permissions, qui utilise les attributs qu'ils contiennent pour représenter le principal et identifier les droits du principal. Pour plus d'informations sur cette intégration, consultez le billet de AWS blog Simplifying fined authorization with Amazon Verified Permissions and Amazon Cognito.

Les autorisations vérifiées vous aident à définir le contrôle d'accès basé sur des politiques (PBAC). Le PBAC est un modèle de contrôle d'accès qui utilise des autorisations exprimées sous forme de politiques pour déterminer qui peut accéder à quelles ressources d'une application. Le PBAC réunit le contrôle d'accès basé sur les rôles (RBAC) et le contrôle d'accès basé sur les attributs (ABAC), ce qui donne un modèle de contrôle d'accès plus puissant et plus flexible. Pour en savoir plus sur le PBAC et sur la façon de concevoir un modèle d'autorisation à l'aide des autorisations vérifiées, consultez le billet de AWS blog Le contrôle d'accès basé sur des politiques dans le développement d'applications avec Amazon Verified Permissions.

Dans la AWS SRA, les autorisations vérifiées sont situées dans le compte de l'application pour prendre en charge la gestion des autorisations pour les applications grâce à son intégration à Amazon Cognito.

Défense en couches

Le compte d'application permet d'illustrer les principes de défense à plusieurs niveaux qui AWS permettent. Prenez en compte la sécurité des EC2 instances qui constituent le cœur d'un exemple d'application simple représenté dans le AWS SRA et vous pourrez voir comment Services AWS travailler ensemble dans le cadre d'une défense à plusieurs niveaux. Cette approche s'aligne sur la vision structurelle des services de AWS sécurité, telle que décrite dans la section Appliquer les services de sécurité dans l'ensemble de votre AWS organisation plus haut dans ce guide.

- La couche la plus interne est constituée des EC2 instances. Comme indiqué précédemment, EC2 les instances incluent de nombreuses fonctionnalités de sécurité natives, soit par défaut, soit sous

forme d'options. Les exemples incluent IMDSv2le système Nitro et le chiffrement du stockage Amazon EBS.

- La deuxième couche de protection se concentre sur le système d'exploitation et les logiciels exécutés sur les EC2 instances. Des services tels qu'Amazon Inspector vous AWS Systems Managerpermettent de surveiller, de signaler et de prendre des mesures correctives sur ces configurations. Amazon Inspector surveille les vulnérabilités de votre logiciel et Systems Manager vous aide à garantir la sécurité et la conformité en analysant l'état des correctifs et de la configuration des instances gérées, puis en signalant et en prenant les mesures correctives que vous spécifiez.
- Les instances et les logiciels exécutés sur ces instances sont intégrés à votre infrastructure AWS réseau. Outre les fonctionnalités de sécurité d'Amazon VPC, la AWS SRA utilise également des points de terminaison VPC pour fournir une connectivité privée entre le VPC et ceux pris en charge Services AWS, et pour fournir un mécanisme permettant de placer des politiques d'accès aux limites du réseau.
- L'activité et la configuration des EC2 instances, du logiciel, du réseau et des rôles et ressources IAM sont également Compte AWS surveillées par des services spécialisés tels que AWS Security Hub CSPM, AWS Security Hub Amazon,, GuardDuty AWS CloudTrail AWS Config, IAM Access Analyzer et Amazon Macie.
- Enfin, au-delà du compte d'application, il AWS RAM permet de contrôler les ressources partagées avec d'autres comptes, et les politiques de contrôle des services IAM vous aident à appliquer des autorisations cohérentes au sein de l' AWS organisation.

AI/ML pour la sécurité

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

L'intelligence artificielle et l'apprentissage automatique (au centre des préoccupations d'Amazon AI/ML) is transforming businesses. AI/ML depuis plus de 20 ans), et de nombreuses fonctionnalités utilisées par les clients AWS, y compris les services de sécurité, reposent sur l'intelligence artificielle et le machine learning. Cela crée une valeur intrinsèque différenciée, car vous pouvez vous y appuyer en toute sécurité AWS sans que vos équipes de sécurité ou de développement d'applications aient besoin d'une expertise en intelligence artificielle et en machine learning.

L'IA est une technologie avancée qui permet aux machines et aux systèmes de gagner en intelligence et en capacité de prédiction. Les systèmes d'IA tirent les leçons de l'expérience passée grâce aux données qu'ils consomment ou sur lesquelles ils sont entraînés. Le ML est l'un des aspects les plus importants de l'IA. Le machine learning est la capacité des ordinateurs à apprendre à partir de données sans être explicitement programmés. Dans la programmation traditionnelle, le programmeur écrit des règles qui définissent le fonctionnement du programme sur un ordinateur ou une machine. Dans le ML, le modèle apprend les règles à partir des données. Les modèles ML peuvent découvrir des modèles cachés dans les données ou établir des prédictions précises sur de nouvelles données qui n'ont pas été utilisées pendant l'entraînement. Services AWS Utilisation multiple AI/ML pour tirer des leçons d'énormes ensembles de données et tirer des conclusions de sécurité.

- Amazon Macie est un service de sécurité des données qui utilise le machine learning et la correspondance de modèles pour découvrir et protéger vos données sensibles. Macie détecte automatiquement une liste longue et croissante de types de données sensibles, y compris les informations personnelles identifiables (PII) telles que les noms, les adresses et les informations financières telles que les numéros de carte de crédit. Cela vous donne également une visibilité constante sur vos données stockées dans Amazon Simple Storage Service (Amazon S3). Macie utilise le traitement du langage naturel (NLP) et des modèles de machine learning formés sur différents types d'ensembles de données afin de comprendre vos données existantes et d'attribuer des valeurs commerciales afin de prioriser les données critiques. Macie génère ensuite des résultats de données sensibles.

- Amazon GuardDuty est un service de détection des menaces qui utilise le machine learning, la détection des anomalies et des informations intégrées sur les menaces pour surveiller en permanence les activités malveillantes et les comportements non autorisés afin de protéger vos instances Comptes AWS, vos charges de travail sans serveur et en conteneur, vos utilisateurs, vos bases de données et votre stockage. GuardDuty intègre des techniques de machine learning très efficaces pour distinguer les activités potentiellement malveillantes des utilisateurs d'un comportement opérationnel anormal mais bénin au sein de l'entreprise. Comptes AWS Cette fonctionnalité modélise en permanence les invocations d'API au sein d'un compte et intègre des prédictions probabilistes pour isoler et alerter plus précisément en cas de comportement hautement suspect des utilisateurs. Cette approche permet d'identifier les activités malveillantes associées à des tactiques de menace connues, notamment la découverte, l'accès initial, la persistance, l'augmentation des privilèges, le contournement de la défense, l'accès aux informations d'identification, l'impact et l'exfiltration de données. Pour en savoir plus sur l' GuardDuty utilisation de l'apprentissage automatique, consultez la session en petits groupes organisée par AWS Re:inForce 2023 sur le développement de nouvelles découvertes grâce à l'apprentissage automatique sur Amazon GuardDuty (0). TDR31

Une sécurité prouvable

AWS développe des outils de raisonnement automatisés qui utilisent la logique mathématique pour répondre aux questions critiques concernant votre infrastructure et pour détecter les erreurs de configuration susceptibles d'exposer vos données. Cette fonctionnalité est appelée sécurité prouvable car elle fournit une meilleure assurance en matière de sécurité dans le cloud et dans le cloud. La sécurité prouvable utilise le raisonnement automatique, une discipline spécifique de l'IA qui applique la déduction logique aux systèmes informatiques. Par exemple, les outils de raisonnement automatisés peuvent analyser les politiques et les configurations d'architecture réseau, et prouver l'absence de configurations involontaires susceptibles d'exposer des données vulnérables. Cette approche fournit le plus haut niveau d'assurance possible pour les caractéristiques de sécurité critiques du cloud. Pour plus d'informations, consultez la section Ressources de sécurité prouvables sur le AWS site Web. Les fonctionnalités Services AWS et fonctionnalités suivantes utilisent actuellement un raisonnement automatique pour vous aider à garantir une sécurité prouvable pour vos applications :

- Amazon Verified Permissions est un service de gestion des autorisations évolutif et précis pour les applications que vous créez. Verified Permissions utilise Cedar, un langage open source pour le contrôle d'accès créé à l'aide d'un raisonnement automatisé et de tests différentiels. Cedar

est un langage permettant de définir les autorisations sous forme de politiques qui décrivent qui doit avoir accès à quelles ressources. Il s'agit également d'une spécification pour évaluer ces politiques. Utilisez les politiques de Cedar pour contrôler ce que chaque utilisateur de votre application est autorisé à faire et à quelles ressources il peut accéder. Les politiques de Cedar sont des déclarations d'autorisation ou d'interdiction qui déterminent si un utilisateur peut agir sur une ressource. Les politiques sont associées aux ressources, et vous pouvez associer plusieurs politiques à une ressource. Les politiques d'interdiction l'emportent sur les politiques d'autorisation. Lorsqu'un utilisateur de votre application tente d'effectuer une action sur une ressource, votre application envoie une demande d'autorisation au moteur de politiques Cedar. Cedar évalue les politiques applicables et renvoie une `ALLOW` `DENY` décision. Cedar prend en charge les règles d'autorisation pour tout type de principal et de ressource, permet un contrôle d'accès basé sur les rôles et les attributs, et soutient l'analyse par le biais d'outils de raisonnement automatisés qui peuvent vous aider à optimiser vos politiques et à valider votre modèle de sécurité.

- AWS Identity and Access Management Access Analyzervous aide à rationaliser la gestion des autorisations. Vous pouvez utiliser cette fonctionnalité pour définir des autorisations détaillées, vérifier les autorisations prévues et affiner les autorisations en supprimant les accès non utilisés. IAM Access Analyzer génère une politique précise basée sur l'activité d'accès enregistrée dans vos journaux. Il fournit également plus de 100 vérifications de politiques pour vous aider à créer et à valider vos politiques. IAM Access Analyzer utilise une sécurité prouvable pour analyser les chemins d'accès et fournir des résultats complets concernant l'accès public et multicompte à vos ressources. Cet outil est basé sur Zelkova, qui traduit les politiques IAM en instructions logiques équivalentes et exécute une suite de résolveurs logiques spécialisés et à usage général (théories du modulo de satisfaisabilité) pour résoudre le problème. l'IAM Access Analyzer applique Zelkova de manière répétitive à une politique avec des requêtes de plus en plus spécifiques pour caractériser les classes de comportements autorisées par la politique, en fonction du contenu de celle-ci L'analyseur n'examine pas les journaux d'accès pour déterminer si une entité externe a accédé à une ressource située dans votre zone de confiance. Il génère une constatation lorsqu'une politique basée sur les ressources autorise l'accès à une ressource, même si l'entité externe n'y a pas accédé. Pour en savoir plus sur les théories modulo de la satisfaisabilité, voir Théories du modulo de la satisfaisabilité dans le manuel de la satisfaisabilité. *
- Amazon S3 Block Public Access est une fonctionnalité d'Amazon S3 qui vous permet de bloquer d'éventuelles erreurs de configuration susceptibles d'entraîner un accès public à vos compartiments et à vos objets. Vous pouvez activer Amazon S3 Block Public Access pour les points d'accès, les compartiments, les comptes et l' AWS organisation (ce qui affecte à la fois les compartiments existants et nouveaux du compte). L'accès public est accordé aux compartiments et aux objets par le biais de listes de contrôle d'accès (ACLs), de politiques de compartiments, ou

des deux. Le système de raisonnement automatisé Zelkova permet de déterminer si une politique ou une ACL donnée est considérée comme publique. Amazon S3 utilise Zelkova pour vérifier la politique de chaque compartiment et vous avertit si un utilisateur non autorisé est en mesure de lire ou d'écrire dans votre compartiment. Si un compartiment est marqué comme public, certaines demandes publiques sont autorisées à y accéder. Si un bucket est marqué comme non public, toutes les demandes publiques sont refusées. Zelkova est capable de prendre de telles décisions car elle dispose d'une représentation mathématique précise des politiques IAM. Il crée une formule pour chaque politique et prouve un théorème à propos de cette formule.

- Amazon VPC Network Access Analyzer est une fonctionnalité d'Amazon VPC qui vous aide à comprendre les chemins réseau potentiels vers vos ressources et à identifier les accès réseau non intentionnels potentiels. Network Access Analyzer vous aide à vérifier la segmentation du réseau, à identifier l'accessibilité à Internet et à vérifier les chemins réseau et les accès réseau fiables. Cette fonctionnalité utilise des algorithmes de raisonnement automatisés pour analyser les chemins réseau qu'un paquet peut emprunter entre les ressources d'un AWS réseau. Il produit ensuite des résultats pour les chemins correspondant à vos étendues d'accès réseau, qui définissent les modèles de trafic sortant et entrant. L’analyseur d’accès réseau effectue une analyse statique de la configuration d’un réseau, ce qui signifie qu’aucun paquet n’est transmis sur le réseau dans le cadre de cette analyse.
- Amazon VPC Reachability Analyzer est une fonctionnalité d'Amazon VPC qui vous permet de déboguer, de comprendre et de visualiser la connectivité de votre réseau. AWS Reachability Analyzer est un outil d'analyse de configuration qui vous permet d'effectuer des tests de connectivité entre une ressource source et une ressource de destination dans vos clouds privés virtuels (). VPCs Lorsque la destination est accessible, Reachability Analyzer hop-by-hop fournit des informations détaillées sur le chemin réseau virtuel entre la source et la destination. Lorsque la destination n'est pas accessible, Reachability Analyzer identifie le composant bloquant. Reachability Analyzer utilise un raisonnement automatique pour identifier les chemins réalisables en élaborant un modèle de configuration réseau entre une source et une destination. Il vérifie ensuite l'accessibilité en fonction de la configuration. Il n'envoie pas de paquets et n'analyse pas le plan de données.

[*] Biere, A. M. Heule, H. van Maaren et T. Walsh. 2009. Manuel de satisfaisabilité. Presse IOS, NLD.

Création de votre architecture de sécurité : une approche progressive

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

L'architecture de sécurité multi-comptes recommandée par la AWS SRA est une architecture de base qui vous aide à intégrer la sécurité dès le début de votre processus de conception. La transition vers le cloud de chaque entreprise est unique. Pour réussir à faire évoluer votre architecture de sécurité cloud, vous devez définir l'état cible que vous souhaitez atteindre, comprendre votre niveau actuel de préparation au cloud et adopter une approche agile pour combler les lacunes. Le AWS SRA fournit un état cible de référence pour votre architecture de sécurité. La transformation progressive vous permet de démontrer rapidement la valeur ajoutée tout en minimisant le besoin de faire des prévisions ambitieuses.

Le cadre d'adoption du AWS cloud (AWS CAF) recommande quatre phases itératives et incrémentielles de transformation du cloud : conception, alignement, lancement et mise à l'échelle. Lorsque vous entamez la phase de lancement et que vous vous concentrez sur la mise en œuvre d'initiatives pilotes en production, vous devez vous concentrer sur la création d'une architecture de sécurité solide comme base pour la phase de mise à l'échelle afin de disposer de la capacité technique nécessaire pour migrer et exploiter vos charges de travail les plus critiques en toute confiance. Cette approche progressive est applicable si vous êtes une start-up, une petite ou moyenne entreprise qui souhaite développer ses activités, ou une entreprise qui acquiert de nouvelles unités commerciales ou procède à des fusions et acquisitions. Le AWS SRA vous aide à mettre en place cette architecture de base de sécurité afin que vous puissiez appliquer les contrôles de sécurité de manière uniforme au sein de votre entreprise en pleine expansion. AWS Organizations L'architecture de base comprend plusieurs Comptes AWS services. La planification et la mise en œuvre doivent être un processus en plusieurs phases afin que vous puissiez passer à des étapes plus petites pour atteindre l'objectif global de configuration de votre architecture de sécurité de base. Cette section décrit les phases typiques de votre transition vers le cloud selon une approche structurée. Ces phases sont conformes aux principes de conception de AWS sécurité du Well-Architected Framework.

Phase 1 : Construisez votre unité d'organisation et votre structure de compte

Une AWS organisation et une structure de comptes bien conçues constituent une condition préalable à une base de sécurité solide. Comme expliqué précédemment dans la section relative aux éléments constitutifs de la SRA de ce guide, le fait d'en avoir plusieurs vous Comptes AWS permet d'isoler les différentes fonctions commerciales et de sécurité dès la conception. Cela peut sembler inutile au début, mais il s'agit d'un investissement pour vous aider à évoluer rapidement et en toute sécurité. Cette section explique également comment gérer plusieurs comptes et AWS Organizations comment utiliser Comptes AWS les fonctionnalités d'accès sécurisé et d'administrateur délégué pour gérer de manière Services AWS centralisée ces multiples comptes.

Vous pouvez l'utiliser AWS Control Towercomme indiqué précédemment dans ce guide pour orchestrer votre zone d'atterrissage. Si vous utilisez actuellement un compte unique Compte AWS, consultez le Comptes AWS guide Transitioning to multiple pour migrer vers plusieurs comptes dès que possible. Par exemple, si votre start-up conçoit et prototype actuellement votre produit en un seul produit Compte AWS, vous devriez envisager d'adopter une stratégie multi-comptes avant de lancer votre produit sur le marché. De même, les petites, moyennes et grandes entreprises devraient commencer à élaborer leur stratégie multi-comptes dès qu'elles planifient leurs charges de travail de production initiales. Commencez par votre fondation Comptes AWS, OUs puis ajoutez vos comptes et comptes liés à la charge de travail OUs .

Pour Compte AWS des recommandations sur la structure de l'UO allant au-delà de ce qui est prévu dans la AWS SRA, consultez le billet de blog sur la stratégie multi-comptes pour les petites et moyennes entreprises. Lorsque vous finalisez votre unité d'organisation et votre structure de compte, réfléchissez aux contrôles de sécurité de haut niveau à l'échelle de l'organisation que vous souhaiteriez appliquer en utilisant des politiques de contrôle des services (SCPs), des politiques de contrôle des ressources (RCPs) et des politiques déclaratives.

> **Considération relative à la conception**
>
> Ne reproduisez pas la structure hiérarchique de votre entreprise lorsque vous concevez votre unité d'organisation et votre structure de compte. Vous OUs devez vous baser sur les fonctions de charge de travail et sur un ensemble commun de contrôles de sécurité applicables aux charges de travail. N'essayez pas de concevoir la structure complète de votre compte dès le début. Concentrez-vous sur les éléments fondamentaux OUs, puis ajoutez de la charge de travail OUs selon vos besoins. Vous pouvez déplacer des comptes entre OUs

eux pour expérimenter d'autres approches dès les premières étapes de votre conception. Cependant, cela peut entraîner une certaine surcharge liée à la gestion des autorisations logiques, en fonction SCPs des politiques déclaratives et des conditions IAM basées sur les chemins d'unité d'organisation et de compte. RCPs

Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation de Account Alternate Contacts. Cette solution définit les contacts alternatifs de facturation, d'exploitation et de sécurité pour tous les comptes d'une organisation.

Phase 2 : Mettre en place une base d'identité solide

Dès que vous en avez créé plusieurs Comptes AWS, vous devez donner à vos équipes l'accès aux AWS ressources de ces comptes. Il existe deux catégories générales de gestion des identités : la gestion des identités et des accès du personnel et la gestion des identités et des accès des clients (CIAM). Workforce IAM est destiné aux organisations où les employés et les charges de travail automatisées doivent se connecter AWS pour faire leur travail. Le CIAM est utilisé lorsqu'une organisation a besoin d'un moyen d'authentifier les utilisateurs afin de fournir un accès aux applications de l'organisation. Vous avez d'abord besoin d'une stratégie IAM pour le personnel, afin que vos équipes puissent créer et migrer des applications. Vous devez toujours utiliser des rôles IAM plutôt que des utilisateurs IAM pour donner accès à des utilisateurs humains ou à des machines. Suivez les directives de la AWS SRA sur la façon de les utiliser AWS IAM Identity Center dans les comptes Org Management et Shared Services pour gérer de manière centralisée l'accès à votre compte avec authentification unique (SSO). Comptes AWS Le guide fournit également des considérations de conception relatives à l'utilisation de la fédération IAM lorsque vous ne pouvez pas utiliser IAM Identity Center.

Lorsque vous utilisez des rôles IAM pour fournir aux utilisateurs un accès aux AWS ressources, vous devez utiliser IAM Access Analyzer et le conseiller d'accès IAM, comme indiqué dans les sections Outils de sécurité et Gestion des organisations de ce guide. Ces services vous aident à obtenir le moindre privilège, ce qui constitue un contrôle préventif important qui vous aide à adopter une bonne posture de sécurité.

Considération relative à la conception

Pour obtenir le moindre privilège, concevez des processus permettant d'examiner et de comprendre régulièrement les relations entre vos identités et les autorisations dont elles ont besoin pour fonctionner correctement. Au fur et à mesure que vous apprenez, affinez ces autorisations et réduisez-les progressivement au minimum d'autorisations possible. Pour ce qui est de l'évolutivité, cette responsabilité doit être partagée entre vos équipes centrales chargées de la sécurité et des applications. Utilisez des fonctionnalités telles que les politiques basées sur les ressources, les limites d'autorisation, les contrôles d'accès basés sur les attributs et les politiques de session pour aider les propriétaires d'applications à définir un contrôle d'accès précis.

Exemples d’implémentation

La bibliothèque de code AWS SRA fournit deux exemples d'implémentations qui s'appliquent à cette phase :

- La politique de mot de passe IAM définit la politique de mot de passe du compte pour les utilisateurs afin de l'aligner sur les normes de conformité communes.
- Access Analyzer configure un analyseur au niveau de l'organisation dans un compte d'administrateur délégué et un analyseur au niveau du compte dans chaque compte.

Phase 3 : Maintien de la traçabilité

Lorsque vos utilisateurs auront accès à AWS et commenceront à créer, vous voudrez savoir qui fait quoi, quand et d'où. Vous aurez également besoin de visibilité sur les erreurs de configuration, les menaces ou les comportements inattendus potentiels en matière de sécurité. Une meilleure compréhension des menaces de sécurité vous permet de hiérarchiser les contrôles de sécurité appropriés. Pour surveiller AWS l'activité, suivez les recommandations de la AWS SRA concernant la mise en place d'un suivi organisationnel en utilisant AWS CloudTrailet en centralisant vos journaux dans le compte Log Archive. Pour la surveillance des événements de sécurité AWS Security Hub CSPM, utilisez Amazon GuardDuty et Amazon Security Lake AWS Config, comme indiqué dans la section relative au compte Security Tooling.

Considération relative à la conception

Lorsque vous commencez à utiliser new Services AWS, assurez-vous d'activer les journaux spécifiques au service pour le service et de les stocker dans votre référentiel de journaux central.

Exemples d'implémentation

La bibliothèque de code AWS SRA fournit les exemples d'implémentations suivants qui s'appliquent à cette phase :

- L'organisation CloudTrail crée un journal organisationnel et définit des valeurs par défaut pour configurer les événements de données (par exemple, dans Amazon S3 et AWS Lambda) afin de réduire la CloudTrail duplication de ceux configurés par. AWS Control Tower Cette solution fournit des options pour configurer les événements de gestion.
- AWS Config Le compte de gestion Control Tower permet AWS Config au compte de gestion de surveiller la conformité des ressources.
- Les règles d'organisation du pack de conformité déploient un pack de conformité sur les comptes et les régions spécifiées au sein d'une organisation.
- AWS Config Aggregator déploie un agrégateur en déléguant l'administration à un compte membre autre que le compte d'audit.
- Security Hub CSPM Organization configure Security Hub CSPM au sein d'un compte d'administrateur délégué pour les comptes et les régions gouvernées au sein de l'organisation.
- GuardDuty L'organisation effectue les GuardDuty configurations au sein d'un compte d'administrateur délégué pour les comptes d'une organisation.

Phase 4 : appliquer la sécurité à tous les niveaux

À ce stade, vous devriez avoir :

- Les contrôles de sécurité appropriés pour votre Comptes AWS.

- Une structure de compte et d'unité d'organisation bien définie avec des contrôles préventifs définis par le biais SCPs de politiques déclaratives et de rôles et de politiques IAM avec le moindre privilège. RCPs
- Possibilité de consigner AWS les activités en utilisant AWS CloudTrail ; de détecter les événements de sécurité en utilisant AWS Security Hub CSPM Amazon GuardDuty AWS Config ; et d'effectuer des analyses avancées sur un lac de données spécialement conçu pour des raisons de sécurité en utilisant Amazon Security Lake.

Au cours de cette phase, prévoyez d'appliquer la sécurité à d'autres niveaux de votre AWS organisation, comme décrit dans la section Appliquer les services de sécurité dans l'ensemble de votre AWS organisation. Vous pouvez créer des contrôles de sécurité pour votre couche réseau en utilisant des services tels que AWS WAF AWS Shield, AWS Firewall Manager, AWS Network Firewall,, AWS Certificate Manager (ACM), Amazon CloudFront, Amazon Route 53 et Amazon VPC, comme indiqué dans la section Compte réseau. Au fur et à mesure que vous avancez dans votre pile technologique, appliquez des contrôles de sécurité spécifiques à votre charge de travail ou à votre pile d'applications. Utilisez les points de terminaison VPC, Amazon Inspector et Amazon Cognito AWS Systems ManagerAWS Secrets Manager, comme indiqué dans la section Compte de l'application.

Considération relative à la conception

Lorsque vous concevez vos contrôles de sécurité « Defense in Depth » (DiD), tenez compte des facteurs d'échelle. Votre équipe de sécurité centrale n'aura pas la bande passante ou ne comprendra pas parfaitement le comportement de chaque application dans votre environnement. Donnez à vos équipes d'application les moyens d'être responsables et responsables de l'identification et de la conception des contrôles de sécurité appropriés pour leurs applications. L'équipe de sécurité centrale doit se concentrer sur la fourniture des outils et des conseils appropriés pour aider les équipes chargées des applications. Pour comprendre les mécanismes de mise à l'échelle AWS utilisés pour adopter une approche de sécurité davantage axée sur la gauche, consultez le billet de blog How AWS built the Security Guardians program, a mechanism to distribute security ownership.

Exemples d'implémentation

La bibliothèque de code AWS SRA fournit les exemples d'implémentations suivants qui s'appliquent à cette phase :

- Le chiffrement EBS par défaut EC2 configure le chiffrement Amazon EBS par défaut dans Amazon EC2 afin d'utiliser le chiffrement par défaut dans les limites fournies. AWS KMS key Régions AWS
- S3 Block Account Public Access configure les paramètres BPA (Block Public Access) au niveau du compte dans Amazon S3 pour les comptes au sein de l'organisation.
- Firewall Manager explique comment configurer une stratégie de groupe de sécurité et des AWS WAF politiques pour les comptes au sein d'une organisation.
- Inspector Organization configure Amazon Inspector au sein d'un compte d'administrateur délégué pour les comptes et les régions gouvernées au sein de l'organisation.

Phase 5 : protéger les données en transit et au repos

Les données de votre entreprise et de vos clients sont des actifs précieux que vous devez protéger. AWS fournit divers services et fonctionnalités de sécurité pour protéger les données en mouvement et au repos. Utilisez Amazon CloudFront avec AWS Certificate Manager, comme indiqué dans la section Compte réseau, pour protéger les données en mouvement collectées sur Internet. Pour les données en mouvement au sein des réseaux internes, utilisez un Application Load Balancer avec AWS Autorité de certification privée, comme expliqué dans la section Compte de l'application. AWS KMS et vous AWS CloudHSM aident à gérer les clés cryptographiques afin de protéger les données au repos.

Phase 6 : Préparation aux événements de sécurité

Lorsque vous exploitez votre environnement informatique, vous serez confronté à des événements de sécurité, c'est-à-dire des changements dans le fonctionnement quotidien de votre environnement informatique qui indiquent une violation possible des politiques de sécurité ou une défaillance du contrôle de sécurité. Une traçabilité adéquate est essentielle pour que vous soyez au courant d'un événement de sécurité le plus rapidement possible. Il est également important d'être prêt à trier et à répondre à de tels événements de sécurité afin de pouvoir prendre les mesures appropriées avant

que l'événement ne dégénère. La préparation vous aide à trier rapidement un événement de sécurité afin de comprendre son impact potentiel.

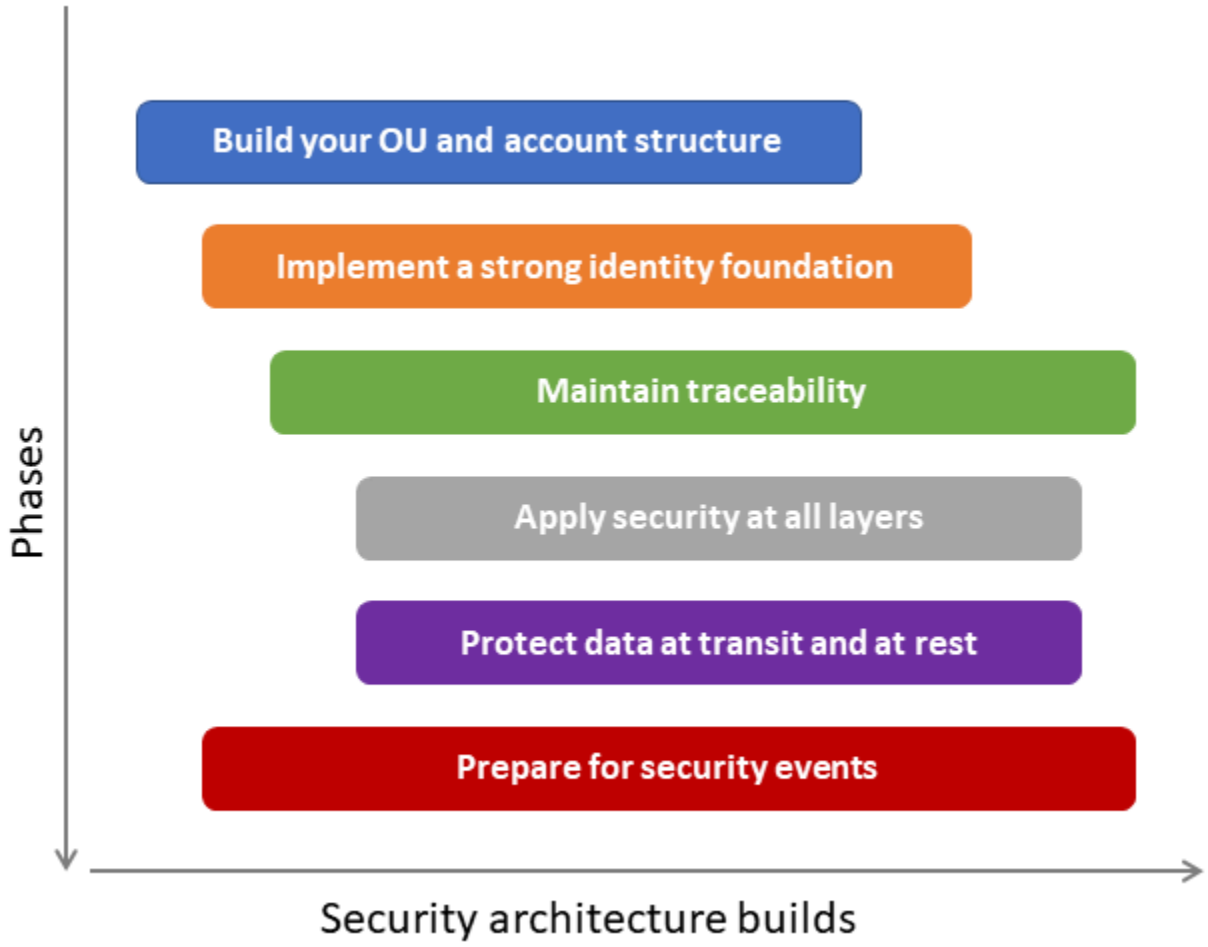
Le AWS SRA, grâce à la conception du compte Security Tooling et au déploiement de services de sécurité communs au sein de tous Comptes AWS, vous permet de détecter les événements de sécurité au sein de votre AWS organisation. Amazon Detective, intégré au compte Security Tooling, vous aide à trier un événement de sécurité et à en identifier la cause première. Au cours d'une enquête de sécurité, vous devez être en mesure de consulter les journaux pertinents pour enregistrer et comprendre l'ampleur et la chronologie de l'incident. Les journaux sont également nécessaires pour générer des alertes lorsque des actions spécifiques présentant un intérêt se produisent. La AWS SRA recommande un compte central d'archivage des journaux pour le stockage immuable de tous les journaux opérationnels et de sécurité. Vous pouvez interroger les CloudWatch journaux en utilisant Logs Insights pour les données stockées dans des groupes de CloudWatch journaux, et Amazon Athena et Amazon OpenSearch Service pour les données stockées dans Amazon S3. Utilisez Amazon Security Lake pour centraliser automatiquement les données de sécurité provenant de l' AWS environnement, des fournisseurs de logiciels en tant que service (SaaS), des sites locaux et d'autres fournisseurs de cloud. Configurez les abonnés du compte Security Tooling ou de tout autre compte dédié, comme indiqué par la AWS SRA, pour interroger ces journaux à des fins d'investigation.

AWS Security Incident Responsevous aide à automatiser la réponse, l'investigation et la correction des incidents de sécurité. Il fournit des playbooks et des flux de travail prédéfinis pour vous aider à répondre aux événements de sécurité rapidement et de manière cohérente. Lorsque la fonctionnalité de réponse proactive est activée, Security Incident Response s'intègre à Security Hub CSPM et déclenche automatiquement des flux GuardDuty de travail de réponse lorsque des résultats de sécurité sont détectés. Le service vous aide à normaliser et à automatiser vos processus de réponse aux incidents au sein de votre AWS organisation. Si vous avez besoin d'une assistance supplémentaire, vous pouvez ouvrir un dossier pris en charge par le service pour contacter l'équipe de réponse aux incidents AWS clients (CIRT).

Considérations relatives à la conception

- Vous devez commencer à vous préparer à détecter les événements de sécurité et à y répondre dès le début de votre transition vers le cloud. Pour mieux utiliser les ressources limitées, assignez les données et l'importance commerciale à vos AWS ressources afin que, lorsque vous détectez un événement de sécurité, vous puissiez hiérarchiser le triage et la réponse en fonction de l'importance des ressources impliquées.

- Les phases de création de votre architecture de sécurité cloud, décrites dans cette section, sont de nature séquentielle. Cependant, il n'est pas nécessaire d'attendre la fin complète d'une phase avant de passer à la phase suivante. Nous vous recommandons d'adopter une approche itérative, dans le cadre de laquelle vous commencez à travailler sur plusieurs phases en parallèle et faites évoluer chaque phase au fur et à mesure de l'évolution de votre posture de sécurité dans le cloud. Au fil des différentes phases, votre design évoluera. Pensez à adapter la séquence suggérée dans le schéma suivant à vos besoins particuliers.



Exemple de mise en œuvre

La bibliothèque de code AWS SRA fournit un exemple d'implémentation d'une Detective Organization, qui active automatiquement Amazon Detective en déléguant l'administration à un compte (par exemple, Audit ou Security Tooling) et configure Detective pour les comptes existants et futurs. AWS Organizations

AWS Liste de contrôle des meilleures pratiques de la SRA

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Cette section résume les meilleures pratiques AWS SRA détaillées dans ce guide dans une liste de contrôle que vous pouvez suivre lors de la création de votre version de l'architecture de sécurité. AWS Utilisez cette liste comme point de référence et non pour remplacer la révision du guide. La liste de contrôle est groupée par Service AWS. Si vous souhaitez valider par programmation votre AWS environnement existant par rapport à la liste de contrôle des meilleures pratiques AWS SRA, vous pouvez utiliser SRA Verify.

SRA Verify est un outil d'évaluation de la sécurité qui vous aide à évaluer l'alignement de votre organisation sur le AWS SRA dans plusieurs Comptes AWS régions. Il correspond directement aux recommandations de la AWS SRA en fournissant des contrôles automatisés qui valident votre mise en œuvre par rapport aux directives de la AWS SRA. L'outil vous aide à vérifier que vos services de sécurité sont correctement configurés conformément à l'architecture de référence. Il fournit des résultats détaillés et des mesures correctives réalisables pour garantir que votre AWS environnement respecte les meilleures pratiques en matière de sécurité. SRA Verify est conçu pour être exécuté AWS CodeBuild dans le compte d'audit de l'organisation (Security Tooling). Vous pouvez également l'exécuter localement ou l'étendre à l'aide de la bibliothèque SRA Verify.

> **Note**
>
> SRA Verify contient des contrôles pour plusieurs services, mais il se peut qu'il n'en contienne pas un pour toutes les considérations relatives au AWS SRA. Pour plus d'informations, consultez les guides de la bibliothèque AWS SRA.

AWS Organizations

- AWS Organizations est activé avec toutes les fonctionnalités.
- Les politiques de contrôle des services (SCPs) sont utilisées pour définir des directives de contrôle d'accès pour les responsables IAM.

- Les politiques de contrôle des ressources (RCPs) sont utilisées pour définir des directives de contrôle d'accès pour les AWS ressources.
- Les politiques déclaratives sont utilisées pour déclarer et appliquer de manière centralisée la configuration souhaitée pour une donnée Service AWS à grande échelle au sein de votre organisation.
- Trois comptes de base OUs sont créés (sécurité, infrastructure et charge de travail) pour regrouper les comptes des membres fournissant des services de base.
- Le compte Security Tooling est créé sous l'unité d'organisation de sécurité. Ce compte fournit une gestion centralisée des services de AWS sécurité et d'autres outils de sécurité tiers.
- Le compte Log Archive est créé sous l'unité d'organisation de sécurité. Ce compte fournit un référentiel central de journaux Services AWS et de journaux d'applications étroitement contrôlé.
- Le compte réseau est créé sous l'unité d'organisation d'infrastructure. Ce compte gère la passerelle entre votre application et Internet au sens large. Il isole les services réseau, la configuration et le fonctionnement des charges de travail des applications individuelles, de la sécurité et des autres infrastructures.
- Le compte Shared Service est créé sous l'unité d'organisation de l'infrastructure. Ce compte prend en charge les services utilisés par de nombreuses applications et équipes pour obtenir leurs résultats.
- Le compte d'application est créé sous l'unité d'organisation Workloads. Ce compte héberge l'infrastructure et les services principaux permettant d'exécuter et de gérer une application d'entreprise. Ce guide fournit une représentation, mais dans le monde réel, il y aura plusieurs comptes OUs et comptes membres séparés en fonction des applications, des environnements de développement et d'autres considérations de sécurité.
- Des informations de contact alternatives pour la facturation, les opérations et la sécurité de tous les comptes membres sont configurées.

AWS CloudTrail

- Un journal d'organisation est configuré pour permettre la diffusion des événements de CloudTrail gestion dans le compte de gestion et dans tous les comptes membres d'une AWS organisation.
- Le parcours de l'organisation est configuré comme un parcours multirégional.
- Le journal de l'organisation est configuré pour capturer les événements provenant de ressources globales.

- Des pistes supplémentaires permettant de capturer des événements de données spécifiques sont configurées selon les besoins pour surveiller les activités liées aux AWS ressources sensibles.
- Le compte Security Tooling est défini en tant qu'administrateur délégué du journal de l'organisation.
- Le journal de l'organisation est configuré pour être automatiquement activé pour tous les nouveaux comptes membres.
- Le journal de l'organisation est configuré pour publier les journaux dans un compartiment S3 centralisé hébergé dans le compte Log Archive.
- La validation des fichiers journaux est activée dans le journal de l'organisation afin de vérifier l'intégrité des fichiers journaux.
- Le parcours d'organisation est intégré aux CloudWatch journaux pour la conservation des journaux.
- Le suivi de l'organisation est chiffré à l'aide d'une clé gérée par le client.
- Le compartiment S3 central utilisé pour le référentiel de journaux dans le compte Log Archive est chiffré à l'aide d'une clé gérée par le client.
- Le compartiment S3 central utilisé pour le référentiel de journaux dans le compte Log Archive est configuré avec S3 Object Lock pour garantir l'immuabilité.
- La gestion des versions est activée pour le compartiment S3 central utilisé pour le référentiel de journaux dans le compte Log Archive.
- Le compartiment S3 central utilisé pour le référentiel de journaux dans le compte Log Archive possède une politique de ressources définie qui limite le téléchargement d'objets uniquement par suivi de l'organisation via la ressource Amazon Resource Name (ARN).

AWS Security Hub CSPM

- Security Hub CSPM est activé pour tous les comptes membres et le compte de gestion.
- AWS Config est activé pour tous les comptes membres en tant que condition préalable au Security Hub CSPM.
- Le compte Security Tooling est défini en tant qu'administrateur délégué de Security Hub CSPM.
- Amazon GuardDuty et Amazon Detective disposent du même compte d'administrateur délégué que Security Hub CSPM pour une intégration fluide des services.
- La configuration centrale est utilisée pour configurer et gérer Security Hub CSPM sur plusieurs Comptes AWS et. Régions AWS
- Tous les comptes UO et membres sont désignés comme étant gérés de manière centralisée par l'administrateur délégué de Security Hub CSPM.

- Security Hub CSPM est automatiquement activé pour tous les nouveaux comptes membres.
- Security Hub CSPM est automatiquement activé pour la configuration des nouvelles normes.
- Les résultats du Security Hub CSPM provenant de toutes les régions sont regroupés dans une seule région d'origine.
- Les résultats du Security Hub CSPM provenant de tous les comptes membres sont agrégés dans le compte Security Tooling.
- La norme AWS Foundational Best Practices (FSBP) de Security Hub CSPM est activée pour tous les comptes membres.
- La norme CIS AWS Foundation Benchmark dans Security Hub CSPM est activée pour tous les comptes membres.
- Les autres normes CSPM du Security Hub sont activées le cas échéant.
- Une règle d'automatisation CSPM du Security Hub est utilisée pour enrichir les résultats en fonction du contexte des ressources.
- La fonctionnalité de réponse automatique et de correction du Security Hub CSPM est utilisée pour créer des EventBridge règles personnalisées afin de prendre des mesures automatiques en fonction de résultats spécifiques.

AWS Config

- L' AWS Config enregistreur est activé pour tous les comptes des membres et pour le compte de gestion.
- L' AWS Config enregistreur est activé pour toutes les régions.
- Le compartiment S3 du canal de AWS Config distribution est centralisé dans le compte Log Archive.
- Le compte d'administrateur AWS Config délégué est défini sur le compte Security Tooling.
- AWS Config possède un agrégateur d'organisations configuré. L'agrégateur inclut toutes les régions.
- AWS Config les packs de conformité sont déployés uniformément sur tous les comptes membres à partir du compte d'administrateur délégué.
- AWS Config les résultats des règles sont automatiquement envoyés au Security Hub CSPM.

Amazon GuardDuty

- GuardDuty le détecteur est activé pour tous les comptes membres et le compte de gestion.
- GuardDuty le détecteur est activé pour toutes les régions.
- GuardDuty le détecteur est automatiquement activé pour tous les nouveaux comptes de membres.
- GuardDuty l'administration déléguée est définie sur le compte Security Tooling.
- GuardDuty les sources de données de base telles que les événements CloudTrail de gestion, les journaux de flux VPC et les journaux de requêtes DNS de Route 53 Resolver sont activées.
- GuardDuty La protection S3 est activée.
- GuardDuty La protection contre les programmes malveillants pour les volumes EBS est activée.
- GuardDuty La protection contre les programmes malveillants pour S3 est activée.
- GuardDuty La protection RDS est activée.
- GuardDuty La protection Lambda est activée.
- GuardDuty La protection EKS est activée.
- GuardDuty La surveillance du temps d'exécution EKS est activée.
- GuardDuty La détection étendue des menaces est activée.
- GuardDuty les résultats sont exportés vers un compartiment S3 central du compte Log Archive pour être conservés.

IAM

- Les utilisateurs IAM ne sont pas utilisés.
- La gestion centralisée de l'accès root pour les comptes des membres est mise en œuvre.
- La tâche centralisée de l'utilisateur root privilégié pour le compte de gestion est exécutée par l'administrateur délégué.
- La gestion centralisée de l'accès root est déléguée au compte Security Tooling.
- Toutes les informations d'identification root du compte membre sont supprimées.
- Toutes les politiques relatives aux Compte AWS mots de passe des membres et des administrateurs sont définies conformément aux normes de sécurité de l'organisation.
- Le conseiller d'accès IAM est utilisé pour examiner les dernières informations utilisées concernant les groupes, les utilisateurs, les rôles et les politiques IAM.

- Les limites d'autorisation sont utilisées pour limiter le maximum d'autorisations possibles pour les rôles IAM.

Analyseur d’accès IAM

- L'analyseur d'accès IAM est activé pour tous les comptes membres et le compte de gestion.
- L'administrateur délégué d'IAM Access Analyzer est défini sur le compte Security Tooling.
- L'analyseur d'accès externe IAM Access Analyzer est configuré avec la zone de confiance de l'organisation dans chaque région.
- L'analyseur d'accès externe IAM Access Analyzer est configuré avec la zone de confiance du compte dans chaque région.
- L'analyseur d'accès interne d'IAM Access Analyzer est configuré avec la zone de confiance de l'organisation dans chaque région.
- L'analyseur d'accès interne d'IAM Access Analyzer est configuré avec la zone de confiance du compte dans chaque région.
- L'analyseur d'accès non utilisé d'IAM Access Analyzer pour le compte courant est créé.
- L'analyseur d'accès non utilisé d'IAM Access Analyzer pour l'organisation actuelle est créé.

Amazon Detective

- Detective est activé pour tous les comptes des membres.
- Detective est automatiquement activé pour tous les nouveaux comptes de membres.
- Detective est activé pour toutes les régions.
- L'administrateur délégué Detective est configuré sur le compte Security Tooling.
- L'administrateur délégué CSPM de Detective GuardDuty, and Security Hub est configuré sur le même compte Security Tooling.
- Detective est intégré à Security Lake pour le stockage et l'analyse des journaux bruts.
- Detective est intégré GuardDuty pour l'ingestion des résultats.
- Detective est en train d'ingérer les journaux d'audit d'Amazon EKS à des fins d'analyse.
- Detective est en train d'ingérer les journaux CSPM de Security Hub à des fins d'analyse.

AWS Firewall Manager

- Les politiques de sécurité de Firewall Manager sont définies.
- L'administrateur délégué de Firewall Manager est défini sur le compte Security Tooling.
- AWS Config est activé comme condition préalable.
- Plusieurs administrateurs de Firewall Manager sont définis avec une portée limitée par unité d'organisation, compte et région.
- Une politique de AWS WAF sécurité Firewall Manager est définie.
- Une politique de journalisation AWS WAF centralisée de Firewall Manager est définie.
- Une politique de sécurité Firewall Manager Shield Advanced est définie.
- Une politique de sécurité du groupe de sécurité Firewall Manager est définie.

Amazon Inspector

- Amazon Inspector est activé pour tous les comptes membres.
- Amazon Inspector est automatiquement activé pour tout nouveau compte membre.
- L'administrateur délégué Amazon Inspector est défini sur le compte Security Tooling.
- L'analyse des EC2 vulnérabilités d'Amazon Inspector est activée.
- L'analyse des vulnérabilités des images ECR par Amazon Inspector est activée.
- La fonction Amazon Inspector Lambda et l'analyse des vulnérabilités des couches sont activées.
- La numérisation du code Lambda par Amazon Inspector est activée.
- L'analyse de sécurité du code Amazon Inspector est activée.

Amazon Macie

- Macie est activé pour les comptes de membres concernés.
- Macie est automatiquement activé pour les nouveaux comptes de membres applicables.
- L'administrateur délégué Macie est configuré sur le compte Security Tooling.
- Les résultats de Macie sont exportés vers un compartiment S3 central dans le compte Log Archive.
- Les compartiments S3 qui stockent les résultats de Macie sont chiffrés à l'aide d'une clé gérée par le client.

- La politique et la politique de classification de Macie sont publiées sur Security Hub CSPM.

Amazon Security Lake

- La configuration de l'organisation Security Lake est activée.
- L'administrateur délégué de Security Lake est défini sur le compte Security Tooling.
- La configuration de l'organisation Security Lake est activée pour les nouveaux comptes membres.
- Le compte Security Tooling est configuré en tant qu'abonné d'accès aux données pour effectuer une analyse des journaux.
- Le compte Security Tooling est configuré en tant qu'abonné aux requêtes de données pour effectuer une analyse des journaux.
- Une source CloudTrail de journal de gestion est activée pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes de membres actifs.
- Une source de journal de flux VPC est activée pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes membres actifs.
- Une source de journal Route 53 est activée pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes de membres actifs.
- CloudTrail un événement de données pour une source de journal S3 est activé pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes membres actifs.
- Une source de journal d'exécution Lambda est activée pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes de membres actifs.
- Une source de journal d'audit Amazon EKS est activée pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes de membres actifs.
- Une source de journal des résultats de Security Hub est activée pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes de membres actifs.
- Une source de AWS WAF journal est activée pour Security Lake dans tous les comptes de membres actifs ou dans certains comptes de membres actifs.
- Les files d'attente SQS de Security Lake dans le compte administrateur délégué sont chiffrées à l'aide d'une clé gérée par le client.
- La file d'attente de lettres mortes SQS de Security Lake dans le compte administrateur délégué est cryptée à l'aide d'une clé gérée par le client.
- Le compartiment S3 de Security Lake est chiffré à l'aide d'une clé gérée par le client.

- Le bucket S3 de Security Lake est doté d'une politique de ressources qui restreint l'accès direct uniquement par Security Lake.

AWS WAF

- Toutes les CloudFront distributions sont associées à AWS WAF.
- Tous les REST d'Amazon API Gateway APIs sont associés AWS WAF.
- Tous les équilibreurs de charge d'application sont associés AWS WAFà.
- Tous les AWS AppSync GraphQL APIs sont associés à. AWS WAF
- Tous les groupes d'utilisateurs Amazon Cognito sont associés à. AWS WAF
- Tous les AWS App Runner services sont associés à AWS WAF.
- Toutes les Accès vérifié par AWS instances sont associées à AWS WAF.
- Toutes les AWS Amplify applications sont associées à AWS WAF.
- AWS WAF la journalisation est activée.
- AWS WAF les journaux sont centralisés dans un compartiment S3 du compte Log Archive.

AWS Shield Advanced

- L'abonnement Shield Advanced est activé et configuré pour être renouvelé automatiquement pour tous les comptes d'applications disposant de ressources destinées au public.
- Shield Advanced est configuré pour toutes les CloudFront distributions.
- Shield Advanced est configuré pour tous les équilibreurs de charge d'application.
- Shield Advanced est configuré pour tous les équilibreurs de charge réseau.
- Shield Advanced est configuré pour toutes les zones hébergées Route 53.
- Shield Advanced est configuré pour toutes les adresses IP Elastic.
- Shield Advanced est configuré pour tous les accélérateurs globaux.
- CloudWatch les alarmes sont CloudFront configurées pour les ressources Route 53 protégées par Shield Advanced.
- L'accès à la Shield Response Team (SRT) est configuré.
- L'engagement proactif de Shield Advanced est activé.
- Les contacts d'engagement proactif de Shield Advanced sont configurés.

- Une AWS WAF règle personnalisée est configurée pour les ressources protégées de Shield Advanced.
- L'atténuation automatique de la couche DDo S de l'application est activée pour les ressources protégées de Shield Advanced.

AWS Réponse aux incidents de sécurité

- AWS La réponse aux incidents de sécurité est activée pour l'ensemble de AWS l'organisation.
- L'administrateur délégué pour la réponse aux incidents de AWS sécurité est défini sur le compte Security Tooling.
- Le flux de travail proactif de réponse et de triage des alertes est activé.
- AWS Les actions de confinement de l'équipe de réponse aux incidents clients (CIRT) sont autorisées.

AWS Audit Manager

- Audit Manager est activé pour tous les comptes membres.
- Audit Manager est automatiquement activé pour les nouveaux comptes membres.
- L'administrateur délégué d'Audit Manager est défini sur le compte Security Tooling.
- AWS Config est activé comme condition préalable à Audit Manager.
- Une clé gérée par le client est utilisée pour les données stockées dans Audit Manager.
- La destination du rapport d'évaluation par défaut est configurée.

Ressources IAM

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Bien que Gestion des identités et des accès AWS (IAM) ne soit pas un service inclus dans un schéma d'architecture traditionnel, il touche tous les aspects de l' AWS organisation Comptes AWS, et Services AWS. Vous ne pouvez pas en déployer Services AWS sans créer d'entités IAM et accorder d'abord des autorisations. Une explication complète de l'IAM dépasse le cadre de ce document, mais cette section fournit des résumés importants des recommandations relatives aux meilleures pratiques et des indications vers des ressources supplémentaires.

- Pour connaître les meilleures pratiques en matière d'IAM, consultez les meilleures pratiques de sécurité en matière d'IAM dans la AWS documentation, les articles IAM du blog sur la AWS sécurité et AWS les présentations de re:Invent.
- Le pilier de sécurité AWS Well-Architected décrit les étapes clés du processus de gestion des autorisations : définir des barrières en matière d'autorisations, accorder le moindre privilège d'accès, analyser les accès publics et intercomptes, partager les ressources en toute sécurité, réduire les autorisations en permanence et établir un processus d'accès d'urgence.
- Le tableau suivant et les notes qui l'accompagnent fournissent un aperçu général des conseils recommandés sur les types de politiques d'autorisation IAM disponibles et sur la manière de les utiliser dans votre architecture de sécurité. Pour en savoir plus, visionnez la vidéo AWS re:Invent 2020 sur le choix de la bonne combinaison de politiques IAM.

Cas d'utilisation ou politique	Effet	Géré par	Objectif	Se rapporte à	Affecte	Déployé dans
Politiques de contrôle des services (SCPs)	Restrict	Équipe centrale, telle que l'équipe chargée	Garde-corps, gouvernance	Organisation, unité d'organisation, compte	Tous les principes de l'organisation, de l'unité	Compte de gestion de l'organisation [2]

		de la plateforme ou de la sécurité [1]			d'organisation et des comptes	
Politiques de contrôle des ressources (RCPs)	Restrict	Équipe centrale, telle que l'équipe chargée de la plateforme ou de la sécurité [1]	Garde-corps, gouvernance	Organisation, unité d'organisation, compte	Ressources figurant dans les comptes des membres [12]	Compte de gestion de l'organisation [2]
Politiques d'automatisation des comptes de base (les rôles IAM utilisés par la plateforme pour gérer un compte)	Accorder et restreindre	Équipe centrale, telle que l'équipe chargée de la plateforme, de la sécurité ou de l'IAM [1]	Autorisations pour les rôles d'automatisation (de base) autres que la charge de travail [3]	Compte unique [4]	Principes utilisés par l'automatisation au sein d'un compte membre	Comptes de membres

Politiques humaines de base (les rôles IAM qui accordent aux utilisateurs les autorisations nécessaires pour effectuer leur travail)	Accorder et restreindre	Équipe centrale, telle que l'équipe chargée de la plateforme, de la sécurité ou de l'IAM [1]	Autorisations pour les rôles humains [5]	Compte unique [4]	Principaux fédérés [5] et utilisateurs IAM [6]	Comptes de membres
Limites d'autorisations (autorisations maximales qu'un développeur habilité peut attribuer à un autre directeur)	Restrict	Équipe centrale, telle que l'équipe chargée de la plateforme, de la sécurité ou de l'IAM [1]	Garde-fous pour les rôles d'application (doivent être appliqués)	Compte unique [4]	Rôles individuels pour une application ou une charge de travail dans ce compte [7]	Comptes de membres

Politiques relatives aux rôles des machines pour les applications (rôle attaché à l'infrastructure déployée par les développeurs)	Accorder et restreindre	Délégué aux développeurs [8]	Autorisation pour l'application ou la charge de travail [9]	Compte unique	Un principal sur ce compte	Comptes de membres
Politiques basées sur une ressource	Accorder et restreindre	Délégué aux développeurs [8,10]	Autorisations d'accès aux ressources	Compte unique	Un principal dans un compte [11]	Comptes de membres
Gestion centralisée des utilisateurs root	Accorder et restreindre	Équipe centrale, telle que l'équipe chargée de la plateforme, de la sécurité ou de l'IAM [1]	Gérez de manière centralisée les utilisateurs root du compte membre à grande échelle	Organisation	Tous les utilisateurs root des comptes membres	Compte de gestion de l'organisation, compte administrateur délégué

Remarques tirées du tableau :

1. Les entreprises disposent de nombreuses équipes centralisées (telles que les équipes chargées des plateformes cloud, des opérations de sécurité ou des équipes de gestion des identités et des accès) qui se répartissent les responsabilités liées à ces contrôles indépendants et évaluent les politiques des uns et des autres. Les exemples présentés dans le tableau sont des espaces réservés. Vous devrez déterminer la séparation des tâches la plus efficace pour votre entreprise.
2. Pour l'utiliser SCPs, vous devez activer toutes les fonctionnalités qu'il contient AWS Organizations.
3. Des rôles et des politiques de base communs sont généralement nécessaires pour permettre l'automatisation, tels que les autorisations pour le pipeline, les outils de déploiement, les outils de surveillance (par exemple, AWS Lambda et AWS Config Rules) et d'autres autorisations. Cette configuration est généralement fournie lors du provisionnement du compte.
4. Bien qu'elles concernent une ressource (telle qu'un rôle ou une politique) dans un seul compte, elles peuvent être répliquées ou déployées sur plusieurs comptes à l'aide de. AWS CloudFormation StackSets
5. Définissez un ensemble de règles et de rôles humains de base qui sont déployés sur tous les comptes des membres par une équipe centrale (souvent lors de la mise en service des comptes). Les développeurs de l'équipe de la plateforme, de l'équipe IAM et des équipes d'audit de sécurité en sont des exemples.
6. Utilisez la fédération d'identité (au lieu des utilisateurs IAM locaux) dans la mesure du possible.
7. Les limites des autorisations sont utilisées par les administrateurs délégués. Cette politique IAM définit les autorisations maximales et remplace les autres politiques (y compris les `"*:*"` politiques qui autorisent toutes les actions sur les ressources). Les limites d'autorisations devraient être requises dans les politiques humaines de base comme condition pour créer des rôles (tels que les rôles de performance de la charge de travail) et pour associer des politiques. Des configurations supplémentaires, telles que SCPs l'imposition de la limite des autorisations, sont obligatoires.
8. Cela suppose que des barrières de sécurité suffisantes (par exemple, SCPs et des limites d'autorisations) ont été déployées.
9. Ces politiques facultatives peuvent être mises en œuvre lors de la création du compte ou dans le cadre du processus de développement de l'application. L'autorisation de créer et d'associer ces politiques sera régie par les autorisations du développeur de l'application.
10. Outre les autorisations des comptes locaux, une équipe centralisée (telle que l'équipe de la plateforme cloud ou l'équipe des opérations de sécurité) gère souvent certaines politiques basées sur les ressources afin de permettre l'accès entre comptes pour gérer les comptes (par exemple, pour fournir un accès aux compartiments S3 à des fins de journalisation).

11. Une politique IAM basée sur les ressources peut faire référence à n'importe quel principal de n'importe quel compte pour autoriser ou refuser l'accès à ses ressources. Il peut même faire référence à des principes anonymes pour permettre l'accès public.
12. RCPs s'appliquent aux ressources d'un sous-ensemble de. Services AWS Pour plus d'informations, consultez la liste de Services AWS ce support RCPs dans la AWS Organizations documentation.

Il est essentiel de s'assurer que les identités IAM disposent uniquement des autorisations nécessaires pour un ensemble bien défini de tâches afin de réduire le risque d'abus d'autorisations malveillant ou involontaire. L'établissement et le maintien d'un modèle de moindre privilège nécessitent un plan délibéré pour continuellement mettre à jour, évaluer et atténuer les privilèges excessifs. Voici quelques recommandations supplémentaires pour ce plan :

- Utilisez le modèle de gouvernance de votre organisation et sa propension au risque établie pour établir des garde-fous et des limites d'autorisations spécifiques.
- Mettez en œuvre le principe du moindre privilège par le biais d'un processus itératif continu. Il ne s'agit pas d'un exercice ponctuel.
- SCPs À utiliser pour réduire les risques exploitables. Il s'agit de barrières de sécurité larges, et non de contrôles étroitement ciblés.
- Utilisez les limites d'autorisations pour déléguer l'administration IAM de manière plus sûre.
  - Assurez-vous que les administrateurs délégués attachent la politique de limite IAM appropriée aux rôles et aux utilisateurs qu'ils créent.
- En tant qu' defense-in-depthapproche (en conjonction avec des politiques basées sur l'identité), utilisez des politiques IAM basées sur les ressources pour refuser un accès étendu aux ressources.
- Utilisez le conseiller d'accès IAM AWS CloudTrail, l'analyseur d'accès IAM et les outils associés pour analyser régulièrement l'historique de l'utilisation et les autorisations accordées. Corrigez immédiatement les autorisations excessives évidentes.
- Délimitez les actions générales à des ressources spécifiques, le cas échéant, au lieu d'utiliser un astérisque comme caractère générique pour indiquer toutes les ressources.
- Mettez en œuvre un mécanisme permettant d'identifier, d'examiner et d'approuver rapidement les exceptions à la politique IAM en fonction des demandes.

Référentiel de code pour les AWS exemples de SRA

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Pour vous aider à commencer à élaborer et à mettre en œuvre les directives de la AWS SRA, un référentiel d'infrastructure en tant que code (IaC) sur https://github.com/aws-samples/aws-security-reference-architecture-examples accompagne ce guide. Ce référentiel contient du code destiné à aider les développeurs et les ingénieurs à déployer certains des conseils et modèles d'architecture présentés dans ce document. Ce code est tiré de l'expérience directe des consultants en services AWS professionnels avec les clients. Les modèles sont de nature générale : leur objectif est d'illustrer un modèle de mise en œuvre plutôt que de fournir une solution complète. Les Service AWS configurations et les déploiements de ressources sont délibérément très restrictifs. Vous devrez peut-être modifier et adapter ces solutions en fonction de votre environnement et de vos besoins en matière de sécurité.

Le référentiel de code AWS SRA fournit des exemples de code avec les options de déploiement à la fois AWS CloudFormation et Terraform. Les modèles de solution prennent en charge deux environnements : l'un nécessite AWS Control Tower et l'autre n'en utilise AWS Organizations pas AWS Control Tower. Les solutions requises dans ce référentiel AWS Control Tower ont été déployées et testées dans un AWS Control Tower environnement à l'aide de AWS CloudFormation et de personnalisations pour AWS Control Tower (CfCT). Les solutions qui n'en nécessitent pas AWS Control Tower ont été testées dans un AWS Organizations environnement à l'aide de AWS CloudFormation. La solution CfCT aide les clients à configurer rapidement un AWS environnement multi-comptes sécurisé basé sur les AWS meilleures pratiques. Il permet de gagner du temps en automatisant la configuration d'un environnement permettant d'exécuter des charges de travail sécurisées et évolutives tout en mettant en œuvre une base de sécurité initiale via la création de comptes et de ressources. AWS Control Tower fournit également un environnement de base pour démarrer avec une architecture multi-comptes, la gestion des identités et des accès, la gouvernance, la sécurité des données, la conception du réseau et la journalisation. Les solutions du référentiel AWS SRA fournissent des configurations de sécurité supplémentaires pour implémenter les modèles décrits dans ce document.

Voici un résumé des solutions du référentiel AWS SRA. Chaque solution inclut un `README.md` fichier contenant des informations détaillées.

- La solution CloudTrail Organization crée une trace de l'organisation dans le compte de gestion de l'organisation et délègue l'administration à un compte membre tel que le compte Audit ou Security Tooling. Ce journal est chiffré à l'aide d'une clé gérée par le client créée dans le compte Security Tooling et transmet les journaux à un compartiment S3 du compte Log Archive. En option, les événements de données peuvent être activés pour Amazon S3 et AWS Lambda ses fonctions. Un journal d'organisation enregistre les événements pour tous les Comptes AWS membres de l' AWS organisation tout en empêchant les comptes des membres de modifier les configurations.
- La solution GuardDuty Organization active Amazon GuardDuty en déléguant l'administration au compte Security Tooling. Il est configuré GuardDuty dans le compte Security Tooling pour tous les comptes d' AWS organisation existants et futurs. Les GuardDuty résultats sont également chiffrés à l'aide d'une clé KMS et envoyés vers un compartiment S3 du compte Log Archive.
- La solution Security Hub CSPM Organization configure Security Hub CSPM en déléguant l'administration au compte Security Tooling. Il configure Security Hub CSPM dans le compte Security Tooling pour tous les comptes d'organisation existants et futurs. AWS La solution fournit également des paramètres pour synchroniser les normes de sécurité activées sur tous les comptes et régions, ainsi que pour configurer un agrégateur de régions au sein du compte Security Tooling. La centralisation du Security Hub CSPM au sein du compte Security Tooling fournit une vue multicompte de la conformité aux normes de sécurité et des résultats des intégrations effectuées à la fois et par des tiers. Services AWS AWS Partner
- La solution Inspector configure Amazon Inspector au sein du compte administrateur délégué (Security Tooling) pour tous les comptes et régions gouvernées au sein de l' AWS organisation.
- La solution Firewall Manager configure les politiques AWS Firewall Manager de sécurité en déléguant l'administration au compte Security Tooling et en configurant Firewall Manager avec une politique de groupe de sécurité et plusieurs politiques. AWS WAF La politique des groupes de sécurité exige un groupe de sécurité maximal autorisé au sein d'un VPC (existant ou créé par la solution), qui est déployé par la solution.
- La solution Macie Organization active Amazon Macie en déléguant l'administration au compte Security Tooling. Il configure Macie dans le compte Security Tooling pour tous les comptes d'organisation existants et futurs. AWS Macie est également configuré pour envoyer ses résultats de découverte à un compartiment S3 central chiffré à l'aide d'une clé KMS.
- AWS Config:
  - La solution Config Aggregator configure un AWS Config agrégateur en déléguant l'administration au compte Security Tooling. La solution configure ensuite un AWS Config agrégateur au sein du compte Security Tooling pour tous les comptes existants et futurs de l'organisation. AWS

  - La solution Conformance Pack Organization Rules se déploie AWS Config Rules en déléguant l'administration au compte Security Tooling. Il crée ensuite un pack de conformité d'organisation dans le compte d'administrateur délégué pour tous les comptes existants et futurs de l' AWS organisation. La solution est configurée pour déployer le modèle d'exemple de pack de conformité aux meilleures pratiques opérationnelles pour le chiffrement et la gestion des clés.
  - La solution AWS Config Control Tower Management Account active l'accès AWS Config au compte AWS Control Tower de gestion et met à jour l' AWS Config agrégateur du compte Security Tooling en conséquence. La solution utilise le AWS Control Tower CloudFormation modèle d'activation AWS Config comme référence afin de garantir la cohérence avec les autres comptes de l' AWS organisation.
- IAM :
  - La solution Access Analyzer active IAM Access Analyzer en déléguant l'administration au compte Security Tooling. Il configure ensuite un analyseur d'accès IAM au niveau de l'organisation dans le compte Security Tooling pour tous les comptes existants et futurs de l'organisation. AWS La solution déploie également IAM Access Analyzer sur tous les comptes membres et régions afin de faciliter l'analyse des autorisations au niveau des comptes.
  - La solution IAM Password Policy met à jour la politique Compte AWS de mot de passe pour tous les comptes d'une AWS organisation. La solution fournit des paramètres permettant de configurer les paramètres de politique de mot de passe afin de vous aider à vous aligner sur les normes de conformité du secteur.
- La solution de chiffrement EBS EC2 par défaut permet le chiffrement Amazon EBS par défaut au niveau du compte au sein de chaque compte Compte AWS et Région AWS au sein de l'organisation. AWS Il applique le chiffrement des nouveaux volumes EBS et des instantanés que vous créez. Par exemple, Amazon EBS chiffre les volumes EBS créés lorsque vous lancez une instance et les instantanés que vous copiez à partir d'un instantané non chiffré.
- La solution S3 Block Account Public Access permet de configurer les paramètres au niveau du compte Amazon S3 au sein de chaque Compte AWS entreprise. AWS La fonction du blocage de l'accès public Amazon S3 fournit des paramètres pour les points d'accès, les compartiments et les comptes afin de vous aider à gérer l'accès public aux ressources Amazon S3. Par défaut, les nouveaux compartiments, points d'accès et objets n'autorisent pas l'accès public. Toutefois, les utilisateurs peuvent modifier les stratégies de compartiment, les stratégies de point d’accès ou les autorisations d’objet pour autoriser l’accès public. Les paramètres de blocage de l'accès public d'Amazon S3 remplacent ces politiques et autorisations afin que vous puissiez limiter l'accès public à ces ressources.

- La solution Detective Organization automatise l'activation d'Amazon Detective en déléguant l'administration à un compte (tel que le compte Audit ou Security Tooling) et en configurant Detective pour tous les comptes existants et futurs. AWS Organizations
- La solution Shield Advanced automatise le déploiement de AWS Shield Advanced afin de fournir une protection DDo S améliorée à vos applications sur AWS.
- La solution AMI Bakery Organization permet d'automatiser le processus de création et de gestion d'images Amazon Machine Image (AMI) standard et renforcées. Cela garantit la cohérence et la sécurité de vos AWS instances et simplifie les tâches de déploiement et de maintenance.
- La solution Patch Manager permet de rationaliser la gestion des correctifs sur plusieurs sites Comptes AWS. Vous pouvez utiliser cette solution pour mettre à jour AWS Systems Manager l'agent (agent SSM) sur toutes les instances gérées, ainsi que pour scanner et installer des correctifs de sécurité et des corrections de bogues critiques et importants sur les instances étiquetées Windows et Linux. La solution configure également le paramètre de configuration de gestion des hôtes par défaut afin de détecter la création de nouveaux comptes Comptes AWS et de déployer automatiquement la solution sur ces comptes.

Collaborateurs

Auteur principal :

- Avik Mukherjee, senior de la sécurité SA AWS

Contributeurs :

- Jason Hurst, enquêteur principal en matière de sécurité du AWS CIRT
- Abhishek Panday, AWS chef de produit principal — Technologie
- Itay Meller, spécialiste AWS principal, États-Unis
- Jonathan VanKim, AWS directeur de la sécurité SA
- Josh Du Lac, stratège en sécurité AWS d'entreprise
- James Thompson, architecte de solutions AWS senior
- Jeremy Girven, AWS spécialiste SA
- Rodney Underkoffler, spécialiste senior SA AWS
- Farhan Farooq, AWS architecte de solutions senior
- Prashob Krishnan, responsable des comptes techniques AWS
- Meg Peddada, consultante AWS principale en sécurité
- Ashwin Phadke, AWS architecte de solutions senior
- Sowjanya Rajavaram, responsable de la sécurité SA AWS
- Tomek Jakubowski, consultant principal AWS
- Arun Thomas, architecte de solutions AWS senior
- Ross Warren, architecte AWS de solutions de produits
- Scott Conklin, consultant principal AWS
- Ilya Epshteyn, directrice AWS principale des solutions d'identité
- Michael Haken, technologue AWS principal
- Mehial Mendrin, consultante principale AWS
- Christopher Evensen, directeur technique AWS principal des comptes

Révision :

- Eric Rose, AWS directeur de la sécurité SA
- Manoj Kumar, consultant en livraison AWS

Rédaction technique :

- Handan Selamoglu, rédacteur technique principal AWS

Annexe : services AWS de sécurité, d'identité et de conformité

Influencez le futur de l'architecture de référence de AWS sécurité (AWS SRA) en répondant à une courte enquête.

Pour une introduction ou un rappel, consultez la section Sécurité, identité et conformité AWS sur le AWS site Web pour obtenir une liste des solutions Services AWS qui vous aident à sécuriser vos charges de travail et vos applications dans le cloud. Ces services sont regroupés en cinq catégories : protection des données, gestion des identités et des accès, protection du réseau et des applications, détection des menaces et surveillance continue, conformité et confidentialité des données.

Protection des données : AWS fournit des services qui vous aident à protéger vos données, vos comptes et vos charges de travail contre tout accès non autorisé.

- Amazon Macie — Découvrez, classez et protégez les données sensibles grâce à des fonctionnalités de sécurité basées sur l'apprentissage automatique.
- AWS KMS— Créez et contrôlez les clés utilisées pour chiffrer vos données.
- AWS CloudHSM— Gérez les modules de sécurité de votre matériel (HSMs) dans le AWS Cloud.
- AWS Certificate Manager— Fournissez, gérez et déployez SSL/TLS des certificats à utiliser avec Services AWS.
- AWS Secrets Manager— Faites pivoter, gérez et récupérez les informations d'identification de base de données, les clés d'API et d'autres secrets tout au long de leur cycle de vie.

Gestion des identités et des accès : les services AWS d'identité vous permettent de gérer en toute sécurité les identités, les ressources et les autorisations à grande échelle.

- IAM — Contrôlez en toute sécurité l'accès Services AWS et les ressources.
- IAM Identity Center — Gérez de manière centralisée l'accès SSO à de multiples Comptes AWS applications professionnelles.
- Amazon Cognito — Ajoutez l'inscription, la connexion et le contrôle d'accès des utilisateurs à vos applications Web et mobiles.
- AWS Directory Service— Utilisez Microsoft Active Directory géré dans le AWS Cloud.

- AWS RAM— Partagez AWS des ressources simplement et en toute sécurité.
- AWS Organizations— Mettez en œuvre une gestion basée sur des règles pour plusieurs Comptes AWS.
- Autorisations vérifiées par Amazon : gérez des autorisations et des autorisations évolutives et détaillées dans vos applications personnalisées.

Protection du réseau et des applications : ces catégories de services vous permettent d'appliquer une politique de sécurité précise aux points de contrôle réseau de votre entreprise. Services AWS vous aident à inspecter et à filtrer le trafic afin d'empêcher tout accès non autorisé aux ressources au niveau de l'hôte, du réseau et des applications.

- AWS Shield— Protégez vos applications Web qui s'exécutent AWS grâce à une protection DDo S gérée.
- AWS WAF— Protégez vos applications Web contre les exploits Web courants et garantissez la disponibilité et la sécurité.
- AWS Firewall Manager— Configurez et gérez les AWS WAF règles pour l'ensemble Comptes AWS des applications à partir d'un emplacement central.
- AWS Systems Manager— Configurez et gérez Amazon EC2 et les systèmes sur site pour appliquer les correctifs du système d'exploitation, créer des images système sécurisées et configurer des systèmes d'exploitation sécurisés.
- Amazon VPC : fournissez une section isolée de manière logique dans AWS laquelle vous pouvez lancer des AWS ressources dans un réseau virtuel que vous définissez.
- AWS Network Firewall— Déployez les protections réseau essentielles pour votre VPCs.
- Pare-feu DNS Amazon Route 53 — Protégez vos requêtes DNS sortantes contre votre VPCs.
- Accès vérifié par AWS— Fournissez un accès sécurisé à vos applications sans avoir besoin de réseaux privés virtuels (VPNs).
- Amazon VPC Lattice — Simplifiez la service-to-service connectivité, la sécurité et la surveillance.

Détection des menaces et surveillance continue : les services AWS de surveillance et de détection fournissent des conseils pour vous aider à identifier les incidents de sécurité potentiels dans votre AWS environnement.

- AWS Security Hub CSPM— Consultez et gérez les alertes de sécurité et automatisez les contrôles de conformité à partir d'un emplacement central.

- AWS Security Hub— Corrélez et enrichissez les résultats de sécurité pour hiérarchiser les problèmes de sécurité critiques sur l'ensemble de vos comptes et Régions AWS.
- Amazon GuardDuty — Protégez votre charge de travail Comptes AWS et celle de vos charges de travail grâce à une détection intelligente des menaces et à une surveillance continue.
- Amazon Inspector — Automatisez les évaluations de sécurité pour améliorer la sécurité et la conformité de vos applications déployées sur AWS.
- AWS Config— Enregistrez et évaluez les configurations de vos AWS ressources pour permettre l'audit de conformité, le suivi des modifications des ressources et l'analyse de sécurité.
- AWS Config Rules— Créez des règles qui agissent automatiquement en réponse aux modifications de votre environnement, par exemple en isolant les ressources, en enrichissant les événements avec des données supplémentaires ou en rétablissant la configuration dans un état dont le fonctionnement a été vérifié.
- AWS Security Incident Response— Automatisez la réponse, l'investigation et la résolution des incidents de sécurité à l'aide de playbooks et de flux de travail prédéfinis.
- AWS CloudTrail— Suivez l'activité des utilisateurs et l'utilisation des API pour permettre la gouvernance et l'audit opérationnel et des risques de votre entreprise Compte AWS.
- Amazon Detective — Analysez et visualisez les données de sécurité pour identifier rapidement la cause première des problèmes de sécurité potentiels.
- AWS Lambda— Exécutez du code sans provisionner ni gérer de serveurs afin de pouvoir adapter votre réponse automatisée et programmée aux incidents.

Conformité et confidentialité des données : vous AWS donne une vue complète de votre état de conformité et surveille en permanence votre environnement en utilisant des contrôles de conformité automatisés basés sur les AWS meilleures pratiques et les normes du secteur suivies par votre entreprise.

- AWS Artifact— Utilisez un portail en libre-service gratuit pour accéder à la demande aux rapports de AWS sécurité et de conformité et à certains accords en ligne.
- AWS Audit Manager— Auditez en permanence votre AWS utilisation pour simplifier la façon dont vous évaluez les risques et la conformité aux réglementations et aux normes du secteur.

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
Restructuration et mises à jour du contenu	• Ajout de conseils pour Security Hub et AWS Nitro Enclaves. • Restructuration de la AWS SRA pour se concentrer sur l'architecture de base et déplacement des sections détaillées vers des guides distincts pour la gestion des identités, la sécurité du périmètre, la cybercriminalistique, l'IA générative et l'IoT. • Mise à jour des directives existantes pour inclure des informations supplémentaires sur AWS CloudTrail AWS Config, Amazon Detective AWS Firewall Manager GuardDuty, Amazon, IAM Access Analyzer, Amazon Security Lake AWS Shield Advanced, et. AWS Audit Manager	22 décembre 2025
Mises à jour majeures		29 août 2025

- Ajout d'informations sur la nouvelle gestion centralisée de l'accès des utilisateurs root IAM, les politiques de contrôle des ressources (RCPs) et les politiques déclaratives.
- Références du Security Hub CSPM mises à jour au nouveau Security Hub CSPM.
- Nouvelles fonctionnalités de service incluses pour Amazon GuardDuty et Security Hub CSPM.
- Ajout AWS Security Incident Response de conseils de service.
- Mise à jour des directives détaillées de l'IAM pour inclure le VPC Lattice machine-to-machine pour la gestion des identités.
- Ajout d'un nouveau guide d'analyse approfondie : le SRA pour l'IoT.

Ajouts et clarifications	• Dans la section du compte Security Tooling, les AWS KMS instructions ont été mises à jour. • Dans la section Gestion de l'identité des clients, vous avez développé les informations relatives à l'autorisation d'API Gateway. • Mise à jour de la section Generative AI pour ajouter une considération de conception pour la conception des unités d'organisation et des comptes. • Dans la section du référentiel de code AWS SRA, des informations ont été ajoutées sur la nouvelle solution de gestion des correctifs.	12 septembre 2024

Mises à jour majeures	• Ajout de deux sections pour des conseils architecturaux approfondis : IA générative utilisant Amazon Bedrock et gestion des identités. • Mise à jour des AWS Identity and Access Management Access Analyzer CloudFron tsections Amazon Detective AWS Artifact, Amazon Inspector AWS Config,, AWS Security Hub CSPM, Amazon Security Lake et Amazon avec de nouvelles fonctionnalités de service. • Mise à jour de la section du référentiel de code AWS SRA pour inclure la nouvelle option de déploiement de Terraform et l'ajout de solutions AWS Shield Advanced AMI Bakery.	7 juin 2024

Mises à jour majeures	• Mise à jour des sections « Compte réseau » et « Compte d'application » afin d'ajouter des conseils architecturaux pour Amazon Verified Permissions et Amazon VPC Lattice. Accès vérifié par AWS • Ajout de conseils architect uraux approfondis basés sur les fonctionnalités de sécurité. • Ajout de nouvelles directive s sur la manière de les Services AWS utiliser AI/ ML pour obtenir de meilleurs résultats en matière de sécurité. • Ajout de conseils sur la façon de planifier votre architecture de sécurité de manière progressive.	4 novembre 2023
Ajout de Security Lake	Les sections relatives au compte Security Tooling et au compte Log Archive ont été mises à jour afin d'ajouter des conseils de conception relatifs à Amazon Security Lake.	22 septembre 2023

Mises à jour mineures	• Mise à jour des directive s existantes pour refléter les nouvelles Services AWS fonctionnalités et les meilleures pratiques. • Consignes architecturales mises à jour pour AWS CloudTrail AWS IAM Identity Center,, et la sécurité périphérique.	10 mai 2023
Sondage	Ajout d'une courte enquête pour mieux comprendre comment vous utilisez le AWS SRA dans votre organisation.	14 décembre 2022
Fichiers source pour les diagrammes d'architecture de référence	Dans la section Architecture AWS de référence de sécurité, un fichier de téléchargement contenant les diagrammes d'architecture de ce guide a été ajouté dans un PowerPoint format modifiable.	17 novembre 2022
Mises à jour de la section Bases de sécurité	Dans la section Bases de la sécurité, les informations sur les piliers de Well-Architected Framework et les principes de conception de sécurité ont été mises à jour.	27 septembre 2022

Ajouts et mises à jour majeurs	• Ajout d'informations sur l'utilisation du AWS SRA et des directives de mise en œuvre clés. • Ajout de conseils architect uraux pour d'autres applicati ons Services AWS telles qu' AWS Artifact Amazon Inspector AWS RAM, Amazon Route 53, AWS Control Tower,, AWS Audit Manager Directory Service, Amazon Cognito et Network Access Analyzer. • Mise à jour des directive s existantes pour refléter les nouvelles Service AWS fonctionnalités et les meilleures pratiques.	25 juillet 2022
—	Publication initiale	23 juin 2021

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 :

- Refactor/re-architect — Déplacez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives du cloud pour améliorer l'agilité, les performances et l'évolutivité. 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' PostgreSQL-Compatible édition Amazon Aurora.
- 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 (Amazon RDS) 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 sur site vers Oracle sur une instance EC2 dans le. 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 une Microsoft Hyper-V application vers 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

A2 (1) Agent-to-Agent

Protocole dynamique pour la collaboration agent-agent prenant en charge la délégation de tâches et le transfert d'état.

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

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 les bases de données source et cible sont synchronisées, mais seule la base de données source gère les transactions liées à la connexion des 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.

Agent

Un système d'IA capable de raisonner, de planifier et de prendre des mesures de manière autonome à l'aide d'outils pour atteindre des objectifs.

Agent Ops

Pratiques opérationnelles pour la création, le test, le déploiement et l'exécution d'agents d'IA en production à grande échelle.

fonction d'agrégation

Fonction SQL 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 solution 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 la façon dont les AIOps sont utilisées dans la stratégie de migration AWS , veuillez consulter 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, cohérence, isolement, 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 par 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 pour AWS dans la documentation Gestion des identités et des accès AWS (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 La CAF organise ses conseils 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, la 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, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

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 Le WQF est 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 appels d'API 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.

blue/green déploiement

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, connus sous le nom de mauvais robots, 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, il s'agit d'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 Mettre en œuvre des procédures permettant de briser le verre dans le AWS Well-Architected guide.

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

Consultez la section Capture des données de modification.

capture des données de modification (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 utiliser la CDC à diverses 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.

Développeur citoyen

Un utilisateur professionnel qui crée des applications d'intelligence artificielle à l'aide de plateformes sans code/low code sans compétences techniques spécialisées.

chiffrement côté client

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

Centre d'excellence 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 articles du CCoE sur le blog de 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 mettre à l'échelle l'adoption du cloud (par exemple, en créant une zone de destination, en définissant un CCoE ou en établissant un modèle opérationnel)
- Migration : migration d'applications individuelles
- Re-invention — 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 ouBitbucket Cloud. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un CI/CD pipeline unique 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, Amazon SageMaker AI 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 des configurations (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 d'une CMDB lors de la phase de découverte et d'analyse du portefeuille 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 modèle YAML. 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 de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD est communément décrit comme un pipeline. CI/CD peut 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 cadre. 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.

défense en profondeur

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 approche de défense approfondie 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. DVSM étend 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 la section Reprise après sinistre des charges de travail sur AWS : Restauration dans le cloud dans le 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 livre, Domain-Driven Design : Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur la manière dont vous pouvez utiliser la conception axée sur le domaine avec le modèle Strangler Fig, consultez la section Modernisation incrémentielle des anciens services Web ASP.NET Microsoft (ASMX) 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 dans lequel les octets sont stockés dans la mémoire de l'ordinateur. Big-endian les systèmes stockent d'abord l'octet le plus significatif. Little-endian les systèmes 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 sur 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 principaux Comptes AWS ou à Gestion des identités et des accès AWS (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

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

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 CI/CD pipeline, 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 points forts de la AWS CAF en matière de 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. L'EDA est 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 la 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. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients 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 à un LLM un petit 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. Few-shot l'envoi d'instructions peut être efficace pour les tâches qui nécessitent un formatage, un raisonnement ou une connaissance du 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'entraîne sur des ensembles de données massifs de données généralisées et non étiquetées. Les FM sont capables d'effectuer une grande variété de tâches générales, telles que la compréhension du langage, la génération de texte et d'images et la conversation en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

Passerelle FM

Un intermédiaire centralisé qui contrôle et normalise l'accès aux modèles de base. Également connue sous le nom de passerelle LLM.

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 d'organisation (UO). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. 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 CSPM GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

rambardes (AI)

Des mécanismes de sécurité qui filtrent, valident et limitent les entrées et sorties des agents afin de garantir un comportement responsable et sûr de l'IA.

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 de l'historien

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.

humain dans la boucle (HiTL)

Un modèle de flux de travail dans lequel l'exécution des agents s'arrête pour examen et approbation par l'homme aux points de décision critiques.

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 principaux IAM qui définit leurs autorisations au sein de l' AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne du processeur et 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.

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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. AI/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, veuillez consulter Building an industrial Internet of Things (IIoT) digital transformation strategy.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau entre les VPC (identiques ou Régions AWS différents), Internet et les réseaux sur site. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et 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. L'ITIL constitue la base de l'ITSM.

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 outils ITSM, veuillez consulter 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. Un 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 les LLM.

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, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

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 la 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.

MCP

Voir Model Context Protocol.

Protocole de contexte du modèle (MCP)

Protocole sans état pour la communication entre un agent et un outil.

serveur MCP

Service qui expose un ou plusieurs outils via le protocole Model Context.

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 AWS Well-Architected cadre.

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.

MAILLES

Voir le système d'exécution de la fabrication.

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

Un protocole de communication léger de machine à machine (M2M), basé sur le publish/subscribemodèle, pour les appareils IoT aux ressources limitées.

microservice

Petit service indépendant qui communique via des API bien définies 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 à l'aide d'API légères. 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.

Programme d'accélération des migrations (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. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'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

Cross-functional des équipes qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des 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 AWS avec le service de migration 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 La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'outil MPA (connexion requise) est disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation 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. La MRA est la première phase de la stratégie de migration AWS.

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-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat 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 Examens de l'état de préparation opérationnelle (ORR) dans le AWS Well-Architected cadre.

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. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant l'adoption des changements, en abordant les problèmes de transition et en favorisant 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, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il 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 précis et amélioré.

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture de référence de sécuritéAWS recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique Limites des autorisations dans la documentation IAM.

informations personnelles 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. Les exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

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.

policy

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.

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 rôle IAM ou un utilisateur. Pour plus

d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

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 qui contient des informations concernant la façon dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines dans un ou plusieurs VPC. 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 invite LLM 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 MES basé sur des microservices, 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 relationnelle SQL.

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

Matrice RACI

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.

Matrice RASCI

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 de 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, redevable, consulté et informé (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 matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

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'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que 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)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend 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

SAML 2.0

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 opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 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 associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM 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, mais aussi 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 en matière AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une instance Amazon EC2 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. Les SCP définissent des barrières de protection ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez utiliser les SCP comme listes d'autorisation ou de refus, pour indiquer 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

URL du point d'entrée pour 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.

contrat 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.

IA de l'ombre

Applications d'IA non autorisées créées ou utilisées en dehors des canaux régis au sein d'une organisation.

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.

modèle split-and-seed

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 d'application de ce modèle, consultez la section Modernisation progressive des anciens services Web Microsoft ASP.NET (ASMX) à l'aide de conteneurs et d'Amazon API Gateway.

sous-réseau

Plage d'adresses IP dans votre VPC. 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 LLM afin d'orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

T

tags

Key-value des paires 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.

outil

Fonction ou API qu'un agent peut invoquer pour effectuer des opérations dans des systèmes externes.

passerelle de transit

Hub de transit de réseau que vous pouvez utiliser pour relier vos VPC et vos réseaux 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.

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.

Appairage de VPC

Connexion entre deux VPC qui vous permet d'acheminer le trafic à l'aide d'adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

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

Fonction SQL 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.

VER

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 à un LLM des instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. Le LLM doit utiliser ses connaissances pré-entraînées pour gérer 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 du processeur et de 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.