AWSArchitecture de référence en matière de sécurité

AWSDirectives prescriptives

AWSDirectives prescriptives: AWSArchitecture de référence en matière de sécurité

Table of Contents

AWSArchitecture de référence de sécurité (AWSSRA)

Amazon Web Services (AWS)

Novembre 2023 (historique du document)

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

L'architecture de référence de sécurité (AWS SRA) d'Amazon Web Services (AWS) est un ensemble global de directives pour le déploiement de l'ensemble des services de sécurité AWS dans un environnement multi-comptes. Utilisez-le pour concevoir, implémenter et gérer les services de sécurité AWS afin qu'ils soient conformes aux pratiques recommandées par AWS. Les recommandations reposent sur une architecture d'une seule page qui inclut les services de sécurité AWS : comment ils contribuent à atteindre les objectifs de sécurité, où ils peuvent être déployés et gérés au mieux dans vos 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 de sécurité AWS.

L'architecture et les recommandations qui l'accompagnent sont basées sur nos expériences collectives avec les entreprises clientes d'AWS. Ce document est une référence, un ensemble complet de directives relatives à l'utilisation des services AWS 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 environnement AWS 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.

L'AWS SRA est un ensemble de directives évolutives mises à jour régulièrement 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 :

- La valeur de l'AWS SRA décrit les raisons qui ont motivé la création de l'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 cadre d'adoption du cloud AWS (AWS CAF), l'AWS Well-Architected Framework et le modèle de responsabilité partagée d'AWS, et met en évidence les éléments particulièrement pertinents pour l'AWS SRA.
- AWS Organizations, accounts, and IAM guardrails présente le service AWS Organizations, décrit les fonctionnalités de sécurité fondamentales et les garde-fous, et donne un aperçu de la stratégie multicompte que nous recommandons.
- L'architecture de référence de sécurité AWS est un schéma d'architecture d'une page qui montre les comptes AWS fonctionnels, ainsi que les services et fonctionnalités de sécurité généralement disponibles.
- L'analyse approfondie de l'architecture aborde les modèles architecturaux avancés basés sur des fonctionnalités de sécurité spécifiques sur lesquelles vous souhaiterez peut-être vous concentrer après avoir créé votre architecture de sécurité de base.
- L'IA et le ML pour la sécurité décrivent comment les différents 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 inclure ces services AWS dans votre conception afin de 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 l'AWS SRA.
- Les ressources IAM présentent un résumé et un ensemble de conseils relatifs aux directives AWS Identity and Access Management (IAM) qui sont importantes pour votre architecture de sécurité.
- Le référentiel de code pour les exemples AWS SRA fournit une vue d'ensemble du GitHubréférentiel associé qui contient des exemples de CloudFormation modèles AWS et du code pour déployer certains des modèles décrits dans l'AWS SRA.

- L'architecture de référence de confidentialité AWS (AWS PRA) introduit une architecture de référence de sécurité supplémentaire basée sur l'AWS SRA pour répondre aux exigences de conformité en matière de confidentialité.

L'annexe contient une liste des différents services AWS de 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.

> **Note**
>
> 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)

La valeur de l'AWS SRA

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

AWS dispose d'un ensemble important (et croissant) de services liés à la sécurité et 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 sécurité AWS. 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 de sécurité AWS 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) influe-t-il sur les objectifs de sécurité ? Quels compromis (considérations de conception) les clients doivent-ils prendre en compte ?
- Les clients souhaitent découvrir différentes perspectives pour organiser de manière logique les nombreux services de sécurité AWS. 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 guide regroupe les services en fonction des couches de protection alignées sur la structure recommandée de votre environnement AWS.
- 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 aligner et connecter au mieux AWS Config à d'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 de sécurité AWS s'appuie sur d'autres services de sécurité ou les prend en charge.

Nous abordons chacune de ces questions dans l'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 architecture AWS Organizations recommandée et une

account-by-account description des services destinés à chaque destination. 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 au sein de votre organisation AWS. Cette section décrit un moyen de regrouper les services de sécurité en fonction de la structure des éléments de votre organisation AWS. En outre, ces mêmes idées se reflètent dans la discussion sur le compte de l'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 différents services dans les sections de cette documentation consacrées aux comptes et dans le code du référentiel de code AWS SRA.

Comment utiliser l'AWS SRA

Il existe différentes manières d'utiliser l'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 ressources 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 transition vers le cloud AWS, en configurant votre premier ensemble de comptes, ou que vous envisagiez d'améliorer un environnement AWS établi, l'AWS SRA est l'endroit idéal pour commencer à 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 d'AWS SRA comme base pour l'architecture de référence de sécurité de votre organisation. Pour savoir comment atteindre l'état cible décrit par l'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 avec l'AWS SRA. L'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 norme AWS SRA, vous pouvez être plus sûr de suivre les meilleures pratiques lors de l'utilisation des services AWS. Si vos conceptions de sécurité divergent ou ne sont pas conformes aux directives de l'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 bonnes pratiques 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 bien, au lieu d'utiliser les services AWS, vous pouvez avoir une préférence de fonctionnalité pour un produit du réseau de partenaires AWS ou pour une application personnalisée que vous avez créée et gérée. Au cours de cet examen, vous découvrirez peut-être que vos décisions précédentes ont été prises en fonction de technologies plus anciennes, de fonctionnalités AWS ou de contraintes commerciales 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 l'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 en tant que 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 AWS SRA, mais ils intègrent également les contrôles de sécurité recommandés tels que les politiques de mot de passe AWS Identity and Access Management (IAM), l'accès public aux comptes de blocage Amazon Simple Storage Service (Amazon S3), le chiffrement Amazon Elastic Block Store (Amazon EBS) par défaut d'Amazon EC2, et intégration à AWS Control Tower afin que les contrôles soient appliqués ou supprimés à mesure que de nouveaux comptes AWS sont intégrés ou mis hors service.

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

Les conseils et les discussions au sein de l'AWS SRA incluent des fonctionnalités importantes ainsi que des considérations relatives au déploiement et à la gestion pour les différents services liés à la sécurité AWS. L'une des caractéristiques de l'AWS SRA est qu'il fournit une introduction de haut

niveau à l'étendue des services de sécurité AWS 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 intègre les résultats de sécurité provenant de divers services AWS, de produits de partenaires AWS et même 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 les clés AWS Key Management Service (AWS KMS) et les comptes dans lesquels ces clés seront gérées. Comprendre les caractéristiques de votre organisation (les différentes équipes et responsabilités) vous aidera à adapter l'AWS SRA à vos besoins. 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. L'AWS SRA peut être un moyen d'identifier et d'éclairer ces discussions.

Principales directives de mise en œuvre de l'AWS SRA

Voici huit points essentiels à retenir de l'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 essentiels 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.

- D efense-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 structure d'AWS Organizations, 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. L'AWS SRA montre comment les différents services AWS fonctionnent à différentes couches de la pile technologique AWS, et comment l'utilisation combinée de ces services peut vous aider à y parvenir defense-in-depth. Ce defense-in-depth concept sur AWS est discuté plus en détail dans une section ultérieure avec des exemples de conception présentés sous Compte d'application.
- Utilisez la grande variété d'éléments de sécurité présents dans les multiples services et fonctionnalités AWS pour créer une infrastructure cloud robuste et résiliente. Lorsque vous adaptez l'AWS SRA à vos besoins particuliers, tenez compte non seulement de la fonction principale des services et fonctionnalités AWS (par exemple, authentification, chiffrement, surveillance, politique d'autorisation), mais également de leur intégration dans la structure de votre architecture. Une section ultérieure du guide décrit le fonctionnement de certains services dans l'ensemble de votre organisation AWS. 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 les services AWS qui peuvent être déployés sur chaque compte (distribués plutôt que centralisés) et créez un ensemble cohérent de barrières de sécurité partagées qui peuvent vous aider à protéger vos charges de travail contre toute utilisation abusive et à réduire l'impact des événements de sécurité. L'AWS SRA utilise AWS Security Hub (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 base de services AWS à déployer sur chaque compte AWS.
- Utilisez la fonctionnalité d'administration déléguée d'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 membre AWS 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, afin de gérer les services AWS dans

l'ensemble de l'environnement. En outre, le recours à un administrateur délégué vous permet de limiter l'accès au compte de gestion AWS Organizations et de gérer le surcroît d'autorisations associé à ce compte.

- Mettez en œuvre une surveillance, une gestion et une gouvernance centralisées au sein de vos organisations AWS. En utilisant les services AWS qui prennent en charge l'agrégation multicompte (et parfois multirégionale), ainsi que les fonctionnalités d'administration déléguée, vous permettez à vos équipes d'ingénierie centralisées chargées de la sécurité, du réseau et du cloud de bénéficier d'une visibilité et d'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).
- Utilisez AWS Control Tower pour configurer et gérer votre environnement AWS multi-comptes en mettant en œuvre des contrôles de sécurité prédéfinis pour démarrer le développement de votre architecture de référence en matière de sécurité. AWS Control Tower fournit un plan pour assurer la gestion des identités, un accès fédéré aux comptes, une 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 référencer les comptes gérés par AWS Control Tower avec des contrôles de sécurité, 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 organisations AWS. Vous pouvez également étendre la gouvernance à un compte AWS individuel existant en l'inscrivant dans une unité organisationnelle (UO) déjà régie 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 multi-comptes AWS Organizations avec ou sans AWS Control Tower. Les solutions de ce référentiel qui nécessitent AWS Control Tower ont été déployées et testées dans un environnement AWS Control Tower à l'aide d'AWS CloudFormation et de Customizations for AWS Control Tower (CfCT). Les solutions qui ne nécessitent pas AWS Control Tower ont été testées dans un environnement AWS Organizations à l'aide d'AWS CloudFormation. Si vous n'utilisez pas AWS Control Tower, vous pouvez utiliser la solution de déploiement basée sur AWS Organizations.

Fondements de la sécurité

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

L'architecture de référence de sécurité AWS repose sur trois fondements de sécurité AWS : le cadre d'adoption du cloud AWS (AWS CAF), AWS Well-Architected et le modèle de responsabilité partagée AWS.

AWS Professional Services a créé 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. L'AWS CAF organise les directives 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 l'AWS CAF vous aide à structurer la sélection et la mise en œuvre des contrôles au sein de votre entreprise. Le respect des recommandations actuelles d'AWS dans le 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 framework repose sur six piliers (excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité) et fournit une approche cohérente aux clients et partenaires AWS afin d'évaluer les architectures et de mettre en œuvre des conceptions évolutives dans le temps. Nous pensons que le fait de disposer de charges de travail bien conçues augmente considérablement les chances de réussite de l'entreprise.

- Le pilier de sécurité Well-Architected 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 recommandations actuelles d'AWS. 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 objectifs sont connus sous le nom d'objectifs AWS Well-Architected.

La sécurité et la conformité sont une responsabilité partagée entre AWS et le client. Ce modèle partagé peut vous aider à alléger votre charge opérationnelle car AWS exploite, gère et contrôle 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 de groupe de sécurité fourni par AWS. Pour les services abstraits tels qu'Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB, AWS gère la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer les 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 AWS Identity and Access Management (IAM) pour appliquer les autorisations appropriées. Ce modèle partagé est souvent décrit en disant qu'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 cloud AWS) et que vous êtes responsable de la sécurité dans le cloud (telle que déterminée par les services cloud AWS 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 l'AWS SRA : les capacités de sécurité et les principes de conception de sécurité.

Capacités de sécurité

Le point de vue de la sécurité d'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'environnement AWS de votre organisation.
- 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 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 œuvre 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 ressources AWS. Centralisez la gestion des identités et visez à éliminer le recours à des informations d'identification statiques à long terme.
- Activez la traçabilité : surveillez, générez des alertes et auditez les actions et les modifications apportées à votre environnement en temps réel. Intégrez la collecte de journaux et de métriques aux systèmes pour enquêter et prendre des mesures automatiquement.
- Appliquez 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 de manière plus rentable. 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 par niveaux de sensibilité et utilisez des mécanismes tels que le chiffrement, la tokenisation et le contrôle d'accès, le cas échéant.
- Éloignez les utilisateurs des données : utilisez des mécanismes et des outils pour réduire ou éliminer le besoin d'accéder directement aux données ou de les traiter manuellement. Cela réduit le risque de mauvaise manipulation ou de modification et d'erreur humaine lors de la manipulation de données sensibles.
- Préparez-vous aux événements liés à la sécurité : préparez-vous à un incident grâce à une politique et à des processus de gestion des incidents et d'investigation adaptés aux exigences de votre organisation. Exécutez des simulations de réponse aux incidents et utilisez des outils automatisés pour accélérer la détection, l'investigation et le rétablissement.

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

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

Il est préférable d'utiliser les services de sécurité AWS, leurs contrôles et leurs interactions sur la base de la stratégie multi-comptes AWS et des 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 dans l'AWS SRA.

Un compte AWS fournit des limites de sécurité, d'accès et de facturation pour vos ressources AWS et vous permet de garantir l'indépendance et l'isolation des ressources. L'utilisation de plusieurs comptes AWS joue un rôle important dans la manière dont vous répondez à vos exigences de sécurité, comme indiqué dans la section Avantages de l'utilisation de plusieurs comptes AWS du livre blanc Organiser votre environnement AWS 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 Payment Card Industry Data Security Standard (PCI DSS) ou Health Insurance Portability and Accountability Act (HIPAA). Bien que vous puissiez commencer votre parcours avec AWS avec un seul compte, AWS vous recommande de configurer plusieurs comptes à mesure que la taille et la complexité de vos charges de travail augmentent.

Les autorisations vous permettent de spécifier l'accès aux ressources AWS. Les autorisations sont accordées aux entités IAM appelées entités principales (utilisateurs, groupes et rôles). Par défaut, les principaux démarrent sans aucune autorisation. Les entités IAM ne peuvent rien faire dans AWS

tant que vous ne leur accordez pas d'autorisations, et vous pouvez mettre en place des garde-fous applicables à l'ensemble de votre organisation AWS ou aussi précis qu'une combinaison individuelle de principe, d'action, de ressource et de conditions.

Utilisation d'AWS Organizations à des fins de sécurité

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

AWS Organizations vous aide à gérer et à gouverner de manière centralisée votre environnement à mesure que vous développez et adaptez vos ressources AWS. En utilisant AWS Organizations, vous pouvez créer par programmation de nouveaux 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 organisation AWS consolide vos 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 services AWS spécifiques. Vous pouvez fournir des outils et un accès à partir d'un emplacement central à votre équipe de sécurité afin de gérer les besoins de sécurité pour le compte d'une organisation AWS. Vous pouvez réduire la duplication des ressources en partageant les ressources critiques au sein de votre organisation AWS. Vous pouvez regrouper les comptes dans des unités organisationnelles (UO) AWS, qui peuvent représenter différents environnements en fonction des exigences et de l'objectif de la charge de travail.

Avec AWS Organizations, vous pouvez utiliser des politiques de contrôle des services (SCP) pour appliquer des garanties en matière d'autorisations au niveau de l'organisation, de l'unité d'organisation ou du compte AWS. Ces garanties s'appliquent aux principaux associés au compte d'une organisation, à l'exception du compte de gestion (ce qui est l'une des raisons de ne pas exécuter de charges de travail sur ce compte). Lorsque vous attachez un SCP à une UO, il est hérité par les UO enfants et les comptes associés à l'UO. Les SCP n'accordent aucune autorisation. Les SCP spécifient plutôt les autorisations maximales pour une organisation, une unité d'organisation ou un compte AWS. Vous devez toujours associer des politiques basées sur l'identité ou les ressources aux principaux ou aux ressources de vos 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 des informations détaillées sur la manière dont les politiques IAM sont évaluées, le rôle des SCP et la manière dont l'accès est finalement accordé ou refusé, consultez la logique d'évaluation des politiques dans la documentation IAM.

AWS Control Tower propose un moyen simplifié de configurer et de gérer plusieurs comptes. Il automatise la configuration des comptes dans votre organisation AWS, automatise le provisionnement, applique des garde-fous (notamment 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 entités IAM spécifiques (utilisateurs ou rôles) et définit les autorisations maximales qu'une politique basée sur l'identité peut accorder à une entité IAM.

AWS Organizations vous aide à configurer les services AWS qui s'appliquent à tous vos comptes. Par exemple, vous pouvez configurer la journalisation centralisée de toutes les actions effectuées au sein de votre organisation AWS à l'aide d'AWS CloudTrail, et empêcher les comptes membres de désactiver la journalisation. Vous pouvez également agréger de manière centralisée les données relatives aux règles que vous avez définies à l'aide d'AWS Config, afin de vérifier la conformité de vos charges de travail et de réagir rapidement aux modifications. Vous pouvez utiliser AWS CloudFormation StackSets pour gérer de manière centralisée les CloudFormation stacks AWS entre les comptes et les unités d'organisation de votre organisation AWS, afin de pouvoir configurer automatiquement un nouveau compte répondant à vos exigences de sécurité.

La configuration par défaut d'AWS Organizations prend en charge l'utilisation de SCP 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 lorsqu'AWS ajoute de nouveaux services. Les déclarations de refus sont généralement plus courtes en caractères, il est donc plus facile de respecter la taille maximale des SCP. Dans une instruction où l'élément `Effect` a une valeur de `Deny`, vous pouvez également limiter l'accès à des ressources spécifiques ou définir des conditions pour le moment où les politiques de contrôle des services sont en vigueur. En revanche, une instruction Allow 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 des SCP dans la documentation AWS Organizations.

> **Considérations relatives à la conception**
>
> - Sinon, pour utiliser les SCP 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 entre le compte AWS et 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 services AWS autorisés dont l'utilisation est approuvée au sein d'une organisation AWS et attachez ce SCP à la racine de votre organisation AWS. Si un ensemble de services différent est autorisé par votre environnement de développement, vous devez associer les SCP respectifs 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.

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

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

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

Le compte de gestion déploie des garde-fous de sécurité universels par le biais de SCP et de déploiements de services (tels qu'AWS CloudTrail) qui affecteront tous les comptes membres de l'organisation 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 organisation AWS. Un compte AWS ne peut être membre que d'une seule organisation AWS 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 un accès sécurisé pour permettre à un service AWS que vous spécifiez, appelé service sécurisé, d'effectuer des tâches au sein de votre organisation AWS et de ses comptes en votre nom. Cela implique d'accorder des autorisations au service de confiance, mais cela n'affecte pas les autorisations pour les entités IAM. Vous pouvez utiliser l'accès sécurisé pour spécifier les paramètres et les détails de configuration que vous souhaitez que le service fiable conserve en votre nom dans les comptes de votre organisation AWS. Par exemple, la section relative au compte de gestion de l'organisation de l'AWS SRA explique comment accorder au CloudTrail service AWS un accès sécurisé afin de créer un suivi de CloudTrail l'organisation dans tous les comptes de votre organisation AWS.

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 membre AWS dans l'organisation AWS en tant qu'administrateur des comptes de l'organisation AWS dans ce service. Cette fonctionnalité permet aux différentes équipes de votre entreprise d'utiliser des comptes distincts, en fonction de leurs responsabilités, afin de gérer les services AWS dans l'ensemble de l'environnement. Les services de sécurité AWS de l'AWS SRA qui prennent actuellement en charge l'administrateur délégué incluent AWS IAM Identity Center (successeur d'AWS Single Sign-On), AWS Config, AWS Firewall Manager GuardDuty, Amazon, AWS IAM Access Analyzer, Amazon Macie, AWS Security Hub, Amazon Detective, AWS Audit Manager, Amazon Inspector et AWS Systems Manager. L'utilisation de la fonctionnalité d'administrateur délégué est soulignée dans l'AWS SRA en tant que bonne 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 (AWSSRA) en répondant à une courte enquête.

Un compte AWS fournit des limites de sécurité, d'accès et de facturation pour vos ressources AWS, 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 d'unités d'organisation de base pour ces fonctions spécifiques, réparties en unités d'organisation d'infrastructure et en unités d'organisation de sécurité. Ces recommandations relatives aux unités d'organisation et aux comptes constituent un sous-ensemble de nos directives plus générales et plus complètes relatives aux organisations AWS et à la conception de structures multicomptes. Pour un ensemble complet de recommandations, consultez Organizing Your AWS Environment Using Multiple Accounts dans la documentation AWS et dans le billet de blog Best Practices for Organizational Units with AWS Organizations.

L'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 toutes les régions et de tous les comptes AWS. Le compte AWS qui héberge la racine de l'organisation AWS.
Outillage de sécurité	Sécurité	Des comptes AWS dédiés permettent de gérer des services de sécurité applicables à tous (tels qu'Amazon

		GuardDuty, AWS Security Hub, AWS Audit Manager, Amazon Detective, Amazon Inspector et AWS Config), de surveiller les comptes AWS et d'automatiser les alertes de sécurité et les réponses. (Dans AWS Control Tower, le nom par défaut du compte dans l'unité d'organisation de sécurité est Audit account.)
Archive du journal	Sécurité	Comptes AWS dédiés pour l'ingestion et l'archivage de tous les journaux et sauvegardes pour toutes les régions AWS et tous les 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 infrastructures 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	Des comptes AWS qui hébergent les applications de l'organisation AWS 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 résiliente face aux changements organisat ionnels.

Organisation AWS et structure de compte de l'AWS SRA

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

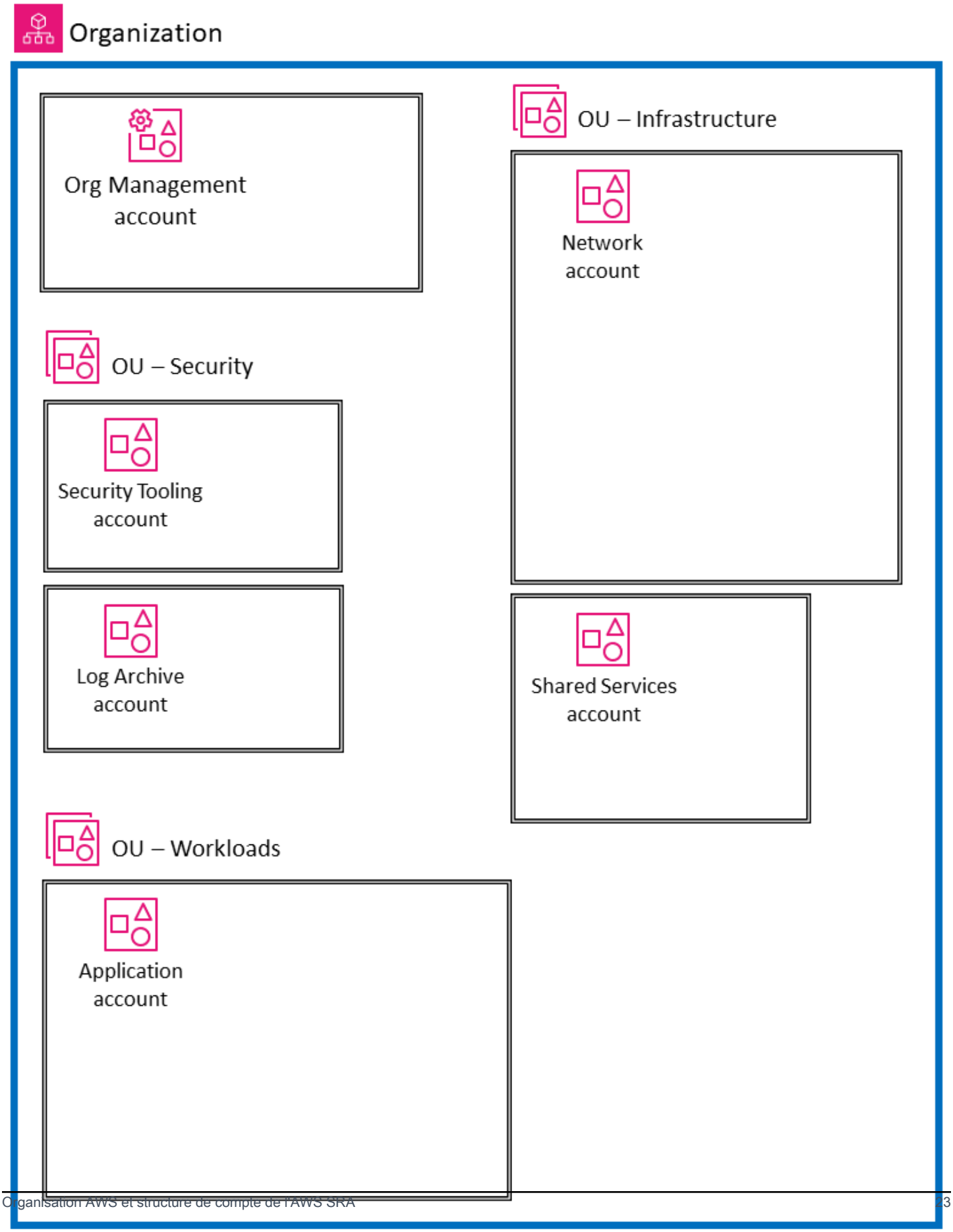
Le schéma suivant illustre la structure de haut niveau de l'AWS SRA sans afficher de services spécifiques. Il reflète la structure de comptes dédiés décrite dans la section précédente, et

nous incluons le schéma ici pour orienter la discussion autour des principaux composants de l'architecture :

- Tous les comptes présentés dans le schéma font partie d'une seule organisation AWS.
- En haut à gauche du diagramme se trouve le compte Org Management, qui est utilisé pour créer l'organisation AWS.
- 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.

Pour ce guide, tous les comptes sont considérés comme des comptes de production (prod) qui fonctionnent dans une seule région AWS. La plupart des services AWS (à l'exception des services internationaux) ont une portée régionale, ce qui signifie que les plans de contrôle et de données du service existent indépendamment dans chaque région AWS. Pour cette raison, vous devez répliquer cette architecture dans toutes les régions AWS que vous prévoyez d'utiliser, afin de garantir la couverture de l'ensemble de votre environnement AWS. Si vous n'avez aucune charge de travail dans une région AWS spécifique, vous devez désactiver la région en utilisant des SCP ou en utilisant des mécanismes de journalisation et de surveillance. Vous pouvez utiliser AWS Security Hub pour agréger les résultats et les scores de sécurité de plusieurs régions AWS dans une seule région d'agrégation afin d'obtenir une visibilité centralisée.

Lorsque vous hébergez une organisation AWS avec 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 multi-comptes AWS. Les exemples de code AWS SRA contenus dans le GitHubréférentiel montrent comment utiliser la solution Customizations for AWS Control Tower (CfCT) pour déployer les structures recommandées par AWS SRA.

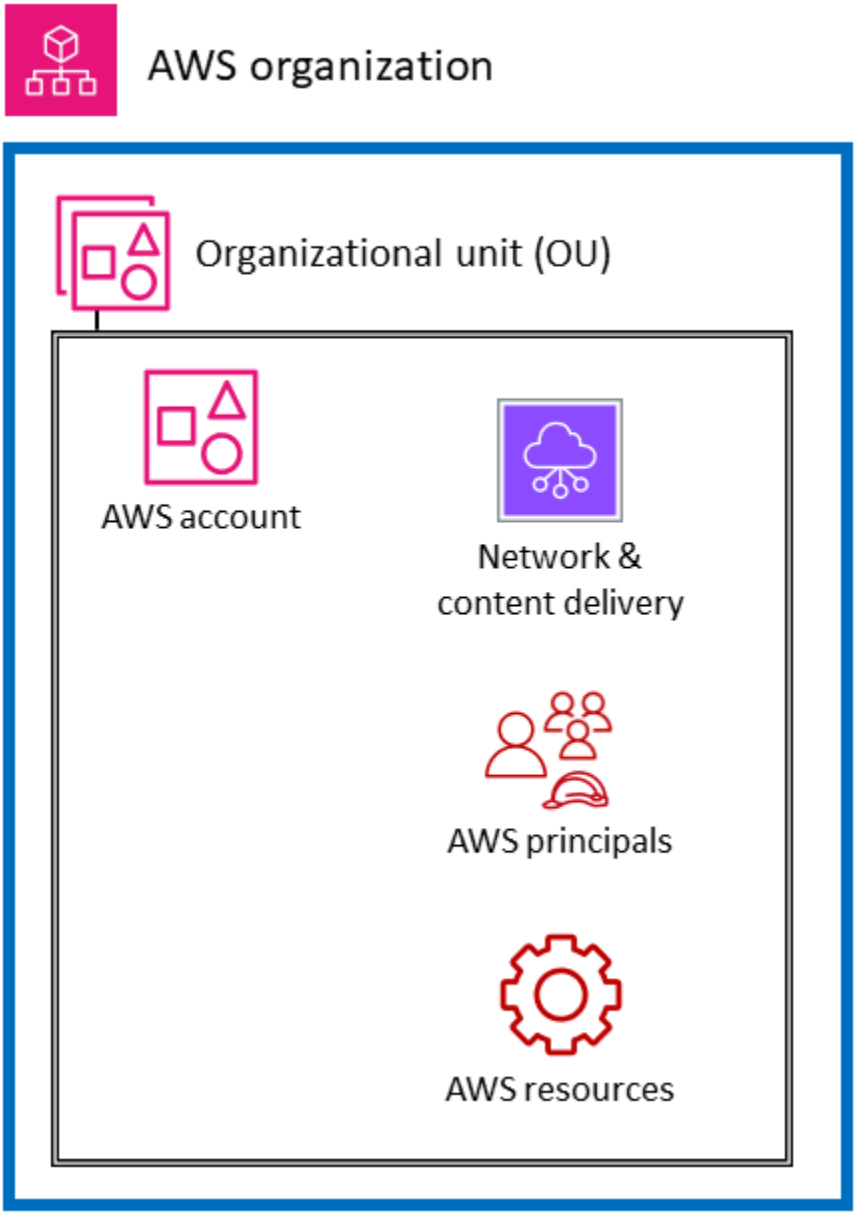

Organization
Org Management account
OU – Infrastructure
Network account
OU – Security
Security Tooling account
Log Archive account
Shared Services account
OU – Workloads
Application account

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

Influencez le futur de l'architecture de référence de AWS sécurité (AWSSRA) 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 sécurité AWS 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 l'AWS CAF répertorie neuf fonctionnalités, notamment la gestion des identités et des accès, la protection de l'infrastructure, la protection des données et la détection des menaces. Associer les services AWS à ces fonctionnalités est un moyen pratique de prendre des décisions de mise en œuvre dans chaque domaine. Par exemple, en matière de gestion des identités et des accès, IAM et IAM Identity Center sont des services à prendre en compte. Lors de l'élaboration de votre approche de détection des menaces, Amazon GuardDuty 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 : « Quels 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 : « Quels services AWS dois-je appliquer à l'ensemble de mon organisation AWS ? 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 mappez les services et fonctionnalités AWS aux couches de votre environnement AWS. Certains services et fonctionnalités conviennent parfaitement à la mise en œuvre de contrôles dans l'ensemble de votre organisation AWS. 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 d'autres services et fonctionnalités pour protéger les ressources individuelles 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 infrastructure AWS. Le schéma suivant montre six couches dans un environnement AWS typique : organisation AWS, unité organisationnelle (UO), compte, infrastructure réseau, principes et ressources.



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

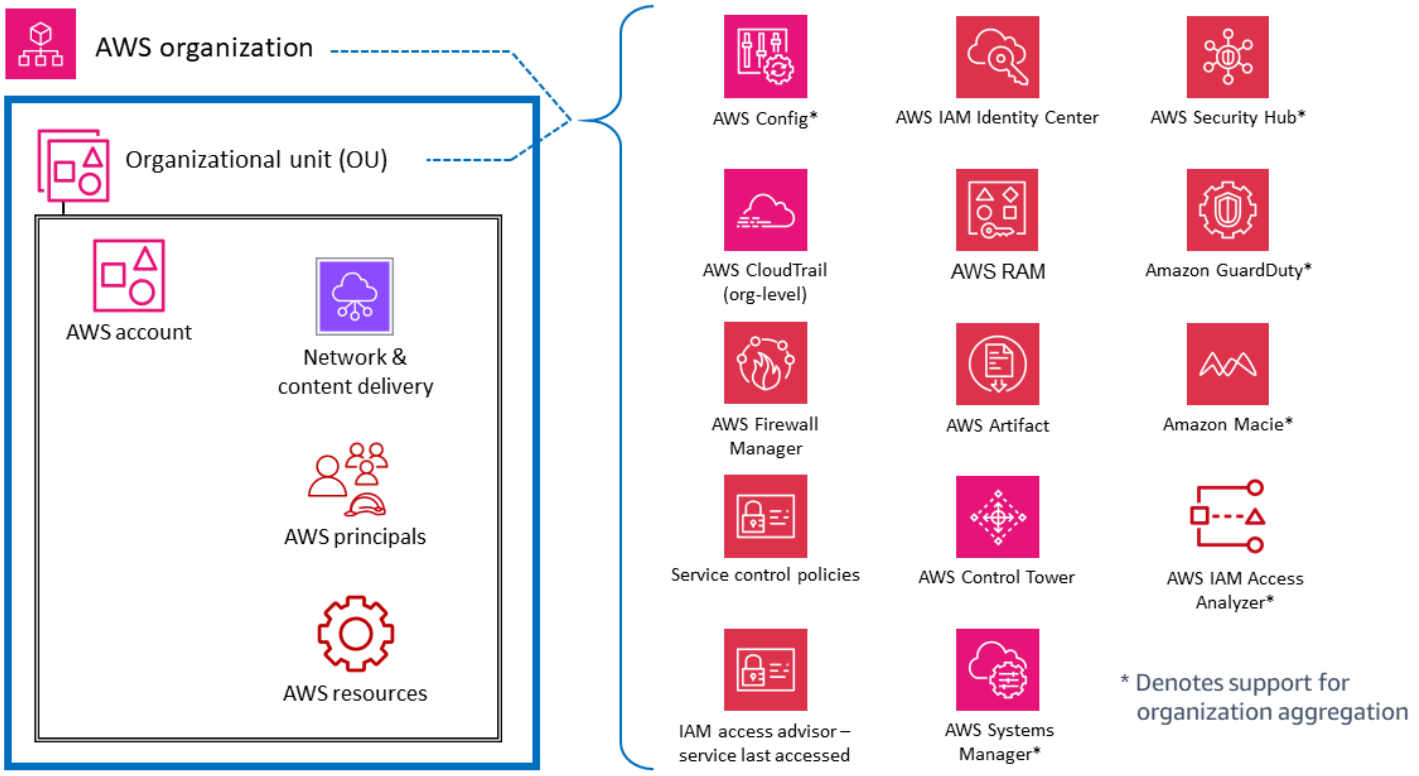
fonctionnalités et répondent à de multiples objectifs de sécurité. Ces services peuvent prendre en charge plusieurs éléments de votre environnement AWS.

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 différents services de chaque compte AWS.

Comptes multiples ou à l'échelle de l'organisation

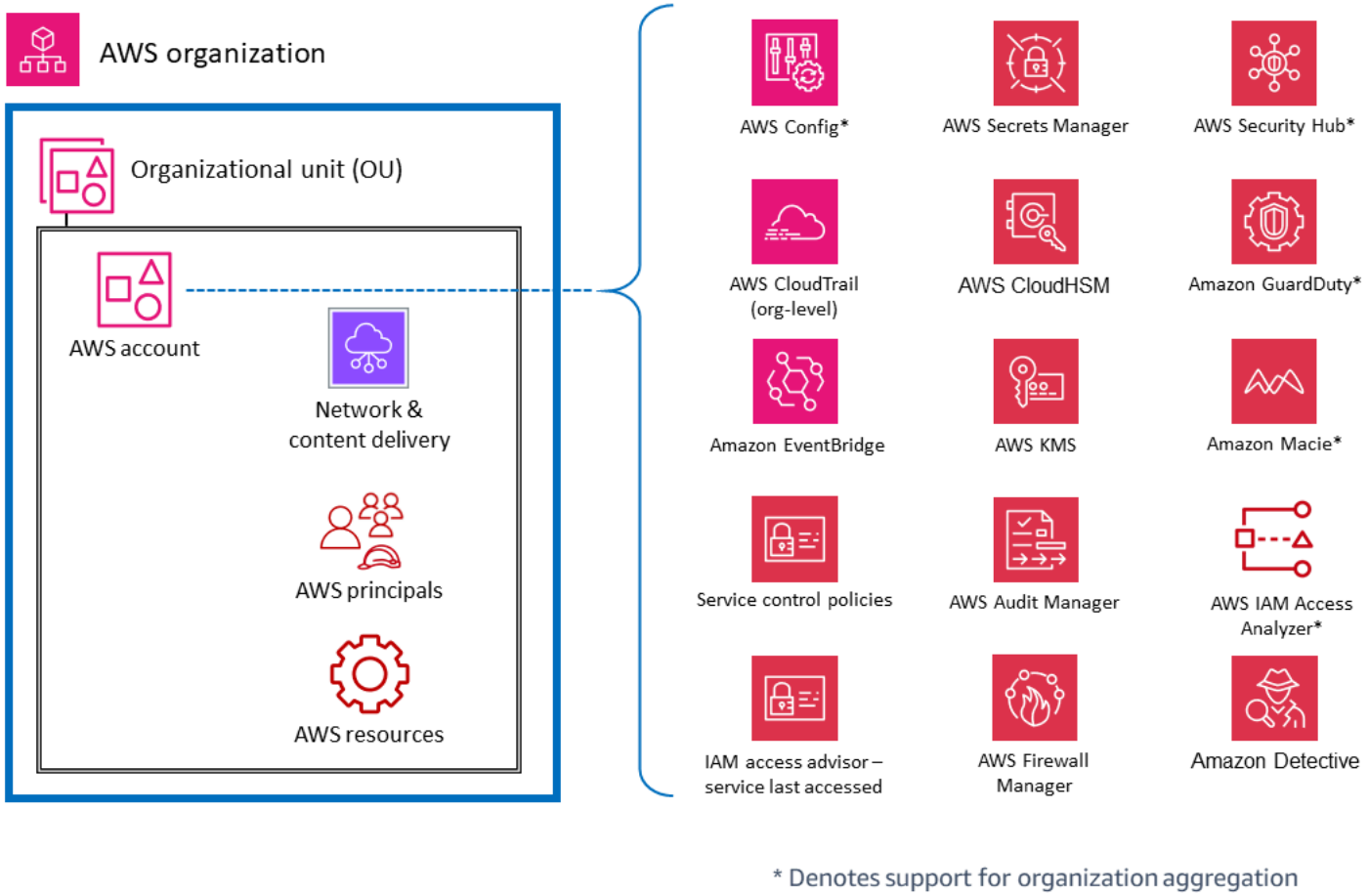
Au niveau supérieur, certains services et fonctionnalités AWS sont conçus pour appliquer des fonctionnalités ou des garde-fous de gouvernance et de contrôle à plusieurs comptes d'une organisation AWS (y compris l'ensemble de l'organisation ou des unités d'organisation spécifiques). Les politiques de contrôle des services (SCP) sont un bon exemple de fonctionnalité IAM qui fournit un garde-fou préventif à l'échelle de l'organisation AWS. Un autre exemple est AWS CloudTrail, qui fournit une surveillance par le biais d'un journal d'organisation qui enregistre tous les événements pour tous les comptes AWS de cette organisation AWS. Ce parcours complet est distinct des parcours individuels qui peuvent être créés dans chaque compte. Le troisième exemple est AWS Firewall Manager, que vous pouvez utiliser pour configurer, appliquer et gérer plusieurs ressources sur tous les comptes de votre organisation AWS : règles AWS WAF, règles AWS WAF Classic, protections AWS Shield Advanced, groupes de sécurité Amazon Virtual Private Cloud (Amazon VPC), politiques AWS Network Firewall et Amazon Route 53 Resolver Politiques de pare-feu 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 les SCP qui s'appliquent à l'ensemble d'une unité d'organisation, d'un compte AWS ou d'une organisation AWS. En revanche, vous pouvez configurer et gérer Amazon à la GuardDuty fois au niveau du compte (où les résultats individuels sont générés) et au niveau de l'organisation AWS (à l'aide de la fonctionnalité d'administrateur délégué), où les résultats peuvent être consultés et gérés de manière globale.



Comptes AWS

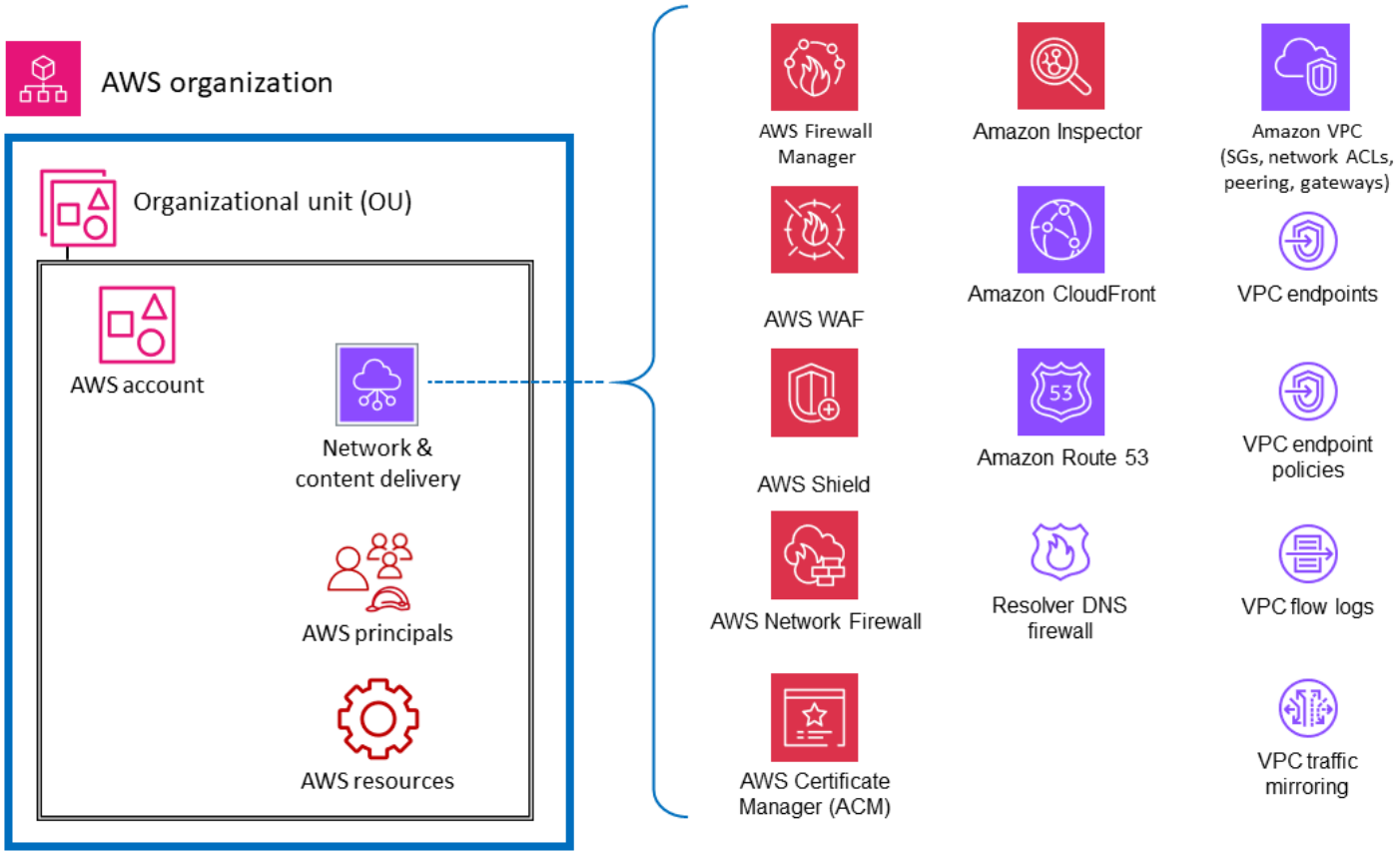
Au sein des unités d'organisation, il existe des services qui aident à protéger plusieurs types d'éléments au sein d'un compte AWS. Par exemple, AWS Secrets Manager est généralement géré à partir d'un compte spécifique et protège les ressources (telles que les informations d'identification de base de données ou d'authentification), les applications et les services AWS de ce compte. AWS IAM Access Analyzer peut être configuré pour générer des résultats lorsque des ressources spécifiées sont accessibles par des personnes extérieures au compte AWS. Comme indiqué dans la section précédente, bon nombre de ces services peuvent également être configurés et administrés au sein d'AWS Organizations, afin de pouvoir 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. Amazon GuardDuty est un exemple de ce type de service. GuardDutysurveille 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 organisation AWS) 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 charges de travail AWS, de nombreux services et fonctionnalités de sécurité AWS sont dédiés à ces ressources. Par exemple, Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos charges de travail AWS 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 Virtual Private Cloud (Amazon VPC) vous permet de définir un réseau virtuel dans lequel vous pouvez lancer des ressources AWS. 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 AWS pris en charge et aux services de point de terminaison optimisés par PrivateLink AWS 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

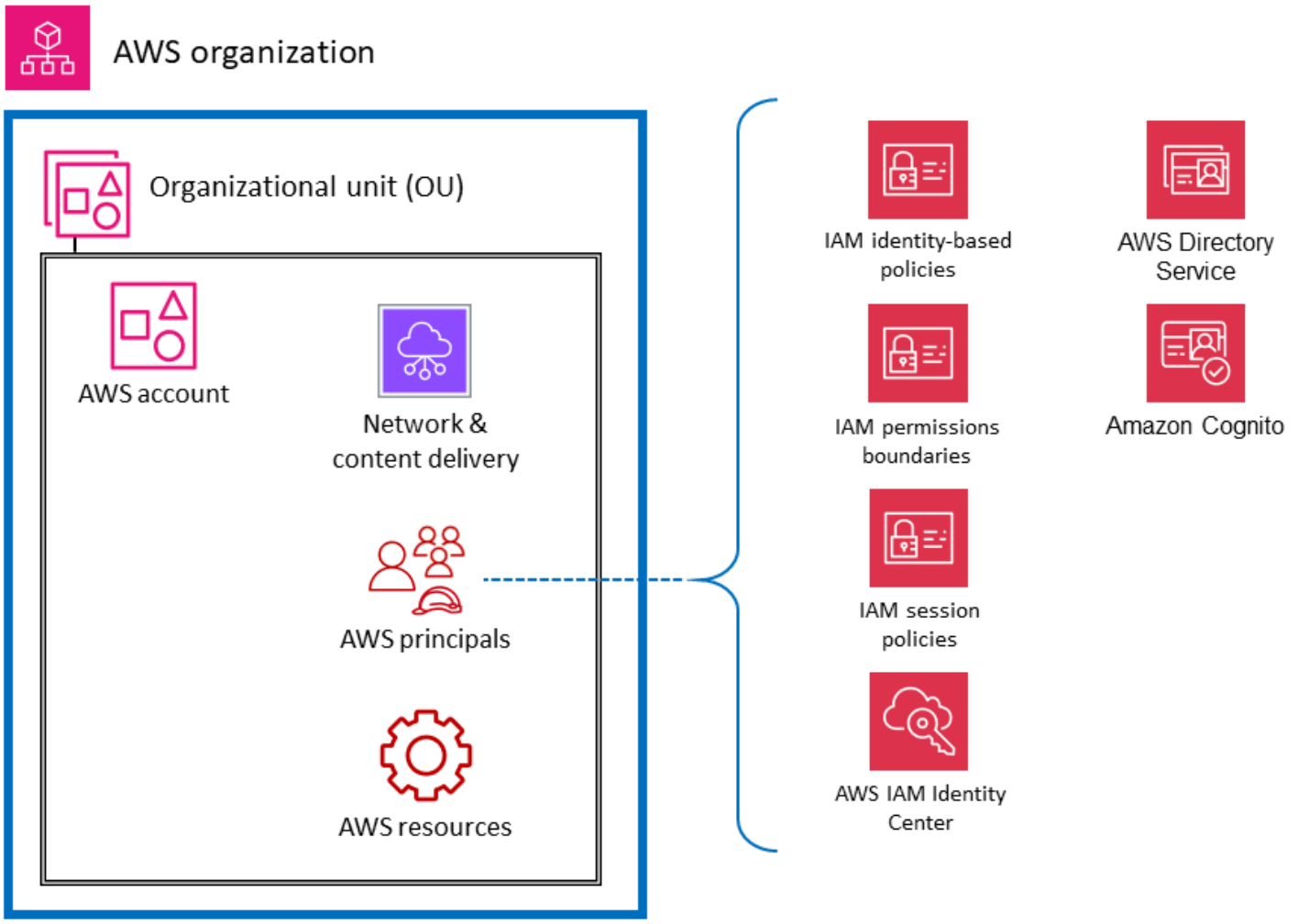
Les principes et les ressources AWS (ainsi que les politiques IAM) sont les éléments fondamentaux de la gestion des identités et des accès sur AWS. Un mandant authentifié dans AWS peut effectuer des actions et accéder aux ressources AWS. Un principal peut être authentifié en tant qu'utilisateur root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

> **Note**
>
> Ne créez pas de clés d'API persistantes associées à l'utilisateur root AWS. L'accès à l'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 visant à protéger l'utilisateur root de votre compte, consultez la documentation AWS.

Une ressource AWS est un objet existant au sein d'un service AWS avec lequel vous pouvez travailler. Les exemples incluent une instance EC2, une CloudFormation pile AWS, 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 une identité IAM (utilisateur, groupe ou rôle) ou à une ressource AWS. 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.

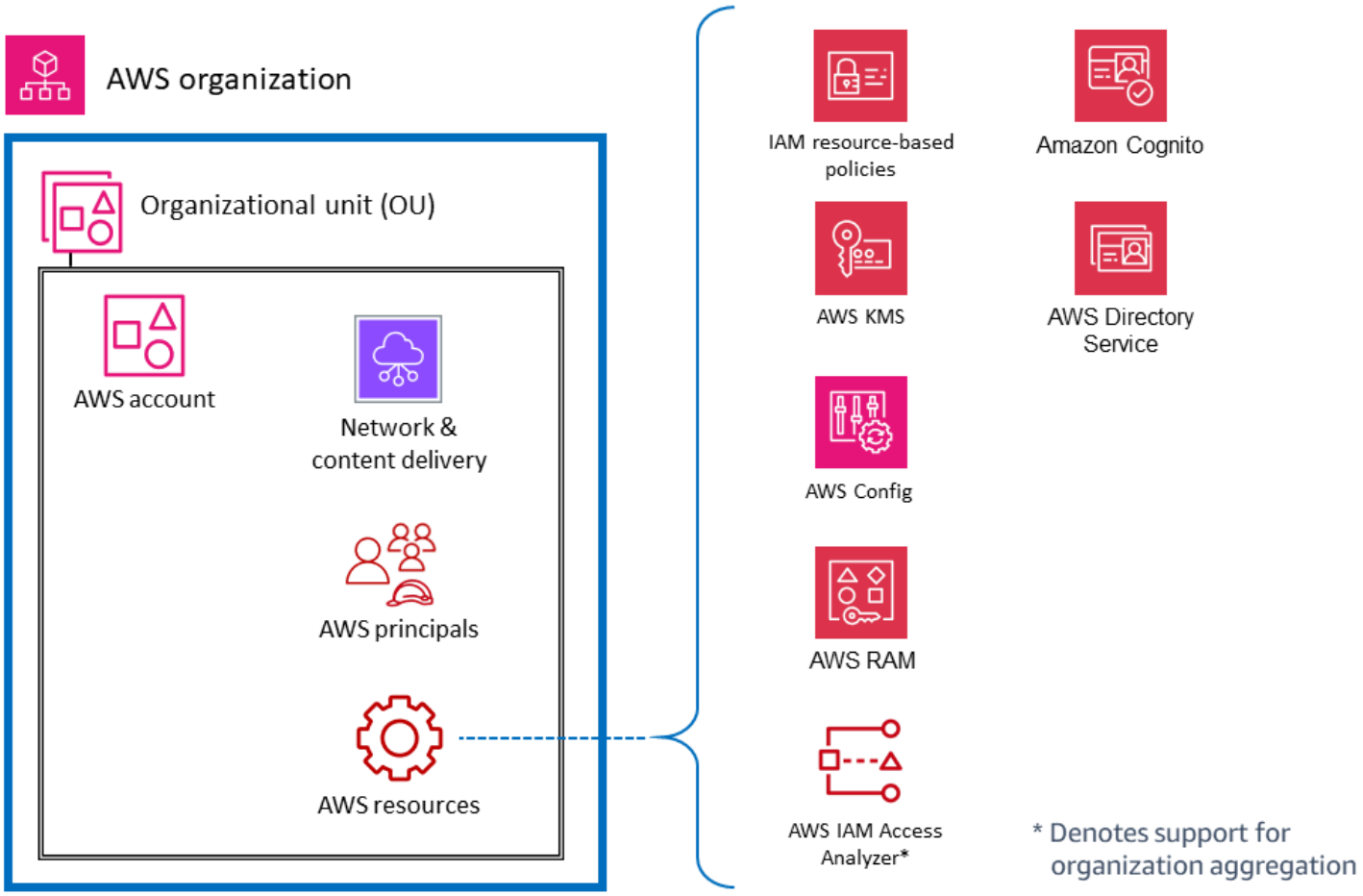
Pour simplifier les choses dans cette discussion, nous listons les services et fonctionnalités de sécurité AWS pour les entités IAM dont l'objectif principal est d'opérer sur les principaux comptes ou de s'appliquer à ceux-ci. Nous conservons cette simplicité tout en reconnaissant la flexibilité et l'étendue des effets des politiques d'autorisation IAM. Une seule déclaration dans une politique peut avoir des effets sur plusieurs types d'entités AWS. Par exemple, bien qu'une politique basée sur l'identité IAM soit associée à une entité IAM et définisse les autorisations (autoriser, refuser) pour cette entité, la politique définit également implicitement les 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 sécurité AWS pour les principaux utilisateurs d'AWS. Les politiques basées sur l'identité sont associées aux objets de ressources IAM utilisés pour l'identification et le regroupement, tels que les utilisateurs, les groupes et les rôles. 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 sont fédérées dans 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 AWS Organizations et aux API AWS, et vous aide à gérer l'accès SSO et les autorisations utilisateur sur vos comptes AWS dans 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 relatives aux compartiments S3, les politiques clés d'AWS KMS et les politiques relatives aux points de terminaison VPC sont des types de politiques basées sur les ressources. AWS 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 imprévus à vos ressources et données, ce qui constitue un risque de sécurité. AWS Config vous permet d'évaluer, d'auditer et d'évaluer les configurations des ressources AWS prises en charge dans vos comptes AWS. AWS Config surveille et enregistre en permanence les configurations

des ressources AWS, et évalue automatiquement les configurations enregistrées par rapport aux configurations souhaitées.



Architecture de référence de sécurité AWS

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

Le schéma suivant illustre l'AWS SRA. Ce schéma architectural regroupe tous les services liés à la sécurité AWS. 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.

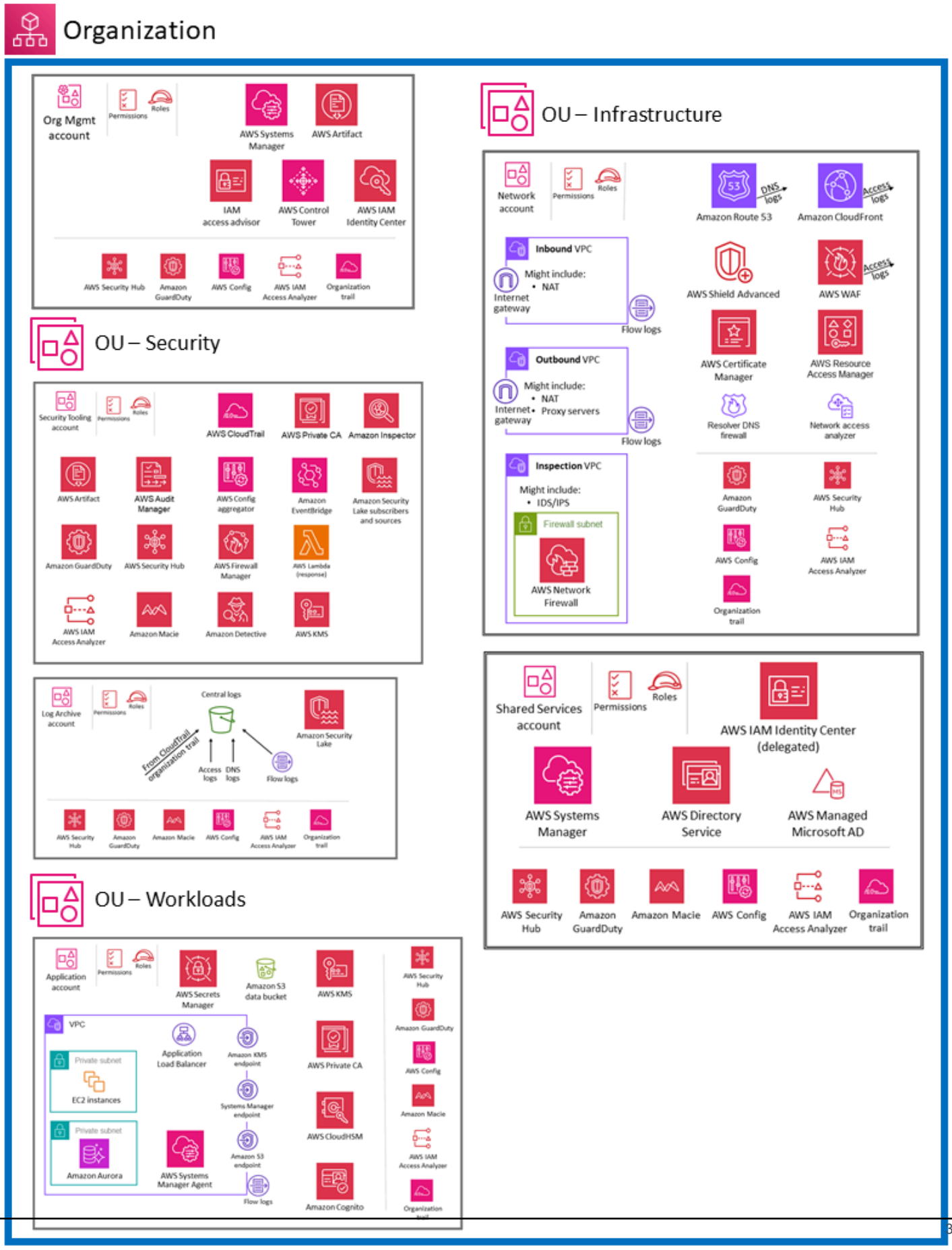
Remarques

Pour des raisons de simplicité, le schéma suivant montre l'architecture à un niveau intentionnellement élevé et masque les détails de chaque compte. Pour visualiser les diagrammes des comptes individuels de manière plus détaillée, consultez les sections distinctes relatives aux UO et aux comptes.

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
Org Mgmt account
Permissions
Roles
AWS Systems Manager
AWS Artifact
IAM access advisor
AWS Control Tower
AWS IAM Identity Center
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS IAM Access Analyzer
Organization trail
OU – Security
Security Tooling account
AWS CloudTrail
AWS Private CA
Amazon Inspector
AWS Artifact
AWS Audit Manager
AWS Config aggregator
Amazon EventBridge
Amazon Security Lake subscribers and sources
Amazon GuardDuty
AWS Security Hub
AWS Firewall Manager
AWS Lambda (response)
AWS IAM Access Analyzer
Amazon Macie
Amazon Detective
AWS KMS
Log Archive account
Central logs
From CloudTrail organization trail
Access logs
DNS logs
Flow logs
Amazon Security Lake
OU – Workloads
Application account
AWS Secrets Manager
Amazon S3 data bucket
AWS KMS
VPC
Application Load Balancer
Amazon KMS endpoint
Private subnet
EC2 instances
Systems Manager endpoint
Private subnet
Amazon Aurora
AWS Systems Manager Agent
Amazon S3 endpoint
Flow logs
AWS Private CA
AWS CloudHSM
Amazon Cognito
OU – Infrastructure
Network account
Amazon Route 53
DNS logs
Amazon CloudFront
Access logs
Inbound VPC
Might include:
• NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS WAF
Outbound VPC
Might include:
• NAT
• Proxy servers
Internet gateway
Flow logs
AWS Certificate Manager
AWS Resource Access Manager
Resolver DNS firewall
Network access analyzer
Inspection VPC
Might include:
• IDS/IPS
Firewall subnet
AWS Network Firewall
Amazon GuardDuty
AWS Security Hub
AWS Config
AWS IAM Access Analyzer
Organization trail
Shared Services account
Permissions
Roles
AWS IAM Identity Center (delegated)
AWS Systems Manager
AWS Directory Service
AWS Managed Microsoft AD
AWS Security Hub
Amazon GuardDuty
Amazon Macie
AWS Config
AWS IAM Access Analyzer
Organization trail

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'instances Amazon Elastic Compute Cloud (Amazon EC2) 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.

L'AWS SRA contient tous les services liés à la sécurité AWS disponibles au moment de la 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 de sécurité AWS 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 l'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.

UO et comptes

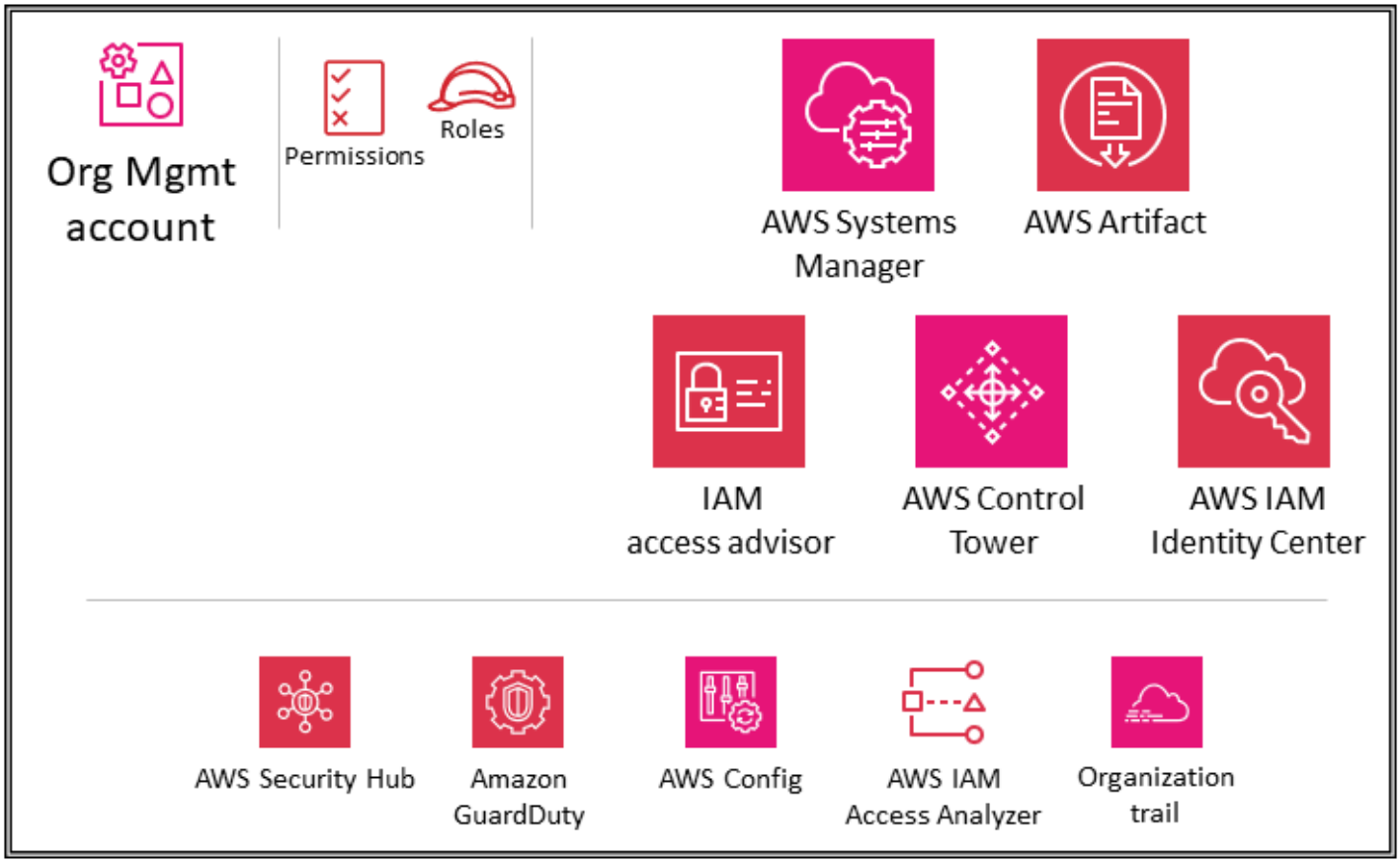
- Compte de gestion de l'organisation
- Security OU — Compte Security Tooling

- 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 (AWSSRA) en répondant à une courte enquête.

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



Les sections Utiliser AWS Organizations pour la sécurité et Le compte de gestion, l'accès sécurisé et les administrateurs délégués plus haut dans ce guide ont décrit en détail le but et les objectifs de sécurité du compte Org Management. 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 AWS aurait besoin de 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 de manière centralisée les politiques de plusieurs comptes AWS. Par exemple, vous pouvez appliquer des politiques de contrôle des services (SCP) à plusieurs comptes AWS membres d'une organisation. Les SCP vous permettent de définir les API de service AWS qui peuvent ou ne peuvent pas être exécutées par les entités AWS Identity and Access Management (IAM) (telles que les utilisateurs et les rôles IAM) dans les comptes AWS membres de votre organisation. Les SCP sont créés et appliqués à partir du compte de gestion de l'organisation, qui est le compte AWS que vous avez utilisé lors de la création de votre organisation. Pour en savoir plus sur les SCP, consultez la section Utiliser AWS Organizations pour la sécurité plus haut dans cette référence.

Si vous utilisez AWS Control Tower pour gérer votre organisation AWS, celle-ci déploiera un ensemble de SCP à titre de 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. Ces SCP utilisent automatiquement une aws-control-tower balise dont la valeur est de managed-by-control-tower.

Considération de conception

- Les SCP concernent uniquement les comptes des membres de l'organisation AWS. 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 du SCP et pour consulter des exemples de structures recommandées, consultez le billet de blog AWS How to Use Service Control Policies in AWS Organizations.

IAM Identity Center

AWS IAM Identity Center (successeur d'AWS Single Sign-On) est un service de fédération d'identité qui vous aide à gérer de manière centralisée l'accès SSO à tous vos comptes AWS, à vos principaux et à vos charges de travail dans le 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 gérés par AWS en tant que fournisseur d'identité grâce à l'utilisation d'AWS Directory Service. IAM Identity Center inclut un portail utilisateur sur lequel vos utilisateurs finaux peuvent trouver et accéder aux comptes AWS, aux rôles, aux applications cloud et aux applications personnalisées qui leur sont attribués en un seul endroit.

IAM Identity Center s'intègre nativement à AWS Organizations et s'exécute par défaut dans le compte Org Management. 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 l'AWS SRA, le compte Shared Services est le compte d'administrateur délégué pour 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 comptes AWS, d'appliquer des ensembles d'autorisations courants et de gérer l'accès depuis 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.

- IAM Identity Center Identity Store : 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 AWS Directory Service pour 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 les 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 de 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 Access 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 vos comptes AWS et vos unités d'organisation. Utilisez ce contrôle de détective pour contribuer à la stratégie du moindre privilège. Pour les entités IAM, vous pouvez consulter deux types d'informations auxquelles vous avez accédé pour la dernière fois : les informations de service AWS autorisées et les informations d'action 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 organisation AWS. Ces informations sont disponibles dans la console IAM du compte de gestion et peuvent également être obtenues par programmation en utilisant les API du conseiller d'accès IAM dans l'AWS Command Line Interface (AWS CLI) ou un client de programmation. 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

Quick Setup et Explorer, qui sont des fonctionnalités d'AWS Systems Manager, sont tous deux compatibles avec 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 organisation AWS. Vous pouvez activer la configuration rapide dans l'ensemble de votre organisation AWS ou choisir des unités d'organisation spécifiques. Quick Setup peut programmer l'agent AWS Systems Manager (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 ressources AWS. Explorer affiche une vue agrégée des données d'exploitation pour vos comptes AWS et pour l'ensemble des régions AWS. Cela inclut les données relatives à vos instances EC2 et les détails de conformité des correctifs. Après avoir terminé la configuration intégrée (qui inclut également Systems Manager OpsCenter) dans AWS Organizations, vous pouvez agréger les données dans Explorer par unité d'organisation ou pour l'ensemble d'une organisation AWS. 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 Systems Manager (agent SSM) sur les instances EC2 du compte d'application.

AWS Control Tower

AWS Control Tower fournit un moyen simple de configurer et de gérer un environnement AWS multi-comptes sécurisé, appelé zone de landing zone. AWS Control Tower crée votre zone de landing

zone à l'aide d'AWS Organizations et fournit une gestion et une gouvernance continues des comptes ainsi que les meilleures pratiques de mise en œuvre. Vous pouvez utiliser AWS Control Tower pour configurer de nouveaux comptes en quelques étapes, tout en vous assurant qu'ils sont conformes aux politiques de votre organisation. Vous pouvez même ajouter des comptes existants à un nouvel environnement AWS Control Tower.

AWS Control Tower propose 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 IAM Identity Center, afin de créer une zone de landing zone. Par exemple, AWS Control Tower utilise par défaut AWS CloudFormation pour établir une base de référence, les politiques de contrôle des services (SCP) d'AWS Organizations pour empêcher les modifications de configuration et les règles AWS Config pour détecter en permanence les non-conformités. AWS Control Tower utilise des plans qui vous aident à aligner rapidement votre environnement AWS multi-comptes sur les principes de conception de base de sécurité d'AWS Well Architected. Parmi les fonctionnalités de gouvernance, 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 met en place une organisation AWS 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 l'AWS SRA, AWS Control Tower fait partie du compte Org Management, car AWS Control Tower utilise ce compte pour configurer automatiquement une organisation AWS et désigne ce compte comme compte de gestion. Ce compte est utilisé pour la facturation au sein de votre organisation AWS. Il est également utilisé pour le provisionnement des comptes par Account Factory, pour gérer les unités d'organisation et pour gérer les garde-fous. Si vous lancez AWS Control Tower dans une organisation AWS existante, vous pouvez utiliser le compte de gestion existant. AWS Control Tower utilisera ce compte comme compte de gestion désigné.

Considération de conception

- Si vous souhaitez établir une base de référence supplémentaire pour les contrôles et les configurations de vos comptes, vous pouvez utiliser Customizations for AWS Control Tower (CfCT). Avec CfCT, vous pouvez personnaliser la zone d'atterrissage de votre AWS

Control Tower à l'aide d'un CloudFormation modèle AWS et de politiques de contrôle des services (SCP). Vous pouvez déployer le modèle et les politiques personnalisés sur des comptes et des unités d'organisation individuels au sein de votre organisation. CfCT s'intègre aux événements du cycle de vie d'AWS Control Tower pour garantir que les déploiements de ressources restent synchronisés avec votre zone de landing zone.

AWS Artifact

AWS Artifact fournit un accès à la demande aux rapports de sécurité et de conformité d'AWS et à certains accords en ligne. Les rapports disponibles dans 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 sécurité AWS. AWS Artifact vous aide à effectuer votre due diligence à l'égard d'AWS en améliorant la transparence de notre environnement de contrôle de sécurité. Il vous permet également de surveiller en permanence la sécurité et la conformité d'AWS avec un accès immédiat aux nouveaux rapports.

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

Vous pouvez fournir les artefacts d'audit AWS à vos auditeurs ou régulateurs comme preuve des contrôles de sécurité d'AWS. Vous pouvez également utiliser les conseils de responsabilité fournis par certains artefacts d'audit AWS 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 Artifacts 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 de conception

- Les utilisateurs du compte Org Management doivent être limités à l'utilisation de la fonctionnalité Contrats d'AWS Artifact et à rien d'autre. Pour mettre en œuvre la séparation des tâches, AWS Artifact 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 documentation AWS.

Garde-corps de service de sécurité distribués et centralisés

Dans l'AWS SRA, AWS Security Hub, Amazon, AWS Config GuardDuty, IAM Access Analyzer, AWS CloudTrail organization trails et souvent Amazon Macie sont déployés avec une administration déléguée ou une agrégation appropriée sur le compte Security Tooling. Cela permet un ensemble cohérent de garde-fous entre les comptes et fournit 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 l'AWS SRA. Ils doivent faire partie des services AWS qui doivent être fournis dans le cadre du processus d'intégration et de définition des bases de référence de votre compte. Le référentiel de GitHub code fournit un exemple d'implémentation des services AWS axés sur la sécurité sur vos comptes, y compris le compte AWS Org Management.

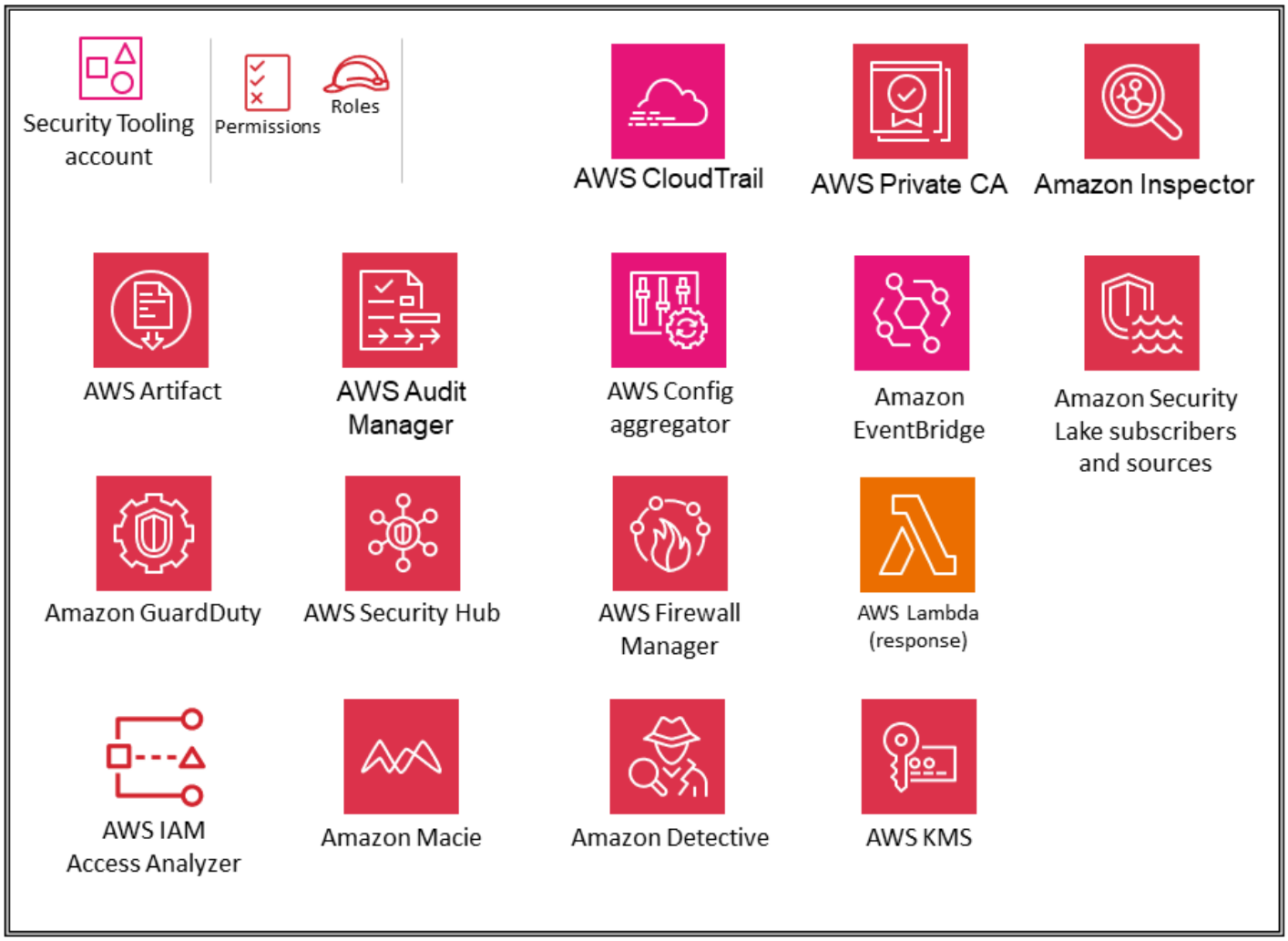
Outre ces services, AWS SRA inclut deux services axés sur la sécurité, Amazon Detective et AWS Audit Manager, qui prennent en charge l'intégration et les fonctionnalités d'administration déléguée dans AWS Organizations. Toutefois, ils ne sont pas inclus dans les services recommandés pour l'établissement 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. Amazon Detective est mieux utilisé par les équipes d'analystes de sécurité, et AWS 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 au début de votre projet, puis vous appuyer sur ceux-ci en utilisant des services offrant des fonctionnalités supplémentaires.

Security OU — Compte Security Tooling

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

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



Le compte Security Tooling est dédié à l'exploitation des services de sécurité, à la surveillance des 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 ou en audit permettant de consulter les informations à l'échelle de l'organisation AWS sont typiques, tandis que les rôles d'écriture/modification sont limités en nombre, étroitement contrôlés, surveillés et consignés.

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 configuration d'AWS Control Tower.
- 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 utilisez AWS Control Tower, cela limite la création de comptes AWS supplémentaires dans le 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 structure administrateur/membre sur l'ensemble des comptes AWS. Comme indiqué précédemment, cela est géré par le biais de la fonctionnalité d'administrateur délégué d'AWS Organizations. Les services de l'AWS SRA qui prennent actuellement en charge l'administrateur délégué incluent AWS Config, AWS Firewall Manager, Amazon GuardDuty, AWS IAM Access Analyzer, Amazon Macie, AWS Security Hub, Amazon Detective, AWS Audit Manager, Amazon Inspector, AWS et AWS CloudTrail 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.

IAM Identity Center prend en charge l'administration déléguée à 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.

AWS CloudTrail

AWS CloudTrail est un service qui prend en charge la gouvernance, la conformité et l'audit de l'activité de votre compte AWS. Vous pouvez ainsi enregistrer, surveiller en permanence et conserver l'activité du compte liée aux actions menées au sein de votre infrastructure AWS. CloudTrail CloudTrail est intégré à AWS Organizations, et cette intégration peut être utilisée pour créer un journal unique qui enregistre tous les événements pour tous les comptes de l'organisation AWS. 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 journal portant le nom que vous spécifiez est créé dans chaque compte AWS appartenant à votre organisation AWS. Le journal enregistre l'activité de tous les comptes, y compris le compte de gestion, de l'organisation AWS 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'organisation AWS peuvent voir le parcours de l'organisation dans leur liste de sentiers. Toutefois, les comptes AWS des membres ont un accès en lecture seule à ce parcours. Par défaut, lorsque vous créez un parcours d'organisation dans la CloudTrail console, il s'agit d'un parcours multirégional. Pour en savoir plus sur les meilleures pratiques en matière de sécurité, consultez la CloudTrail documentation AWS.

Dans l'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'une organisation, consultez la CloudTrail documentation AWS.

> **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.

Considération de conception

- 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 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

AWS Security Hub vous fournit une vue complète de votre niveau de sécurité dans AWS et vous aide à vérifier que votre environnement est conforme aux normes du secteur de la sécurité et aux meilleures pratiques. Security Hub collecte des données de sécurité provenant des services intégrés AWS, des produits tiers pris en charge et d'autres produits de sécurité personnalisés que vous pouvez utiliser. Il vous permet de surveiller et d'analyser en permanence les tendances en matière de sécurité et d'identifier les problèmes de sécurité les plus prioritaires. Outre les sources ingérées, Security Hub génère ses propres résultats, représentés par des contrôles de sécurité correspondant à une ou plusieurs normes de sécurité. Ces normes incluent les meilleures pratiques de sécurité fondamentales d'AWS (FSBP), les tests de référence AWS v1.20 et v1.4.0 du Center for Internet Security (CIS), 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 Security Hub dans la documentation de Security Hub.

Security Hub s'intègre à AWS Organizations pour simplifier la gestion du niveau de sécurité sur tous les comptes existants et futurs de votre organisation AWS. Security Hub est automatiquement activé sur le compte administrateur délégué de Security Hub (dans ce cas, Security Tooling) et peut choisir les comptes AWS à activer en tant que comptes membres. Le compte d'administrateur délégué 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 prend en charge les intégrations avec plusieurs services AWS. Amazon GuardDuty, AWS Config, Amazon Macie, AWS IAM Access Analyzer, AWS Firewall Manager, Amazon Inspector et AWS Systems Manager Patch Manager peuvent transmettre les résultats à Security Hub. En outre, vous pouvez passer de Security Hub à Amazon Detective pour étudier une GuardDuty découverte d'Amazon. Security Hub recommande d'aligner les comptes d'administrateur délégué pour ces services (lorsqu'ils existent) pour une intégration plus fluide. Par exemple, si vous n'alignez pas les comptes d'administrateur entre Detective et Security Hub, le passage des résultats à Detective ne fonctionnera pas. Pour obtenir une liste complète, consultez la section Présentation des intégrations des services AWS avec Security Hub dans la documentation de Security Hub.

Vous pouvez utiliser Security Hub 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 blog AWS intitulé Vérification continue de la conformité du réseau à l'aide d'Amazon VPC Network Access Analyzer et d'AWS Security Hub.

Outre la surveillance, Security Hub 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. D'autres discussions et exemples sont disponibles dans ces deux articles de blog AWS : Automated Response and Remediation with AWS Security Hub et How to deploy the AWS Solution for Security Hub Automated Response and Remediation.

Security Hub utilise les règles AWS Config liées aux services pour effectuer la plupart de ses contrôles de sécurité. Pour prendre en charge ces contrôles, AWS Config doit être activé sur tous les comptes, y compris le compte administrateur (ou administrateur délégué) et les comptes des membres, dans chaque région AWS où Security Hub est activé.

Considérations relatives à la conception

- Si une norme de conformité, telle que PCI-DSS, est déjà présente dans Security Hub, le service Security Hub 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 conformité AWS Config constituent une méthode simplifiée pour effectuer cette personnalisation. (Pour plus d'informations sur AWS Config et les packs de conformité, consultez la section AWS Config.)

- Les cas d'utilisation courants de Security Hub sont les suivants :
  - En tant que tableau de bord qui fournit aux propriétaires d'applications une visibilité sur le niveau de sécurité et de conformité de leurs ressources AWS
  - 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 et prendre des mesures en fonction des résultats de sécurité et de conformité d'AWS sur les comptes et les régions AWS
  - Pour agréger et acheminer les résultats de sécurité et de conformité provenant de différents comptes et régions AWS 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 façon de les configurer, consultez le billet de blog Three Recurrent Security Hub 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. Cela inclut l'activation automatique du service, l'administration déléguée à un compte membre (Security Tooling) et la configuration permettant d'activer Security Hub pour tous les comptes existants et futurs de l'organisation AWS.

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 vos comptes et charges de travail AWS. Vous devez toujours capturer et stocker les journaux appropriés à des fins de surveillance et d'audit, mais Amazon GuardDuty extrait des flux de données indépendants directement depuis AWS CloudTrail, les journaux de flux Amazon VPC et les journaux DNS AWS.

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 analyses sans agent sur les volumes Amazon Elastic Block Store (Amazon EBS) connectés.
- 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 l'environnement AWS au sens large.

GuardDuty est activé dans tous les comptes via AWS Organizations, et tous les résultats sont consultables et exploitables par les équipes de sécurité appropriées sur le compte d'administrateur GuardDuty délégué (dans ce cas, le compte Security Tooling).

Lorsque AWS Security Hub est activé, GuardDuty les résultats sont automatiquement transmis à 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 d'Amazon 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'organisation AWS.

AWS Config

AWS Config est un service qui vous permet d'évaluer, d'auditer et d'évaluer les configurations des ressources AWS prises en charge dans vos comptes AWS. AWS Config surveille et enregistre en permanence les configurations des ressources AWS, et évalue automatiquement les configurations enregistrées par rapport aux configurations souhaitées. Vous pouvez également intégrer AWS Config à d'autres services pour effectuer le gros du travail en matière de 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 ressources AWS à l'aide des règles AWS Config. AWS Config fournit une bibliothèque de règles prédéfinies personnalisables appelées règles gérées. Vous pouvez également écrire vos propres règles personnalisées. Vous pouvez exécuter les règles AWS Config en mode proactif (avant le déploiement des ressources) ou en mode détective (après le déploiement des ressources). Les ressources peuvent être évaluées lors de modifications de configuration, selon un calendrier périodique, ou les deux.

Un pack de conformité est un ensemble de règles et d'actions correctives AWS Config 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 gérées ou personnalisées par AWS Config et des actions de correction.

Pour commencer à évaluer votre environnement AWS, utilisez l'un des exemples de modèles de pack de conformité.

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

Les règles AWS Config peuvent être utilisées conjointement avec AWS Systems Manager pour remédier efficacement aux ressources non conformes. Vous utilisez AWS Systems Manager Explorer pour connaître l'état de conformité des règles AWS Config dans vos comptes AWS dans toutes les régions AWS, puis vous utilisez les documents d'automatisation de Systems Manager (runbooks) pour résoudre vos règles AWS Config non conformes. Pour plus de détails sur la mise en œuvre, consultez le billet de blog Remediate non-compliant AWS Config rules with AWS Systems Manager Automation runbooks.

Si vous utilisez AWS Control Tower pour gérer votre organisation AWS, elle déploiera un ensemble de règles AWS Config à titre de garde-fous (classées comme obligatoires, fortement recommandées ou facultatives). Ces garde-fous vous aident à gérer vos ressources et à contrôler la conformité entre les comptes de votre organisation AWS. Ces règles AWS Config 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'organisation AWS et de la région AWS qui contient les ressources que vous souhaitez protéger. Vous pouvez gérer de manière centralisée (par exemple, créer, mettre à jour et supprimer) les règles AWS Config sur tous les comptes de votre organisation AWS. À partir du compte d'administrateur délégué AWS Config, vous pouvez déployer un ensemble commun de règles AWS Config sur tous les comptes et spécifier les comptes pour lesquels les règles AWS Config ne doivent pas être créées. Le compte d'administrateur délégué AWS Config 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 les API du compte d'administrateur délégué pour appliquer la gouvernance en vous assurant que les règles AWS Config sous-jacentes ne peuvent pas être modifiées par les comptes membres de votre organisation AWS.

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 événements AWS Config 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 AWS Config best practices.

- Outre l'évaluation proactive des règles d'AWS Config, vous pouvez utiliser AWS CloudFormation Guard, un outil d' policy-as-code évaluation qui vérifie de manière proactive la conformité de la configuration des ressources. L'interface de ligne de commande (CLI) AWS CloudFormation Guard vous fournit un langage déclaratif spécifique au domaine (DSL) que vous pouvez utiliser pour exprimer une politique sous forme de code. En outre, vous pouvez utiliser les commandes CLI 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 CLI AWS CloudFormation Guard dans le cadre de votre processus de création ou dans le cadre de votre pipeline de déploiement. Si vous possédez des applications AWS Cloud Development Kit (AWS CDK), 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 les packs de conformité AWS Config sur tous les comptes et régions AWS au sein d'une organisation AWS. Le module AWS Config Aggregator vous aide à configurer un agrégateur AWS Config en déléguant l'administration à un compte membre (Security Tooling) au sein du 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 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 environnements AWS, 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.

AWS 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 — Log Archive account account. 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 entre comptes avec les autorisations appropriées pour le compte Security Tooling et la source personnalisée soutenue par les fonctions AWS Lambda ou les robots d'exploration AWS Glue, 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 des tables AWS Lake Formation 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 d'AWS 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, les tables Athena et AWS Glue 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 QuickSight OpenSearch, Amazon et Amazon SageMaker pour configurer des analyses par rapport aux données de sécurité que vous stockez dans Security Lake.

> **Considération de 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 seul 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 dans Amazon Macie dans la documentation Macie.

Les résultats de Macie sont transmis à AWS Security Hub pour examen et 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 à l'aide d'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 d'administrateur délégué pour tous les comptes existants et futurs

de l'organisation AWS. Macie est également configuré pour envoyer les résultats à un compartiment S3 central chiffré avec une clé gérée par le client dans AWS KMS.

AWS IAM Access Analyzer

AWS IAM Access Analyzer vous aide à identifier les ressources de votre organisation et de vos comptes AWS, tels que les compartiments Amazon S3 ou les rôles IAM, qui sont partagés avec une entité externe. Ce contrôle de détection vous aide à identifier les accès involontaires à vos données et à vos ressources, qui constituent un risque pour la sécurité. IAM Access Analyzer permet également de valider les politiques IAM par rapport à la grammaire des politiques et aux meilleures pratiques, et génère des politiques IAM basées sur l'activité d'accès dans vos journaux AWS. CloudTrail

Access Analyzer 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'organisation AWS comme zone de confiance. Les résultats d'Access Analyzer sont automatiquement transmis à Security Hub. Access Analyzer envoie également un événement EventBridge pour chaque résultat généré, lorsque le statut d'un résultat existant change et lorsqu'un résultat est supprimé. EventBridge peut en outre rediriger ces événements vers des flux de notification ou de correction.

Considération de 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 à Security Hub au niveau du compte membre. De là, ils sont transférés vers le compte administrateur délégué du Security Hub (Security Tooling).

Exemple de mise en œuvre

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.

AWS Firewall Manager

AWS Firewall Manager aide à protéger votre réseau en simplifiant les tâches d'administration et de maintenance pour AWS WAF, AWS Shield Advanced, les groupes de sécurité Amazon VPC, AWS Network Firewall et Route 53 Resolver DNS Firewall sur plusieurs comptes et ressources. Avec Firewall Manager, vous ne configurez qu'une seule fois les règles de pare-feu AWS WAF, les protections Shield Advanced, les groupes de sécurité Amazon VPC, les pare-feux AWS 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 l'ensemble de votre organisation AWS 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 de VPC. 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 via AWS Organizations, et la configuration et la gestion sont effectuées par les équipes de sécurité appropriées sur le compte administrateur délégué de Firewall Manager (dans ce cas, le compte Security Tooling).

Vous devez activer AWS Config pour chaque région AWS contenant les ressources que vous souhaitez protéger. Si vous ne souhaitez pas activer AWS Config pour toutes les ressources, vous devez l'activer pour les ressources associées au type de politiques Firewall Manager que vous utilisez. Lorsque vous utilisez à la fois AWS Security Hub et Firewall Manager, Firewall Manager envoie automatiquement vos résultats à Security Hub. Firewall Manager crée des résultats pour les ressources non conformes et pour les attaques qu'il détecte, et envoie les résultats à Security Hub. 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 (ACL Web) pour tous les comptes concernés et centraliser les journaux sous un seul compte.

> **Considération de conception**
>
> - Les responsables de comptes des comptes membres individuels de l'organisation AWS peuvent configurer des contrôles supplémentaires (tels que les règles AWS WAF et

les 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 d'AWS 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 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 associant les règles AWS Config et Security Hub GuardDuty EventBridge, vous créez un pipeline flexible et automatisé pour le routage des données de sécurité, le lancement d'alertes et la gestion des 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 connecter des événements particuliers à des répondeurs AWS Lambda 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 système de bogues/problèmes 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 des CloudTrail journaux AWS et des journaux de flux Amazon VPC. Vous pouvez utiliser Detective pour accéder à un an de données historiques sur les événements. Detective utilise ces événements en utilisant des flux indépendants de CloudTrail journaux et des journaux de flux Amazon VPC. 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 ingère également les résultats détectés par Amazon GuardDuty. 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 activer 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. Cela permet de réduire le temps de triage et de permettre des enquêtes de sécurité plus complètes.

Detective s'intègre à AWS Organizations. Le compte Org Management délègue un compte membre en tant que compte administrateur Detective. Dans l'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 détective, et d'ajouter de nouveaux comptes membres au fur et à mesure de leur ajout à l'organisation AWS. Les comptes d'administrateur Detective ont également la possibilité d'inviter des comptes membres qui ne résident pas actuellement dans l'organisation AWS, 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 de conception

- Vous pouvez accéder à Detective pour trouver des profils depuis les consoles AWS Security Hub GuardDuty et AWS Security Hub. 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 (GuardDuty ou Security Hub). Si les comptes principaux sont les mêmes pour les services, les liens d'intégration fonctionnent parfaitement.

AWS Audit Manager

AWS Audit Manager vous aide à auditer en permanence votre utilisation d'AWS 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. Au moment d'effectuer un audit, Audit Manager vous aide à gérer les révisions de vos contrôles par les parties prenantes.

Avec Audit Manager, vous pouvez effectuer des audits 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 permet également de créer vos propres frameworks 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 d'AWS Config et d'AWS Security Hub, les preuves

des événements de gestion provenant d'AWS CloudTrail et les preuves de configuration issues des appels d' service-to-service API AWS. Pour les preuves qui ne peuvent pas être automatisées, Audit Manager vous permet de télécharger des preuves manuelles.

> **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 vos organisations AWS. 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 vos comptes AWS.

> **Considérations relatives à la conception**
>
> - Audit Manager complète d'autres services de sécurité AWS tels que 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 vous aide à superviser vos risques et que les packs de conformité AWS Config vous aident à gérer vos risques. Les professionnels de l'audit qui connaissent le modèle à trois lignes développé par l'Institute of Internal Auditors (IIA) doivent noter que cette combinaison de services AWS vous permet de couvrir les trois lignes de défense. Pour plus d'informations, consultez la série de blogs en deux parties sur le blog AWS Cloud Operations & Migrations.
> - Pour qu'Audit Manager puisse collecter les preuves du Security Hub, le compte d'administrateur délégué pour les deux services doit être le même compte AWS. C'est pourquoi, dans l'AWS SRA, le compte Security Tooling est l'administrateur délégué d'Audit Manager.

AWS Artifact

AWS Artifact est hébergé dans le compte Security Tooling afin de déléguer la fonctionnalité de gestion des artefacts de conformité depuis le compte AWS Org Management. Cette délégation est importante car nous vous recommandons d'éviter d'utiliser le compte AWS Org Management pour les déploiements, sauf en cas de nécessité absolue. Déléguez 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 aux équipes de sécurité et de conformité, le compte Security Tooling est désigné comme compte d'administrateur délégué pour AWS Artifact. Vous pouvez utiliser les rapports AWS Artifact pour télécharger des documents de sécurité et de conformité AWS, tels que les certifications ISO AWS, les rapports PCI (Payment Card Industry) et les rapports SOC (System and Organization Controls). Vous pouvez limiter cette fonctionnalité aux seuls rôles AWS Identity and Access Management (IAM) 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 rapports AWS Artifact spécifiques par le biais de politiques IAM. Pour des exemples de politiques IAM, consultez la documentation AWS Artifact.

Considération de conception

- Si vous choisissez de disposer d'un compte AWS dédié aux équipes d'audit et de conformité, vous pouvez héberger AWS Artifact dans un compte d'audit de sécurité, distinct du compte Security Tooling. Les rapports AWS Artifact 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 de services AWS et dans vos applications. 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 vous 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 gérées par AWS et les clés détenues par AWS. Les clés gérées par le client sont des clés AWS KMS de votre compte AWS que vous créez, détenez et gérez. Les clés gérées par AWS sont des clés AWS KMS de votre compte qui sont créées, gérées et utilisées en votre nom par un service AWS intégré à AWS KMS. Les clés détenues par AWS sont un ensemble de clés AWS KMS qu'un service AWS possède et gère pour être utilisées dans plusieurs comptes AWS. Pour plus d'informations sur l'utilisation des clés KMS, consultez la documentation AWS KMS et les détails cryptographiques d'AWS KMS.

L'une des options de déploiement consiste à centraliser la responsabilité de la gestion des clés KMS 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 vous pouvez rencontrer des obstacles en raison des limites de régulation d'AWS KMS, 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 un seul compte AWS 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 clés KMS soit auditée conformément aux meilleures pratiques et politiques établies. Pour plus d'informations, consultez le livre blanc AWS Key Management Service Best Practices. AWS SRA recommande un modèle de gestion distribuée des clés dans lequel les clés KMS résident localement dans le compte sur lequel 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 est utilisé pour gérer le chiffrement des services de sécurité centralisés tels que le CloudTrail journal d'organisation AWS géré par l'organisation AWS.

Autorité de certification privée AWS

AWS Private Certificate Authority(Autorité de certification privée AWS) 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, via des autorités de certification subordonnées, pour des certificats d'entité finale) et émettre des certificats avec cette hiérarchie pour authentifier les utilisateurs internes, les ordinateurs, les applications, les services, les serveurs et autres appareils, et pour signer le code informatique. Autorité de certification privée AWS Les certificats émis par une autorité de certification privée ne sont fiables qu'au sein de votre organisation AWS, 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. L'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 répartissant l'autorité de certification sur un compte d'application à l'aide d'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 la RAM AWS pour partager vos Autorité de certification privée AWS comptes entre comptes.

> **Note**
>
> ACM vous aide également à fournir, gérer et déployer des certificats TLS publics à utiliser avec les services AWS. Pour prendre en charge cette fonctionnalité, ACM doit résider dans le 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 Autorité de certification privée AWS, vous pouvez créer une hiérarchie d'autorités de certification avec cinq niveaux maximum. Vous pouvez également créer plusieurs hiérarchies, chacune ayant sa propre racine. La Autorité de certification privée AWS 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, vos autorités de certification racine et subordonnées se trouvent dans des comptes AWS distincts. Pour plus d'informations sur la planification d'une hiérarchie CA à l'aide deAutorité de certification privée AWS, consultez la Autorité de certification privée AWSdocumentation et le billet de blog Comment sécuriser une Autorité de certification privée AWS hiérarchie à l'échelle de l'entreprise pour l'automobile et le secteur manufacturier.
- Autorité de certification privée AWSpeut s'intégrer à votre hiérarchie de CA existante, ce qui vous permet d'utiliser l'automatisation et la capacité d'intégration AWS 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 Autorité de certification privée AWS 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 Autorité de certification privée AWS 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 Container Registry (Amazon ECR) et les fonctions AWS Lambda pour détecter les vulnérabilités logicielles connues et les expositions involontaires 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) affectant la ressource.

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 (VPN) via une passerelle virtuelle. Ces règles permettent d'automatiser la surveillance de vos réseaux AWS 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 (ACL), 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.

Pour détecter les vulnérabilités, les instances EC2 doivent être gérées dans AWS Systems Manager à l'aide de l'agent AWS Systems Manager (agent SSM). 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 à AWS Organizations et prend en charge l'administration déléguée. Dans l'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'organisation AWS. 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'organisation AWS.

Considérations relatives à la conception

- Amazon Inspector s'intègre automatiquement à AWS Security Hub lorsque les deux services sont activés. Vous pouvez utiliser cette intégration pour envoyer tous les résultats

d'Amazon Inspector à Security Hub, 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 clé AWS KMS qu'Amazon Inspector peut utiliser pour chiffrer les résultats et d'un compartiment S3 doté d'autorisations permettant à Amazon Inspector de télécharger des objets. EventBridge l'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.

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'organisation AWS.

Déploiement de services de sécurité communs au sein de tous les comptes AWS

La section Appliquer les services de sécurité à l'ensemble de votre organisation AWS 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 d'AWS Organizations. Certains de ces services doivent être déployés dans tous les comptes, et vous les verrez dans l'AWS SRA. Cela permet de disposer d'un ensemble cohérent de garde-fous et de centraliser la surveillance, la gestion et la gouvernance au sein de votre organisation AWS.

Security Hub GuardDuty, AWS Config, Access Analyzer et les traces d' CloudTrail organisation AWS apparaissent dans tous les comptes. Les trois premiers prennent en charge la fonctionnalité d'administrateur délégué décrite précédemment dans les sections Compte de gestion, accès sécurisé et 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 GuardDuty, AWS Config, Firewall Manager et les traces d' CloudTrail organisation sur tous vos comptes, y compris le compte AWS Org Management.

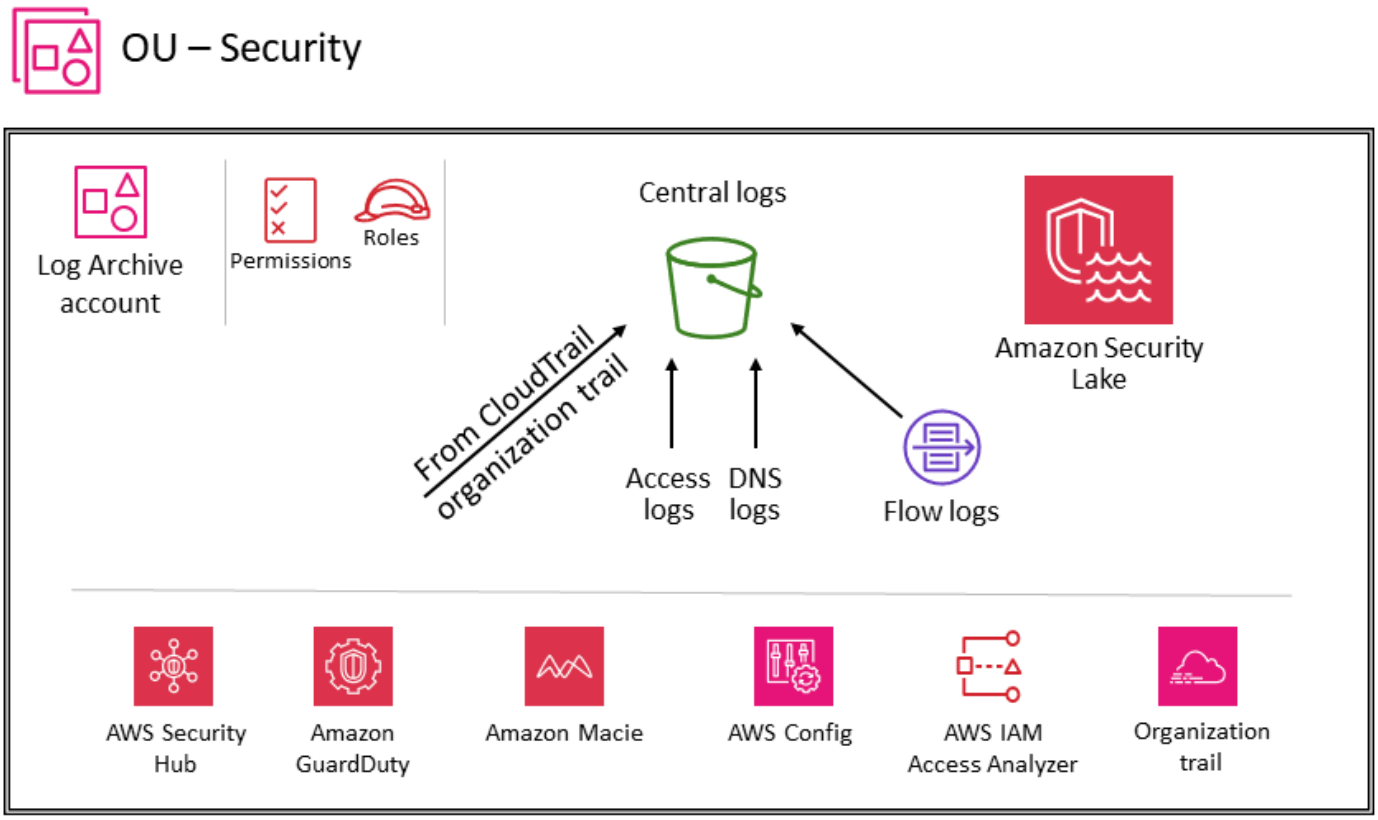
Considérations relatives à la conception

- 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, l'AWS SRA inclut deux services axés sur la sécurité, Amazon Detective et AWS Audit Manager, qui prennent en charge l'intégration d'AWS Organizations 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 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 (AWSSRA) en répondant à une courte enquête.

Le schéma suivant illustre les services de sécurité AWS 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 de rôles de moindre privilège à utiliser pour l'accès et le chiffrement des journaux à l'aide d'une clé AWS KMS contrôlée, utilisez des contrôles de détection tels qu'AWS Config pour surveiller (et alerter et corriger) cet ensemble d'autorisations en cas de modifications inattendues.

Considération de 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 l'AWS SRA incluent CloudTrail (suivi de l'organisation), les journaux de flux Amazon VPC, les journaux d'accès d' CloudFront Amazon et d'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, un service AWS ou une entité réseau (identifié, par exemple, par une adresse IP). 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 nombreux services AWS enregistrent des informations dans Amazon S3, par défaut ou exclusivement. AWS CloudTrail, Amazon VPC Flow Logs, AWS Config et Elastic Load Balancing sont 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 l'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 les clés AWS KMS 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 gérée par AWS `AWSCloudTrail_FullAccess` peuvent désactiver ou reconfigurer les fonctions d'audit les plus sensibles et les plus importantes de leurs 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 et AWS 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 bloqués Amazon S3. Ce module bloque l'accès public à Amazon S3 pour tous les comptes existants et futurs de l'organisation AWS.

Amazon Security Lake

AWS 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 clé contrôlée AWS Key Management Services (AWS KMS), utilisez des contrôles de détection tels qu'AWS Config pour surveiller (et alerter et corriger) cet ensemble d'autorisations en cas de modifications inattendues.

L'administrateur de Security Lake peut activer la collecte de journaux au sein de votre organisation AWS. 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 des services AWS pris en charge 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 d'AWS et d'autres sources de sécurité d'entreprise afin de créer un référentiel unifié et fiable d'informations relatives à la sécurité.

Security Lake peut collecter des journaux associés aux événements de CloudTrail gestion AWS 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 des fichiers journaux provenant de plusieurs régions vers un seul compartiment S3 pour un seul 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 est une source de données native prise en charge dans Security Lake, et vous devez ajouter les résultats de Security Hub à Security Lake. Security Hub génère des résultats à partir de nombreux services AWS et d'intégrations tierces. Ces résultats vous permettent d'avoir une

vue d'ensemble de votre niveau de conformité et de savoir si vous suivez les recommandations de sécurité pour AWS et les solutions de ses partenaires.

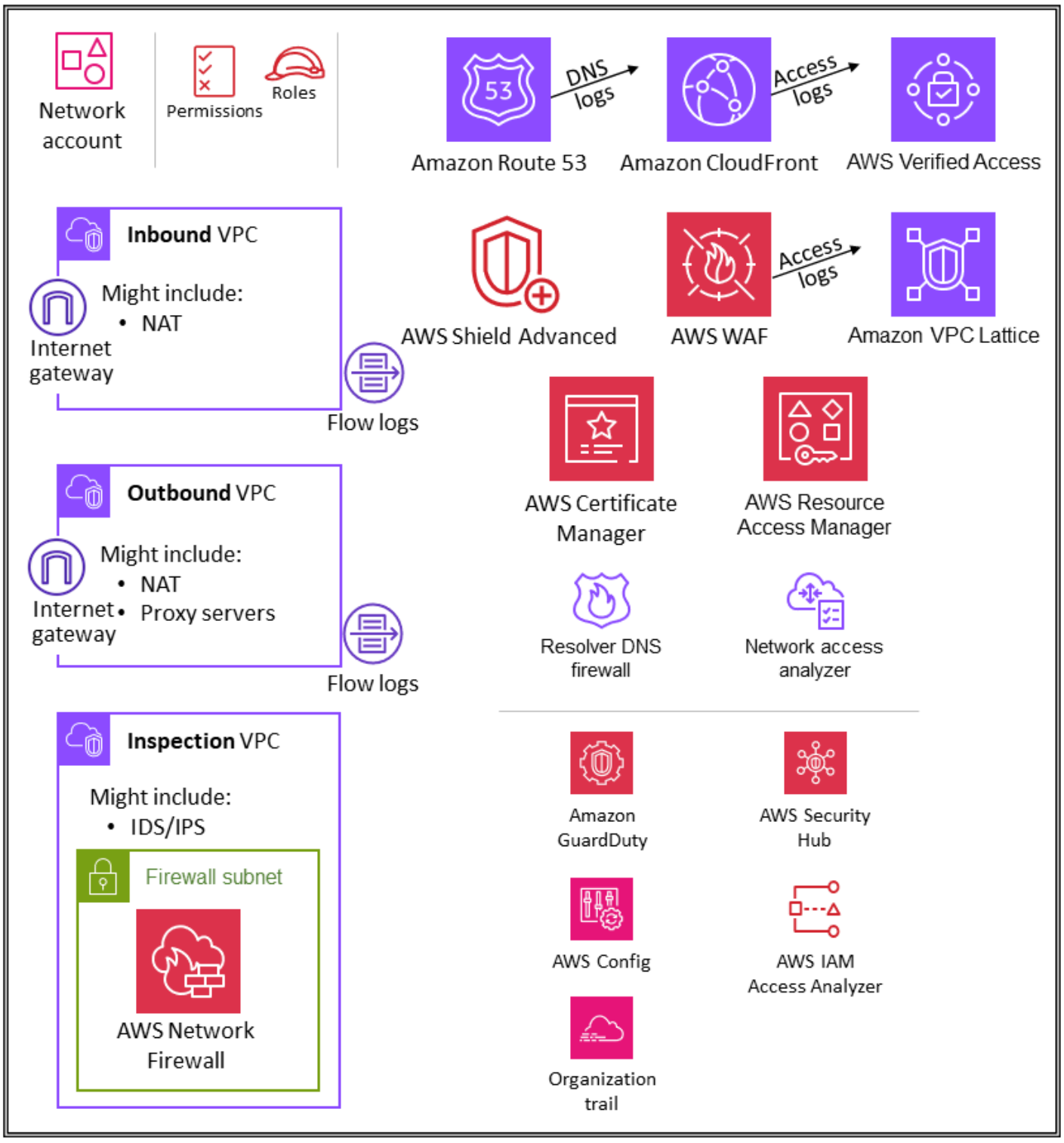
Pour obtenir de la visibilité et des informations exploitables à partir des journaux et des événements, vous pouvez interroger les données à l'aide d'outils tels qu'Amazon Athena, OpenSearch Amazon Service, Amazon Quicksight et de solutions tierces. Les utilisateurs qui ont besoin d'accéder aux données 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 comptes AWS ou des sites sur site qui fournissent des outils d'analyse tels que OpenSearch Service QuickSight, 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 — Security Tooling account de ce guide.

Security Lake fournit une politique gérée par AWS pour vous aider à gérer l'accès des administrateurs au service. Pour plus d'informations, consultez le guide de l'utilisateur de Security Lake. Comme bonne pratique, nous vous recommandons de restreindre la configuration de Security Lake par le biais de pipelines de développement et d'empêcher les modifications de configuration via les consoles AWS ou l'interface de ligne de commande (AWS CLI) AWS. En outre, vous devez définir des politiques IAM et des politiques de contrôle des services (SCP) 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.

Infrastructure UO – Compte réseau

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

Le schéma suivant illustre les services de sécurité AWS qui sont 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 du réseau en clouds privés virtuels (VPC) entrants et sortants distincts, 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 ces trois options pour la connectivité réseau entre les différents comptes : l'appairage de 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.

- L'appairage de VPC : le moyen le plus simple de connecter deux VPC est d'utiliser l'appairage de VPC. Une connexion permet une connectivité bidirectionnelle complète entre les VPC. Les VPC qui se trouvent dans des comptes et des Régions AWS distincts peuvent également être appairés ensemble. À grande échelle, lorsque vous avez des dizaines, voire des centaines de VPC, leur interconnexion par l'appairage se traduit par un maillage de centaines, voire de milliers de connexions d'appairage, ce qui peut être difficile à gérer et à mettre à l'échelle. 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 VPC est contrôlé et sécurisé et que le nombre de VPC à connecter est inférieur à 10 (pour permettre la gestion individuelle de chaque connexion).
- AWS PrivateLink : PrivateLink fournit une connectivité privée entre les VPC, les services et les applications. Vous pouvez créer votre propre application dans votre VPC et la configurer en tant que service à technologie PrivateLink (dénommé service de point de terminaison). D'autres principaux AWS peuvent créer une connexion à partir de leur VPC à votre service de point de terminaison en utilisant un point de terminaison d'un VPC d'interface ou un point de terminaison d'équilibreur de charge de passerelle, selon le type de service. Lorsque vous utilisez PrivateLink, le trafic du service ne passe pas par un réseau routable publiquement. Utilisez PrivateLink lorsque vous disposez d'une configuration client-serveur dans laquelle vous souhaitez accorder à un ou plusieurs VPC consommateurs un accès 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 clients et les serveurs des deux VPC ont des adresses IP qui se chevauchent, car 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 propose une conception en étoile permettant de connecter des VPC et des réseaux sur site sous la forme d'un service entièrement géré sans que vous ayez à provisionner d'appareils virtuels. AWS gère la haute disponibilité et la capacité de mise à l'échelle. Une passerelle de transit est une ressource régionale qui peut connecter des milliers de VPC au sein d'une même Région AWS. Vous pouvez associer votre connectivité hybride (connexions VPN et AWS Direct Connect) à une passerelle de transit unique, consolidant et contrôlant ainsi l'ensemble de la configuration de routage de votre organisation AWS 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 en dehors 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 apparaître du trafic NAT, des points de terminaison d'un VPC spécifiques au service AWS 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 offre une approche simplifiée et centralisée de la gestion des inspections entre les VPC (dans la même Région AWS ou dans des régions différentes), Internet et les réseaux sur site. Pour l'AWS SRA, assurez-vous que tout le trafic entre les VPC 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 Firewall est un service de pare-feu réseau géré à haute disponibilité pour votre VPC. Il vous permet de déployer et de gérer facilement l'inspection dynamique, la prévention et la détection des intrusions, ainsi que le filtrage Web, afin de protéger vos réseaux virtuels sur AWS. 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 métriques Amazon CloudWatch et offre une visibilité accrue du trafic réseau en envoyant des journaux à Amazon Simple Storage Service (Amazon S3), CloudWatch et Amazon Kinesis Data Firehose. Network Firewall est interopérable avec votre approche de sécurité existante, y compris les technologies des partenaires AWS. 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 l'AWS SRA, Network Firewall est utilisé dans le compte réseau, car la fonctionnalité du service axée sur le contrôle du réseau correspond à l'intention du compte.

Considérations relatives à la conception

- AWS Firewall Manager prend en charge Network Firewall, ce qui vous permet de configurer et de déployer de manière centralisée les règles de Network Firewall au sein de votre organisation. (Pour en savoir plus, consultez AWS Network Firewall policies dans la documentation AWS.) Lorsque vous configurez Firewall Manager, il crée automatiquement un pare-feu avec des ensembles de règles dans les comptes et les VPC que vous spécifiez. 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 dans des VPC individuels.
  - 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.

L'analyseur d'accès réseau utilise des algorithmes de raisonnement automatisés pour analyser les chemins réseau qu'un paquet peut emprunter entre les ressources d'un réseau AWS 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. L'analyseur d'accès réseau et l'accessibilité du réseau utilisent tous deux la dernière technologie de l'initiative AWS Provable Security, qu'ils appliquent dans des domaines différents. Le package d'accessibilité du réseau se concentre spécifiquement sur les instances EC2 et leur accessibilité à Internet.

Le compte réseau définit l'infrastructure réseau critique qui contrôle le trafic entrant et sortant de votre environnement AWS. Ce trafic doit être étroitement surveillé. Dans l'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 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

- L'analyseur d'accès réseau est une fonctionnalité d'Amazon VPC qui peut être utilisée dans n'importe quel compte AWS doté d'un VPC. Les administrateurs réseau peuvent obtenir des rôles IAM à portée réduite et intercomptes afin de vérifier que les chemins réseau approuvés sont appliqués dans chaque compte AWS.

AWS RAM

AWS Resource Access Manager (AWS RAM) vous permet de partager en toute sécurité les ressources AWS que vous créez dans un compte AWS avec d'autres 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, AWS RAM vous permet de partager des ressources avec tous les comptes de l'organisation, ou uniquement avec les comptes d'une ou de plusieurs unités organisationnelles (UO) spécifiées. Vous pouvez également partager avec des comptes AWS spécifiques 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. En outre, avec AWS RAM, les propriétaires d'une ressource peuvent voir quels principaux ont accès aux ressources individuelles qu'ils ont partagées. Les entités IAM peuvent récupérer directement la liste des ressources partagées avec elles, ce qu'elles ne peuvent pas faire avec les ressources partagées par les politiques de ressources IAM. Si AWS RAM est utilisé pour partager des ressources en dehors de votre organisation AWS, un processus d'invitation est lancé. Le destinataire doit accepter

l'invitation avant que l'accès aux ressources ne soit accordé. Cela permet de renforcer les contrôles et les équilibres.

AWS RAM est invoqué et géré par le propriétaire de la ressource, dans le compte où la ressource partagée est déployée. L'un des cas d'utilisation courants d'AWS RAM illustré dans l'AWS SRA consiste pour les administrateurs réseau à partager les sous-réseaux VPC et les passerelles de transit avec l'ensemble de l'organisation AWS. Cela permet de dissocier les fonctions de gestion des comptes AWS et du réseau et contribue à la séparation des tâches. Pour en savoir plus sur le partage de VPC, consultez le billet du blog AWS VPC sharing: A new approach to multiple accounts and VPC management et AWS network infrastructure whitepaper.

Considération relative à la conception

- Bien que le service AWS RAM ne soit déployé qu'au sein du compte Réseau dans l'AWS SRA, il est généralement déployé dans plus d'un compte. 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 données AWS Lake Formation (bases de données et tables) avec d'autres comptes de votre organisation AWS. Pour en savoir plus, consultez AWS Lake Formation documentation et le billet de blog AWS Securely share your data across AWS accounts using AWS Lake Formation. En outre, les administrateurs de la sécurité peuvent utiliser AWS RAM pour suivre les meilleures pratiques lorsqu'ils créent une hiérarchie Autorité de certification privée AWS. Les autorités de certification peuvent être partagées 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

L'accès vérifié par AWS fournit un accès sécurisé aux applications d'entreprise sans VPN. Il améliore le niveau de sécurité 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. 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. L'accès vérifié prend également en charge l'intégration avec AWS WAF pour vous aider à filtrer

les menaces courantes telles que l'injection SQL et les scripts inter-site (XSS). L'accès vérifié est parfaitement intégré à AWS IAM Identity Center, qui permet aux utilisateurs de s'authentifier auprès de fournisseurs d'identité (IdP) tiers basés sur SAML. 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. L'accès vérifié prend en charge la livraison de ces journaux à Amazon Simple Storage Service (Amazon S3), Amazon CloudWatch Logs et Amazon Kinesis 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, l'accès vérifié nécessite un équilibreur de charge interne. Dans la mesure où l'accès vérifié prend en charge AWS WAF au niveau de l'instance, une application existante qui dispose d'une intégration AWS WAF avec un Application Load Balancer peut déplacer les stratégies de l'équilibreur de charge vers l'instance de l'accès vérifié. 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 l'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 Resource Access Manager (AWS RAM). Cela permet aux équipes chargées des applications de gérer les points de terminaison sous-jacents qui gèrent leurs applications sans que d'autres équipes aient à s'en soucier. 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 entre services. Un service, souvent appelé microservice, est une unité logicielle déployable indépendante qui exécute une tâche spécifique. VPC Lattice gère automatiquement la connectivité réseau et le routage de la couche application entre les services à travers les VPC et les comptes AWS sans que vous ayez à gérer la connectivité réseau sous-jacente, les équilibreurs de charge frotend ou les proxys sidecar. 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 à travers un large éventail de types de calcul tels qu'Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS) et AWS Lambda. VPC Lattice prend également en charge le routage pondéré pour les déploiements bleu/vert et de type canary. Vous pouvez utiliser VPC Lattice pour créer un réseau de services avec une limite logique qui implémente automatiquement la découverte de service et la connectivité. VPC Lattice s'intègre à AWS Identity and Access Management (IAM) pour l'authentification et l'autorisation de service à service à l'aide de politiques d'authentification.

VPC Lattice s'intègre à AWS Resource Access Manager (AWS RAM) pour permettre le partage des services et des réseaux de services. AWS SRA présente 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 les VPC et les services VPC

Lattice à un ou plusieurs réseaux de services. Pour une présentation détaillée de cette architecture distribuée, consultez le billet de blog AWS Build secure multi-account multi-VPC connectivity for your applications with Amazon VPC Lattice.

Considération relative à la conception

- Selon le modèle d'exploitation de votre organisation en matière de visibilité des services ou des réseaux de services, les administrateurs réseau peuvent partager leurs réseaux de services et donner aux propriétaires de services la possibilité d'associer leurs services et leurs VPC 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 à la périphérie implique généralement trois types de protection : la diffusion sécurisée de contenu, la protection du réseau et de la couche d'application, et l'atténuation des attaques par déni de service distribué (DDoS). Le contenu tel que les données, les vidéos, les applications et les API doit être diffusé 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 URL signées, des cookies signés et une authentification par jeton. 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 des attaques DDoS fournit une couche de défense importante qui garantit la disponibilité continue des opérations et des services essentiels à la mission de l'entreprise. Les applications et les API doivent être protégées contre les saturations SYN, les saturations UDP ou autres attaques par réflexion, et disposer de mesures d'atténuation en ligne pour arrêter les attaques de base de la couche réseau.

AWS propose plusieurs services qui contribuent à créer un environnement sécurisé, depuis la partie centrale du cloud jusqu'à la périphérie du réseau AWS. 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 Amazon CloudFront, le contenu, les API ou les applications peuvent être diffusés via HTTPS en utilisant TLSv1.3 pour chiffrer et sécuriser les communications entre les clients utilisateurs et CloudFront. Vous pouvez utiliser ACM pour créer un certificat SSL personnalisé et le déployer gratuitement sur une distribution CloudFront. ACM gère automatiquement le renouvellement des certificats. AWS Shield est un service géré de protection contre les attaques DDoS qui permet de protéger les applications exécutées sur AWS. Il offre une détection dynamique et des mesures d'atténuation automatiques en ligne qui minimisent les temps d'arrêt et de 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 URI personnalisés), d'attaques Web courantes et de 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 AWS ou sur site. L'AWS SRA adopte une architecture d'entrée réseau centralisée en utilisant AWS Transit Gateway, hébergé dans le compte réseau, de sorte que l'infrastructure de sécurité à la périphérie est également centralisée dans ce compte.

Amazon CloudFront

Amazon CloudFront est un réseau de diffusion de contenu (CDN) sécurisé qui fournit une protection inhérente contre les tentatives d'attaques DDoS courantes au niveau de la couche réseau et du transport. Vous pouvez diffuser votre contenu, vos API ou vos applications à l'aide de certificats TLS, et les fonctionnalités TLS avancées sont activées automatiquement. Vous pouvez utiliser 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 un chiffrement de bout en bout 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 des sites Web des compartiments S3 servent d'origine pour CloudFront, vous ne pouvez pas configurer CloudFront pour utiliser HTTPS avec votre origine, car Amazon S3 ne prend pas en charge HTTPS pour les points de terminaison de site Web. (Cependant, vous pouvez toujours exiger HTTPS entre les spectateurs 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 URL et des cookies

signés. Pour en savoir plus, consultez Configuring secure access and restricting access to content dans la documentation CloudFront.

L'AWS SRA illustre les distributions CloudFront centralisées dans le compte réseau, car elles s'alignent sur le modèle de réseau centralisé mis en œuvre à l'aide de Transit Gateway. En déployant et en gérant les distributions CloudFront dans le compte réseau, vous bénéficiez des avantages des contrôles centralisés. Vous pouvez gérer toutes les distributions CloudFront en un seul endroit, ce qui facilite le contrôle de l'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 journalisation CloudFront à partir d'un compte centralisé.

Considérations relatives à la conception

- Vous pouvez également déployer CloudFront en tant que partie 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 distributions CloudFront sont déployées, détermine les stratégies de cache appropriées et assume la responsabilité de la gouvernance, de l'audit et de la surveillance des distributions CloudFront. En répartissant les distributions CloudFront sur plusieurs comptes, vous pouvez bénéficier de quotas de service supplémentaires. Autre avantage, vous pouvez utiliser la configuration inhérente et automatisée de l'identité d'accès d'origine (OAI) et de contrôle d'accès d'origine (OAC) de CloudFront pour restreindre l'accès aux origines Amazon S3.
- Lorsque vous diffusez du contenu Web via un CDN tel que CloudFront, vous devez empêcher les spectateurs de contourner le CDN et d'accéder directement à votre contenu d'origine. Pour réaliser cette restriction d'accès d'origine, vous pouvez utiliser CloudFront et AWS WAF pour ajouter des en-têtes personnalisés et vérifier les en-têtes avant de transmettre les demandes à votre origine personnalisée. Pour une explication détaillée de cette solution, consultez le billet de blog sécurité AWS How to enhance Amazon CloudFront origin security with AWS WAF and AWS Secrets Manager. Une autre méthode consiste à limiter uniquement la liste des préfixes CloudFront dans le groupe de sécurité associé à l'Application Load Balancer. Cela permettra de garantir que seule une distribution CloudFront peut accéder à l'équilibreur de charge.

AWS WAF

AWS WAF est un pare-feu d'application Web qui aide à protéger vos applications Web contre les attaques Web telles que les vulnérabilités courantes et les bots susceptibles d'affecter la disponibilité des applications, de compromettre la sécurité ou de consommer des ressources excessives. Ce service peut être intégré avec une distribution Amazon CloudFront, une API REST Amazon API Gateway, un Application Load Balancer, une API AWS AppSync GraphQL, un groupe d'utilisateurs Amazon Cognito et le service AWS App Runner.

AWS WAF utilise des listes de contrôle d'accès (ACL) pour protéger un ensemble de ressources AWS. 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 des bots) si une demande 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 et les partenaires AWS. 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, ainsi qu'une protection contre la prise de contrôle des comptes (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 console AWS WAF pour surveiller ces activités, puis décider si vous avez besoin d'un groupe de règles AWS WAF à niveau intelligent.

Dans l'AWS SRA, AWS WAF est intégré à CloudFront dans le compte réseau. Dans cette configuration, le traitement des règles WAF 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 des journaux AWS WAF complets vers un compartiment S3 du compte d'archivage des journaux en configurant l'accès intercompte au compartiment S3. Pour plus d'informations, consultez l'article AWS re:Post à ce sujet.

Considérations relatives à la conception

- Au lieu de déployer AWS WAF de manière centralisée dans le compte réseau, il est préférable de déployer AWS WAF dans le compte d'application pour répondre à certains cas d'utilisation. Par exemple, vous pouvez choisir cette option lorsque vous déployez vos distributions CloudFront dans votre compte d'application ou que vous utilisez des Application Load Balancers destinés au public, ou si vous utilisez Amazon API Gateway devant vos applications Web. Si vous décidez de déployer AWS WAF dans chaque compte d'application, utilisez AWS Firewall Manager pour gérer les règles AWS WAF dans ces comptes à partir du compte d'outils de sécurité centralisé.
- Vous pouvez également ajouter des règles AWS WAF générales au niveau de la couche CloudFront et des règles AWS WAF supplémentaires spécifiques à l'application au niveau d'une ressource régionale telle que l'Application Load Balancer ou la passerelle API.

AWS Shield

AWS Shield est un service géré de protection contre les attaques DDoS qui protège les applications exécutées sur AWS. Il existe deux niveaux de Shield : Shield Standard et Shield Advanced. Shield Standard fournit à tous les clients AWS 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 protégées Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator et Route 53. Si vous possédez des sites Web à haute visibilité ou si vous êtes sujet à des attaques DDoS fréquentes, envisagez les fonctionnalités supplémentaires proposées par Shield Advanced.

Vous pouvez utiliser la fonctionnalité d'atténuation automatique des attaques DDoS de la couche d'application Shield Advanced pour configurer Shield Advanced afin qu'il réponde automatiquement pour atténuer les attaques de la couche d'application (couche 7) contre vos distributions CloudFront protégées et vos Application Load Balancers. Lorsque vous activez cette fonctionnalité, Shield Advanced génère automatiquement des règles AWS WAF personnalisées pour atténuer les attaques DDoS. Shield Advanced vous donne également accès à l'équipe AWS Shield Response Team (SRT). Vous pouvez contacter l'équipe SRT à tout moment pour créer et gérer des mesures d'atténuation personnalisées pour votre application ou lors d'une attaque DDoS active. Si vous souhaitez que l'équipe SRT surveille de manière proactive vos ressources protégées et vous contacte lors d'une tentative d'attaque DDoS, pensez à activer la fonctionnalité d'engagement proactif.

Considérations relatives à la conception

- Si vous avez des charges de travail qui sont dirigées vers des ressources Internet dans le compte d'application, comme Amazon CloudFront, un Application Load Balancer ou un Network Load Balancer, configurez Shield Advanced dans le compte d'application et ajoutez ces ressources à la protection Shield. Vous pouvez utiliser AWS Firewall Manager pour configurer ces options à grande échelle.
- Si vous avez plusieurs ressources dans le flux de données, comme une distribution CloudFront devant un Application Load Balancer, n'utilisez que 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 métriques que vous pouvez surveiller dans Amazon CloudWatch. (Pour en savoir plus, consultez les AWS Shield Advanced metrics and alarms dans la documentation AWS.) Configurez les alarmes CloudWatch pour recevoir des notifications SNS à votre centre de sécurité lorsqu'un événement DDoS est détecté. En cas de suspicion d'événement DDoS, contactez l'équipe AWS Enterprise Support en déposant un ticket d'assistance et en lui attribuant la plus haute priorité. 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'engagement d'AWS Shield pour créer un ticket d'assistance et envoyer un e-mail à l'équipe SRT.

AWS Certificate Manager

AWS Certificate Manager (ACM) vous permet de fournir, de gérer et de déployer des certificats TLS publics et privés à utiliser avec les services AWS et vos ressources connectées internes. Avec ACM, vous pouvez rapidement demander un certificat, le déployer sur des ressources AWS intégrées à ACM, telles que les équilibreurs de charge Elastic Load Balancing, les distributions Amazon CloudFront et les API sur Amazon API 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 une 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 autorités de certification tierces et de les déployer avec les services intégrés d'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 distributions CloudFront pour établir la connexion HTTPS entre les utilisateurs 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 instances EC2, à vos compartiments S3, à vos distributions CloudFront et à d'autres ressources AWS. La nature distribuée des serveurs DNS AWS permet de garantir que vos utilisateurs finaux sont acheminés de manière cohérente vers votre application. Des fonctionnalités telles que le flux de trafic et le contrôle du routage de 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 vos réseaux VPC et sur site via AWS Direct Connect ou VPN géré par AWS.

En utilisant le service AWS Identity and Access Management (IAM) avec Route 53, vous pouvez contrôler précisément 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 fournit une protection pour les demandes DNS sortantes provenant de vos VPC. 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'instances EC2 publiques ou privées.

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

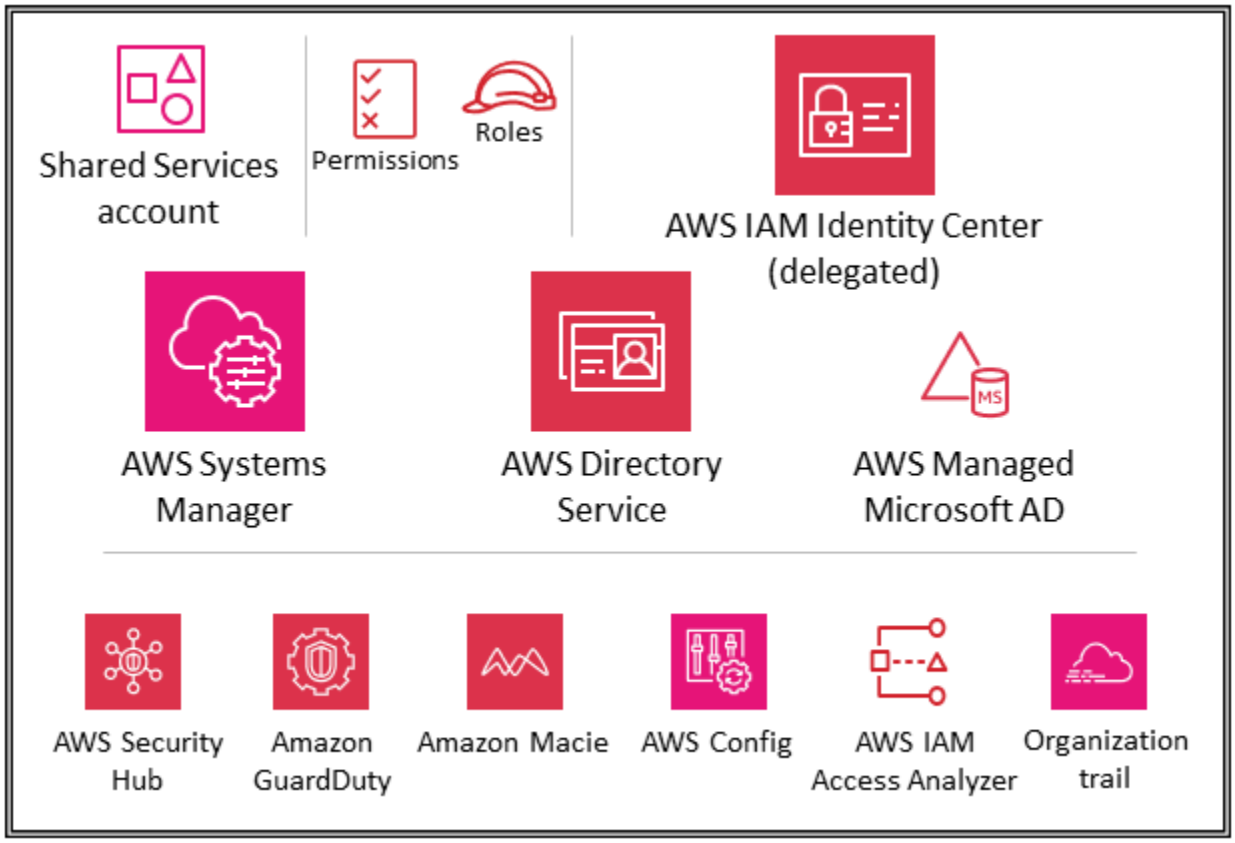
Considération relative à la conception

- Le pare-feu DNS et AWS Network Firewall offrent tous deux le filtrage des noms de domaine, mais pour différents types de trafic. Vous pouvez utiliser à la fois le pare-feu DNS et Network Firewall pour configurer le filtrage basé sur le domaine pour le trafic de la couche d'application sur deux chemins réseau différents.
  - Le pare-feu DNS fournit le filtrage des requêtes DNS sortantes qui passent par Route 53 Resolver à partir des applications de vos VPC. 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 (AWSSRA) en répondant à une courte enquête.

Le schéma suivant illustre les services de sécurité AWS 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. L'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 d'application) fournit un ensemble de fonctionnalités qui permettent la visibilité et le contrôle de vos ressources AWS. L'une de ces fonctionnalités, Systems Manager Explorer, est un tableau de bord d'opérations personnalisable qui fournit des informations sur vos ressources AWS. Vous pouvez synchroniser les données d'exploitation entre tous les comptes de votre organisation AWS à l'aide d'AWS Organizations et 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 au déploiement approprié sur les comptes AWS individuels des membres (par exemple, le compte Application), vous pouvez coordonner la collecte des données d'inventaire des instances et centraliser les automatisations telles que les correctifs et les mises à jour de sécurité.

Microsoft AD géré par AWS

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

AWS Managed Microsoft AD vous aide à étendre votre Active Directory existant à AWS et à utiliser vos informations d'identification utilisateur sur site 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 domaine Microsoft AD géré par AWS.

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 (GPO), les approbations de domaine, les politiques de mot de passe détaillées, les comptes de services gérés de groupe (GMSA), 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 répertoire Microsoft AD géré par AWS dans 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 via les ports 636 (SSL) et 389 (TLS). Vous activez les communications LDAPS côté serveur en installant un certificat sur vos contrôleurs de domaine Microsoft AD gérés par AWS à partir d'une autorité de certification (CA) Active Directory Certificate Services (AD CS) basée sur AWS. 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 émis par les émetteurs de certificats de votre serveur dans AWS, puis en activant LDAPS dans votre annuaire.

Dans l'AWS SRA, AWS Directory Service 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 de conception

- Vous pouvez autoriser vos utilisateurs Active Directory locaux à se connecter à l'AWS Management Console et à l'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 utiliser AWS Managed Microsoft AD pour permettre à vos utilisateurs d'assumer un rôle AWS Identity and Access Management (IAM).

IAM Identity Center

L'AWS SRA utilise la fonctionnalité d'administrateur délégué prise en charge par 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 l'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 d'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 votre AWS Managed Microsoft AD au sein d'un 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 d'administrateur délégué. Ainsi, l'instance AWS Managed Microsoft AD est contrôlée dans le compte d'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 disposez de plusieurs instances Microsoft AD gérées par AWS 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 un compte AWS dédié à la gestion des identités. Dans ce scénario, vous désignez ce compte comme administrateur délégué pour IAM Identity Center, et il héberge également votre répertoire Microsoft AD géré par AWS. Vous pouvez atteindre le

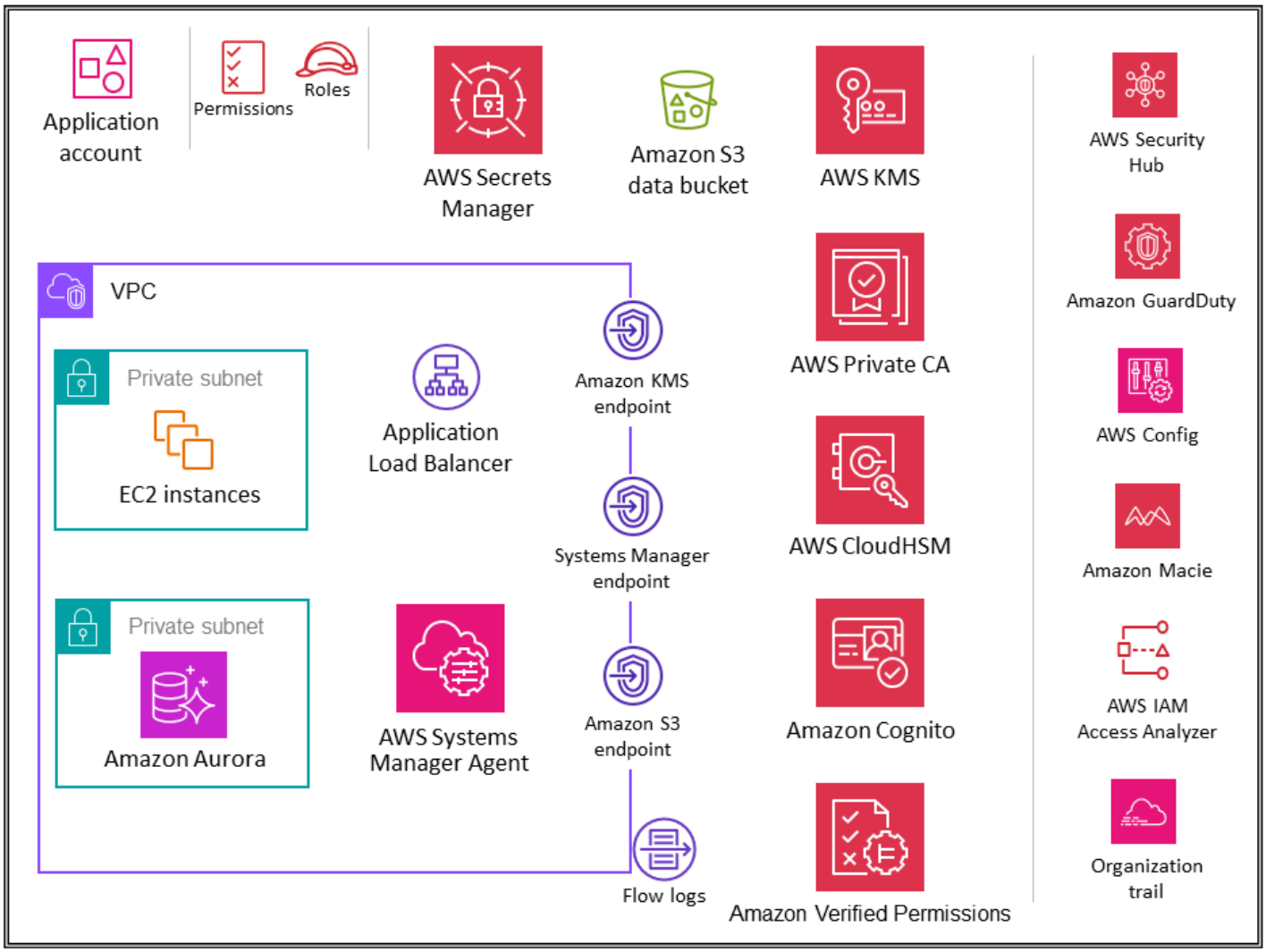
même niveau d'isolation logique entre vos charges de travail de gestion des identités et les charges de travail des autres services partagés en utilisant des autorisations IAM précises au sein d'un seul compte de service partagé.

- 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 à AWS et autoriser ces identités d'utilisateurs externes à utiliser les ressources AWS 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 à l'AWS Management Console ou d'appeler les opérations d'API AWS. 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 et dans les ateliers AWS Identity Federation.

Workloads OU — Compte d'application

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

Le schéma suivant illustre les services de sécurité AWS 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, Amazon EventBridge, AWS 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 de 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 unités d'organisation enfants en 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 les unités d'organisation relatives à différentes applications. Un autre schéma courant consiste à avoir des unités d'organisation enfants distinctes par application, puis à utiliser des comptes AWS enfants distincts pour les environnements de développement individuels. 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 mettre en œuvre ces contrôles en tant que SCP sur les unités d'organisation. Pour plus d'informations sur l'organisation des unités d'organisation axées sur la charge de travail, consultez la section Organisation des unités d'organisation axées sur la charge de travail du livre blanc AWS Organizing Your AWS Environment Using Multiple Accounts.

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 des applications ou des services 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 instances EC2 (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 de conception

- Vous pouvez utiliser Traffic Mirroring pour copier le trafic réseau à partir d'une interface réseau élastique d'instances EC2. 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 réseau élastique des instances EC2 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 d'autres services AWS. (Dans le compte d'application, l'AWS SRA utilise des points de terminaison VPC pour AWS KMS, 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 AWS pris en charge et aux services de point de terminaison VPC optimisés par AWS PrivateLink sans avoir besoin d'une passerelle Internet, d'un appareil 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 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 politique IAM lorsque vous créez un point de terminaison, AWS attache pour vous une politique IAM par défaut qui permet un accès complet au service. Une politique de point de terminaison ne remplace ni ne remplace les politiques IAM ou les politiques spécifiques au service (telles que les politiques de compartiment S3). Il s'agit d'une politique IAM distincte permettant de contrôler l'accès du point de terminaison au service spécifié. Cela ajoute ainsi un niveau de contrôle supplémentaire sur lequel les responsables d'AWS peuvent communiquer avec les ressources ou les services.

Amazon EC2

Les instances Amazon EC2 qui composent notre application utilisent la version 2 du service de métadonnées d'instance (IMDSv2). IMDSv2 protège quatre types de vulnérabilités susceptibles d'être utilisées pour tenter d'accéder à l'IMDS : les pare-feux d'applications Web, les proxys inverses ouverts, les vulnérabilités de falsification de requêtes côté serveur (SSRF), les pare-feux ouverts de couche 3 et les NAT. 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'instance EC2.

Utilisez des VPC distincts (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'API Amazon EC2 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 des journaux de flux VPC pour surveiller la trafic atteignant vos instances. Utilisez le gestionnaire de session, une fonctionnalité d'AWS Systems Manager, pour accéder à vos instances à distance au lieu d'ouvrir des ports SSH entrants et de gérer des 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 AWS et de chaque région AWS de l'organisation AWS.

Application Load Balancers

Les équilibreurs de charge des applications distribuent le trafic applicatif entrant sur plusieurs cibles, telles que les instances EC2, dans plusieurs zones de disponibilité. Dans l'AWS SRA, le groupe cible de l'équilibreur de charge est constitué des instances EC2 de l'application. L'AWS SRA utilise des écouteurs HTTPS pour s'assurer que le canal de communication est chiffré. 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 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 de plus amples informations, veuillez consulter 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. Autorité de certification privée AWS Dans l'AWS SRA, l'autorité de certification privée racine d'ACM est hébergée dans le compte Security Tooling et peut être partagée avec l'ensemble de l'organisation AWS ou avec des comptes AWS spécifiques pour émettre des certificats d'entité finale, comme décrit précédemment dans la section relative au 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 les outils SSL/TLS 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 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 politiques AWS WAF afin de 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.

Autorité de certification privée AWS

AWS Private Certificate Authority(Autorité de certification privée AWS) 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 l'AWS SRA, Autorité de certification privée AWS il est hébergé dans le compte Security Tooling et partagé avec le compte d'application à l'aide de la RAM AWS. Cela permet aux développeurs d'un compte d'application de demander un certificat à une autorité de certification privée partagée. Le partage des autorités de certification au sein de votre organisation ou entre des comptes AWS permet de réduire le coût et la complexité liés à la création et à la gestion des autorités de certification dupliquées dans tous vos 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

L'AWS SRA utilise Amazon Inspector pour détecter et analyser automatiquement les instances EC2 et les images de conteneur qui se trouvent dans l'Amazon Elastic Container Registry (Amazon ECR) afin de détecter les vulnérabilités logicielles et les expositions involontaires sur le réseau.

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

Amazon Inspector dans les comptes membres est géré de manière centralisée par le compte d'administrateur délégué. Dans l'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'organisation AWS.

Considération de conception

- Vous pouvez utiliser Patch Manager, une fonctionnalité d'AWS Systems Manager, pour déclencher l'application de correctifs à la demande afin de corriger les failles de sécurité critiques d'Amazon Inspector, notamment les failles de sécurité « zero-day ». 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 dans AWS à l'aide d'Amazon Inspector et d'AWS Systems Manager.

Amazon Systems Manager

AWS Systems Manager est un service AWS que vous pouvez utiliser pour consulter les données opérationnelles de plusieurs services AWS et automatiser les tâches opérationnelles sur l'ensemble de vos ressources AWS. Grâce aux flux de travail d'approbation et aux runbooks automatisés, vous pouvez réduire les erreurs humaines et simplifier les tâches de maintenance et de déploiement sur les ressources AWS.

Outre ces fonctionnalités d'automatisation générales, Systems Manager prend en charge un certain nombre de fonctionnalités de sécurité préventives, détectives et réactives. L'agent AWS Systems Manager (agent SSM) est un logiciel Amazon qui peut être installé et configuré sur une instance EC2, 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.

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. L'AWS SRA utilise le Patch Manager, une fonctionnalité de Systems Manager, pour appliquer des correctifs aux instances EC2 à la fois pour les systèmes d'exploitation et les applications.

L'AWS SRA utilise également l'automatisation, une fonctionnalité de Systems Manager, pour simplifier les tâches courantes de maintenance et de déploiement des instances Amazon EC2 et des autres ressources AWS. 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'images Amazon Machine (AMI) dorées et la restauration d'instances EC2 inaccessibles. 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 instances EC2 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 d'instance EC2 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 différents services et ressources AWS tels que les messages Amazon EC2, 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. L'AWS SRA utilise des points de terminaison VPC pour que l'agent SSM établisse des chemins réseau privés vers divers 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 les régions et les groupes AWS. 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'organisation AWS. 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 les instances EC2 à grande échelle. Pour plus de détails sur la mise en œuvre, consultez la documentation de Systems Manager.

Amazon Aurora

Dans l'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 instances EC2 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 de 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 base de données et les instances de base de données Aurora, vous utilisez IAM. Pour contrôler quels appareils et instances EC2 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 s'agit de l'épine dorsale de nombreuses applications basées sur 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

L'AWS SRA illustre le modèle de distribution recommandé pour la gestion des clés, dans lequel la clé KMS réside dans le même compte AWS que la ressource à chiffrer. Pour cette raison, AWS KMS est utilisé dans le compte d'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 de conception

- Dans un modèle distribué, la responsabilité de la gestion des clés AWS KMS 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.
  - Une clé KMS a été supprimée.
  - Le taux d'échec du déchiffrement est élevé.

AWS CloudHSM

AWS CloudHSM fournit des modules de sécurité matériels gérés (HSM) dans le cloud AWS. Il vous permet de générer et d'utiliser vos propres clés de chiffrement sur AWS en utilisant des HSM validés FIPS 140-2 de niveau 3 auxquels vous contrôlez l'accès. Vous pouvez utiliser CloudHSM pour décharger le traitement SSL/TLS de vos serveurs Web. Cela réduit la charge du serveur Web et renforce la sécurité en stockant la clé privée du serveur Web dans CloudHSM. Vous pouvez également déployer un HSM depuis CloudHSM dans le VPC entrant du 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 de conception

- Si vous avez des exigences strictes en matière de norme FIPS 140-2 de niveau 3, vous pouvez également choisir de configurer AWS KMS pour utiliser le cluster CloudHSM 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 les services AWS qui chiffrent vos données, tout en étant responsable des HSM qui protègent vos clés KMS. Cela combine les HSM à locataire unique sous votre contrôle avec la facilité d'utilisation et d'intégration d'AWS KMS. Pour gérer votre infrastructure CloudHSM, vous devez utiliser une infrastructure à clé publique (PKI) et disposer d'une équipe expérimentée dans la gestion des HSM.

AWS Secrets Manager

AWS Secrets Manager vous 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 d'AWS KMS. Secrets Manager s'intègre également aux services de journalisation et de surveillance AWS pour un audit centralisé.

Secrets Manager utilise le chiffrement des enveloppes avec des clés AWS KMS 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 le compte et la région AWS, ou vous pouvez utiliser la clé gérée par AWS 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 prend actuellement en charge 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 depuis la console Secrets Manager et les appels de code vers les API de Secrets Manager. En outre, CloudTrail capture d'autres événements connexes (non liés à l'API) susceptibles d'avoir un impact sur la sécurité ou la conformité de votre 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 sources AWS, telles que la clé de chiffrement KMS ou les fonctions AWS Lambda utilisées pour la rotation des secrets. Vous pouvez également configurer Amazon EventBridge, qui reçoit les notifications de modification de configuration et de conformité d'AWS Config, pour acheminer des événements secrets particuliers à des fins de notification ou de mesures correctives.

Dans l'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 instances EC2 dans le 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 de 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 groupes 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 les JavaScript kits SDK pour Amazon Cognito afin d'ajouter des pages d'inscription et de connexion utilisateur à vos applications. Amazon Cognito Sync est un service et une bibliothèque client AWS qui permettent 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 de 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 fonction AWS Lambda, puis la déclencher lors des opérations du groupe d'utilisateurs, telles que l'inscription, la confirmation et la connexion (authentification) des utilisateurs à l'aide d'un déclencheur AWS 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 vous aider à atteindre 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 blog AWS Simplifying fine 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 blog AWS intitulé Le contrôle d'accès basé sur des politiques dans le développement d'applications avec Amazon Verified Permissions.

Dans l'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 qu'AWS met en œuvre. Prenez en compte la sécurité des instances EC2 qui constituent le cœur d'un exemple d'application simple représenté dans l'AWS SRA et vous pourrez voir comment les services AWS fonctionnent ensemble dans le cadre d'une défense à plusieurs niveaux. Cette approche s'aligne sur la vision structurelle des services de sécurité AWS, comme décrit dans la section Appliquer les services de sécurité au sein de votre organisation AWS plus haut dans ce guide.

- La couche la plus interne est constituée des instances EC2. Comme indiqué précédemment, les instances EC2 incluent de nombreuses fonctionnalités de sécurité natives par défaut ou en option. Les exemples incluent IMDSv2, le 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 instances EC2. Des services tels qu'Amazon Inspector et AWS Systems Manager vous permettent de surveiller, de signaler et de prendre des mesures correctives sur ces configurations. 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 réseau AWS. Outre les fonctionnalités de sécurité d'Amazon VPC, l'AWS SRA utilise également des points de terminaison VPC pour fournir une connectivité privée entre le VPC et les services AWS pris en

charge, et pour fournir un mécanisme permettant de placer des politiques d'accès aux limites du réseau.

- L'activité et la configuration des instances EC2, du logiciel, du réseau et des rôles et ressources IAM sont également surveillées par des services axés sur les comptes AWS tels qu'AWS Security Hub, Amazon, AWS, GuardDuty AWS CloudTrail Config, AWS IAM Access Analyzer et Amazon Macie.
- Enfin, au-delà du compte d'application, la RAM AWS 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'organisation AWS.

Présentation détaillée de l'architecture

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

Lorsque vous élaborez votre architecture de sécurité de base, comme indiqué dans la section précédente, vous pouvez vous concentrer sur des domaines fonctionnels de sécurité spécifiques et les développer davantage afin d'atteindre un niveau de maturité supérieur dans votre architecture de sécurité globale. Cette section se concentre sur deux domaines, la sécurité périmétrique et les analyses judiciaires dans le contexte de la réponse aux incidents de sécurité, et fournit un guide prescriptif approfondi sur les modèles architecturaux courants. Ce guide s'appuie sur les sections précédentes du guide de conception d'AWS SRA et renvoie aux sections pertinentes de ce guide.

Sécurité périmétrique

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

Cette section développe le guide AWS SRA afin de fournir des recommandations pour la création d'un périmètre de sécurité sur AWS. Il approfondit les services de périmètre AWS et la manière dont ils s'intègrent dans les unités d'organisation définies par l'AWS SRA.

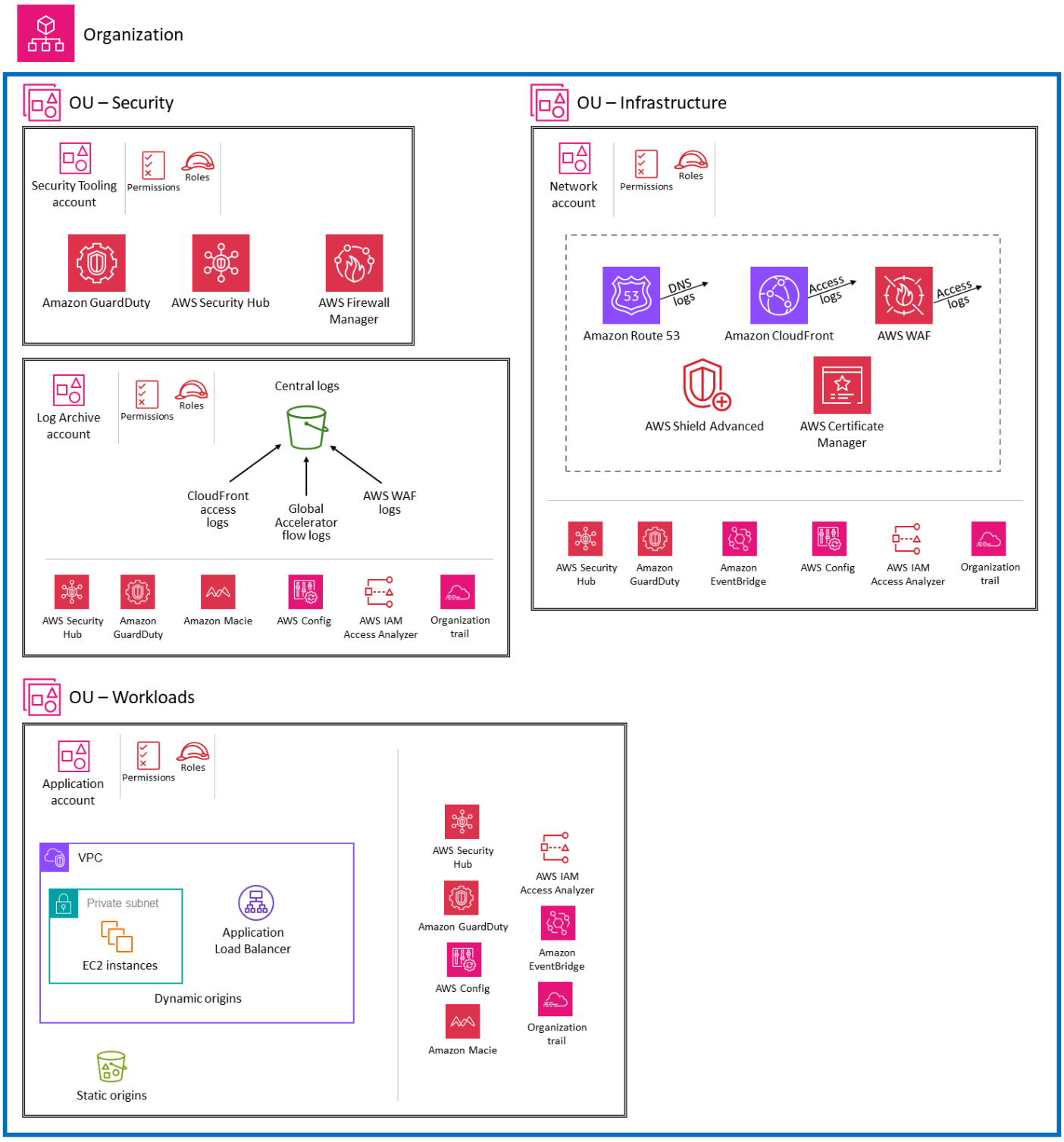
Dans le contexte de ce guide, un périmètre est défini comme la limite à laquelle vos applications se connectent à Internet. La sécurité du périmètre inclut la diffusion sécurisée du contenu, la protection de la couche d'application et l'atténuation des attaques par déni de service distribué (DDoS). Les services de périmètre AWS incluent Amazon CloudFront, AWS WAF, AWS Shield, Amazon Route 53 et AWS Global Accelerator. Ces services sont conçus pour fournir un accès sécurisé, à faible latence et à haute performance aux ressources AWS et à la diffusion de contenu. Vous pouvez utiliser ces services de périmètre avec d'autres services de sécurité tels qu'Amazon GuardDuty et AWS Firewall Manager pour vous aider à créer un périmètre sécurisé pour vos applications.

Il existe plusieurs modèles d'architecture pour la sécurité périmétrique afin de répondre aux différents besoins des organisations. Cette section se concentre sur deux modèles courants : le déploiement

des services de périmètre dans un compte central (réseau) et le déploiement de certains services de périmètre dans des comptes de charge de travail individuels (application). Cette section présente les avantages des deux architectures et leurs principales considérations.

Déploiement de services de périmètre dans un seul compte réseau

Le schéma suivant s'appuie sur l'AWS SRA de base pour illustrer l'architecture dans laquelle les services de périmètre sont déployés dans le compte réseau.



Le déploiement des services de périmètre dans un seul compte réseau présente plusieurs avantages :

- Ce modèle prend en charge des cas d'utilisation tels que les secteurs hautement réglementés, dans lesquels vous souhaitez limiter l'administration des services de périmètre au sein de votre organisation à une seule équipe spécialisée.
- Il simplifie la configuration nécessaire pour limiter la création, la modification et la suppression de composants de réseau.
- Il simplifie la détection, car l'inspection s'effectue en un seul endroit, ce qui réduit le nombre de points d'agrégation des journaux.
- Vous pouvez créer des ressources personnalisées relatives aux meilleures pratiques, telles que les stratégies CloudFront et les fonctions de périphérie, et les partager entre les distributions au sein d'un même compte.
- Il simplifie la gestion des ressources critiques sensibles aux erreurs de configuration, telles que les paramètres de cache du réseau de diffusion de contenu (CDN) ou les enregistrements DNS, en réduisant le nombre d'emplacements où ces modifications sont mises en œuvre.

Les sections suivantes abordent chaque service et les considérations architecturales.

Amazon CloudFront

Amazon CloudFront est un service de réseau de diffusion de contenu (CDN) conçu pour optimiser les performances, la sécurité et le confort des développeurs. Pour les points de terminaison HTTP publics accessibles sur Internet, nous vous recommandons d'utiliser CloudFront pour distribuer votre contenu accessible sur Internet. CloudFront est un proxy inverse qui sert de point d'entrée unique pour votre application au niveau mondial. Il peut également être associé à AWS WAF et à des fonctions périphériques telles que Lambda@Edge et les fonctions CloudFront afin de créer des solutions sécurisées et personnalisables pour la diffusion de contenu.

Dans cette architecture de déploiement, toutes les configurations CloudFront, y compris les fonctions de périphérie, sont déployées dans le compte réseau et gérées par une équipe de mise en réseau centralisée. Seuls les employés autorisés de l'équipe de mise en réseau doivent avoir accès à ce compte. Les équipes chargées des applications qui souhaitent apporter des modifications à leur configuration CloudFront ou à leur liste de contrôle d'accès Web (ACL Web) pour AWS WAF doivent en faire la demande auprès de l'équipe de mise en réseau. Nous vous recommandons d'établir un flux de travail, tel qu'un système de tickets, pour que les équipes chargées des applications puissent demander des modifications de configuration.

Dans ce modèle, les origines dynamiques et statiques sont situées dans les comptes d'application individuels. L'accès à ces origines nécessite donc des autorisations et des rôles entre comptes.

Les journaux provenant des distributions CloudFront sont configurés pour être envoyés au compte d'archivage de journaux.

AWS WAF

AWS WAF est un pare-feu d'application Web qui vous permet de surveiller les requêtes HTTP et HTTPS qui sont transmises à vos ressources d'application Web protégées. Ce service peut contribuer à protéger vos ressources contre les attaques Web courantes et les menaces volumétriques, ainsi que contre les menaces plus sophistiquées telles que la fraude liée à la création de comptes, l'accès non autorisé aux comptes d'utilisateurs et les robots qui tentent d'échapper à la détection. AWS WAF peut aider à protéger les types de ressources suivants : distributions CloudFront, API REST Amazon API Gateway, Application Load Balancers, API AWS AppSync GraphQL, groupes d'utilisateurs Amazon Cognito, services AWS App Runner et instances à accès vérifié par AWS.

Dans cette architecture de déploiement, AWS WAF est associé aux distributions CloudFront configurées dans le compte réseau. Lorsque vous configurez AWS WAF avec CloudFront, l'empreinte du périmètre est étendue aux emplacements périphériques de CloudFront au lieu du VPC de l'application. Cela permet de rapprocher le filtrage du trafic malveillant de la source de ce trafic et d'empêcher le trafic malveillant d'entrer dans votre réseau central.

Bien que les listes ACL Web soient déployées dans le compte réseau, nous vous recommandons d'utiliser AWS Firewall Manager pour gérer de manière centralisée les listes ACL Web et vous assurer que toutes les ressources sont conformes. Définissez le compte d'outils de sécurité comme compte administrateur pour Firewall Manager. Déployez des stratégies Firewall Manager avec correction automatique pour garantir que toutes les distributions CloudFront de votre compte (ou certaines d'entre elles) soient dotées d'une liste ACL Web.

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

Surveillances de l'état AWS Shield et AWS Route 53

AWS Shield Standard et AWS Shield Advanced offrent des protections contre les attaques par déni de service distribué (DDoS) pour les ressources AWS au niveau des couches réseau et transport (couches 3 et 4) et de la couche application (couche 7). Shield Standard est inclus automatiquement, sans frais supplémentaires au-delà de ce que vous avez déjà payé pour AWS WAF et vos autres services AWS. Shield Advanced offre une protection étendue contre les événements DDoS pour

vos instances Amazon EC2, les équilibreurs de charge Elastic Load Balancing, les distributions CloudFront et les zones hébergées Route 53. Si vous possédez des sites Web à haute visibilité ou si vos applications sont sujettes à des événements DDoS fréquents, pensez aux fonctionnalités supplémentaires proposées par Shield Advanced.

Cette section se concentre sur les configurations de Shield Advanced, car Shield Standard n'est pas configurable par l'utilisateur.

Pour configurer Shield Advanced afin de protéger vos distributions CloudFront, abonnez le compte réseau à Shield Advanced. Dans le compte, ajoutez l'assistance de l'équipe SRT (Shield Response Team) et accordez les autorisations nécessaires à l'équipe SRT pour accéder à vos listes ACL Web lors d'un événement DDoS. Vous pouvez contacter l'équipe SRT à tout moment pour créer et gérer des mesures d'atténuation personnalisées pour votre application lors d'un événement DDoS actif. La configuration préalable de l'accès donne à l'équipe SRT la flexibilité nécessaire pour déboguer et réviser les listes ACL Web sans avoir à gérer les autorisations lors d'un événement.

Utilisez Firewall Manager avec correction automatique pour ajouter vos distributions CloudFront en tant que ressources protégées. Si vous disposez d'autres ressources accessibles sur Internet, telles que les Application Load Balancers, vous pouvez envisager de les ajouter en tant que ressources protégées par Shield Advanced. Toutefois, si le flux de données contient plusieurs ressources protégées par Shield Advanced (par exemple, votre Application Load Balancer est à l'origine de CloudFront), nous vous recommandons de n'utiliser que le point d'entrée comme ressource protégée afin de réduire les frais de double transfert de données e, double (DTO) pour Shield Advanced.

Activez la fonctionnalité d'engagement proactif pour permettre à l'équipe SRT de surveiller de manière proactive vos ressources protégées et de vous contacter si nécessaire. Pour configurer efficacement la fonctionnalité d'engagement proactif, créez des surveillances de l'état de Route 53 pour votre application et associez-les aux distributions CloudFront. Shield Advanced utilise les surveillances de l'état comme point de données supplémentaire lorsqu'il évalue un événement. Les surveillances de l'état doivent être correctement définies afin de réduire le nombre de faux positifs lors de la détection. Pour plus d'informations sur l'identification des métriques appropriées pour les surveillances de l'état, consultez Best practices for using health checks with Shield Advanced dans la documentation AWS. Si vous détectez une tentative de DDoS, vous pouvez contacter l'équipe SRT et choisir le niveau de gravité le plus élevé disponible pour votre plan de support.

AWS Certificate Manager et AWS Route 53

AWS Certificate Manager (ACM) vous aide à allouer, gérer et renouveler les certificats X.509 SSL/TLS publics et privés. 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.

ACM est déployé dans le compte réseau afin de générer un certificat TLS public pour les distributions CloudFront. Les certificats TLS sont nécessaires pour établir une connexion HTTPS entre les utilisateurs et CloudFront. Pour plus d'informations, consultez la documentation CloudFront. ACM fournit une validation DNS ou par e-mail pour valider la propriété du domaine. Nous vous recommandons d'utiliser la validation DNS plutôt que la validation par e-mail, car en utilisant Route 53 pour gérer vos enregistrements DNS publics, vous pouvez mettre à jour vos enregistrements directement via ACM. ACM renouvelle automatiquement les certificats qui ont fait l'objet d'une validation DNS tant que le certificat est utilisé et que l'enregistrement DNS est en place.

Journaux d'accès CloudFront et journaux AWS WAF

Par défaut, les journaux d'accès CloudFront sont stockés dans le compte réseau et les journaux AWS WAF sont regroupés dans le compte d'outils de sécurité à l'aide de l'option de journalisation Firewall Manager. Nous vous recommandons de répliquer ces journaux dans le compte d'archivage des journaux afin que les équipes de sécurité centralisées puissent y accéder à des fins de surveillance.

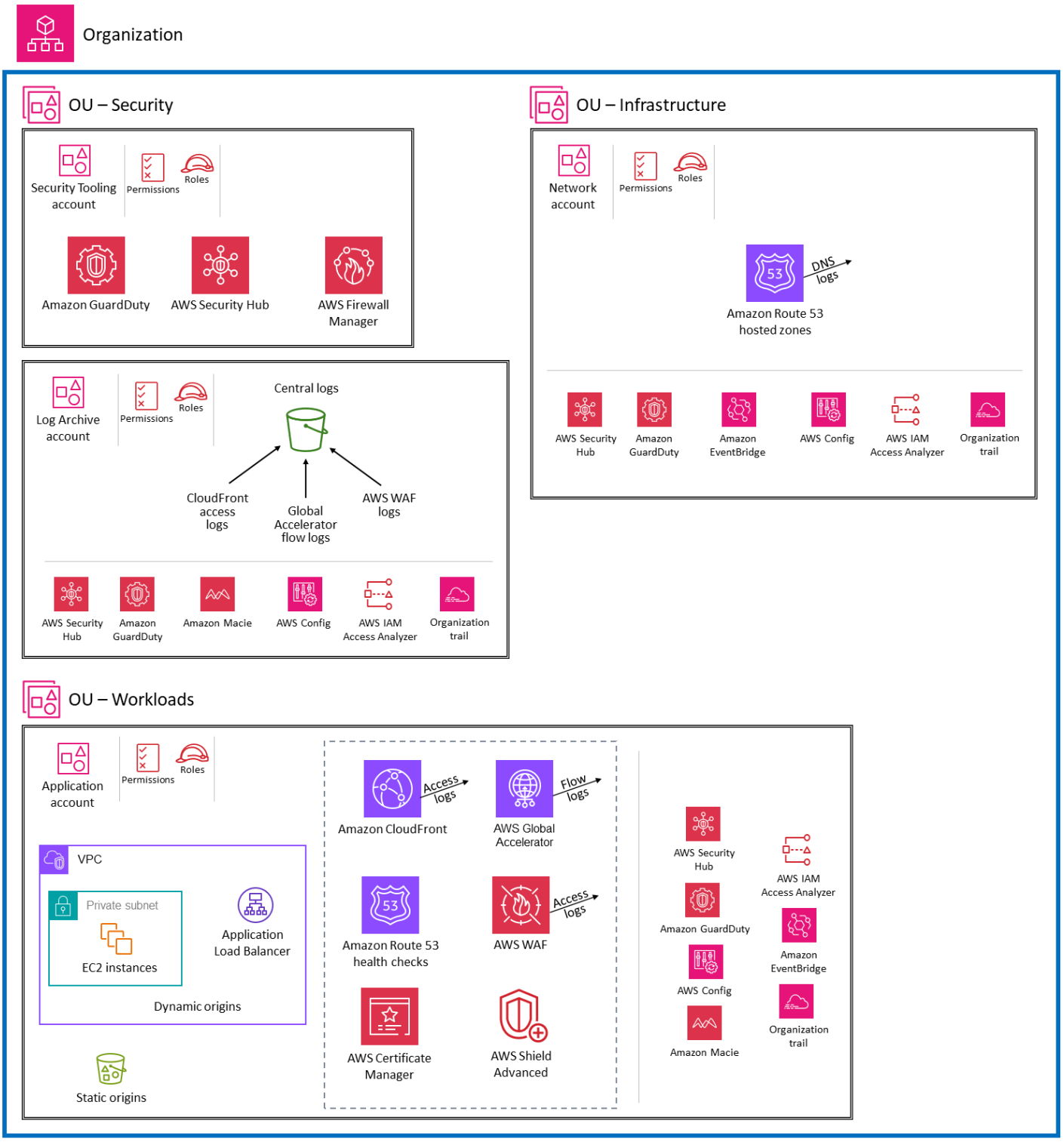
Considérations relatives à la conception

- Dans cette architecture, le grand nombre de dépendances à l'égard d'une seule équipe réseau peut affecter votre capacité à apporter des modifications rapidement.
- Surveillez les quotas de service pour chaque compte. Les quotas de service, également appelés limites, représentent le nombre maximal de ressources ou d'opérations de service pour votre compte AWS. Pour plus d'informations, consultez AWS service quotas dans la documentation AWS.
- Fournir des métriques spécifiques aux équipes responsables de la charge de travail peut s'avérer complexe.
- Les équipes chargées des applications ont un accès limité aux configurations, ce qui peut entraîner une surcharge de travail en attendant que les équipes chargées des réseaux mettent en œuvre les changements en leur nom.
- Les équipes qui partagent les ressources d'un même compte peuvent se disputer les mêmes ressources et les mêmes budgets, ce qui peut entraîner des problèmes d'affectation des ressources. Nous vous recommandons de mettre en place des

mécanismes de remboursement par les équipes d'application qui utilisent les services de périmètre déployés dans le compte de mise en réseau.

Déploiement de services de périmètre dans des comptes d'applications individuels

Le schéma suivant illustre le modèle d'architecture dans lequel les services de périmètre sont déployés et gérés indépendamment dans des comptes d'application individuels.



Le déploiement des services de périmètre dans les comptes d'applications présente plusieurs avantages :

- Cette conception permet aux comptes de charge de travail individuels de personnaliser les configurations de service en fonction de leurs besoins. Cette approche supprime la dépendance à l'égard d'une équipe spécialisée pour mettre en œuvre les modifications apportées aux ressources d'un compte partagé, et permet aux développeurs de chaque équipe de gérer les configurations de manière indépendante.
- Chaque compte possède ses propres quotas de service, de sorte que les propriétaires d'applications n'ont pas à respecter les quotas d'un compte partagé.
- Cette conception permet de contenir l'impact des activités malveillantes en les limitant à un compte particulier et en empêchant l'attaque de se propager à d'autres charges de travail.
- Cela élimine les risques liés au changement, car l'impact est limité à la charge de travail en question. Vous pouvez également utiliser l'IAM pour limiter le nombre d'équipes habilitées à mettre en œuvre des changements, afin d'établir une séparation logique entre les équipes chargées de la charge de travail et l'équipe de mise en réseau centrale.
- En décentralisant la mise en œuvre des entrées et sorties du réseau, tout en disposant de contrôles logiques communs (en utilisant des services tels qu'AWS Firewall Manager), vous pouvez ajuster les contrôles du réseau à des charges de travail spécifiques tout en continuant à respecter une norme minimale d'objectifs de contrôle.

Les sections suivantes abordent chaque service et les considérations architecturales.

Amazon CloudFront

Dans cette architecture de déploiement, les configurations Amazon CloudFront, y compris les fonctions de périphérie, sont gérées et déployées dans les comptes d'applications individuels. Cela permet de vérifier que chaque propriétaire d'application et chaque compte de charge de travail disposent de l'autonomie nécessaire pour configurer les services de périmètre en fonction des besoins de leur application.

Les origines dynamiques et statiques se trouvent dans le même compte d'application, et les distributions CloudFront ont un accès à ces origines au niveau du compte. Les journaux des distributions CloudFront sont stockés localement dans chaque compte d'application. Les journaux peuvent être répliqués sur le compte d'archivage des journaux pour répondre aux besoins de conformité et de réglementation.

AWS WAF

Dans cette architecture de déploiement, AWS WAF est associé aux distributions CloudFront configurées dans le compte d'application. Comme pour le modèle précédent, nous vous recommandons d'utiliser AWS Firewall Manager pour gérer de manière centralisée les listes ACL Web et vous assurer que toutes les ressources sont conformes. Les règles AWS WAF courantes, telles que le groupe de règle de base géré par AWS et la liste de réputation d'adresses IP Amazon, doivent être ajoutées par défaut. Ces règles sont automatiquement appliquées à toute ressource éligible dans le compte de l'application.

Outre les règles appliquées par Firewall Manager, chaque propriétaire d'application peut ajouter à la liste ACL Web des règles AWS WAF pertinentes pour la sécurité de son application. Cela permet une certaine flexibilité dans chaque compte d'application tout en conservant le contrôle global du compte d'outils de sécurité.

Utilisez l'option de journalisation de Firewall Manager pour centraliser les journaux et les envoyer vers un compartiment S3 du compte d'outils de sécurité. Chaque équipe d'application a accès aux tableaux de bord AWS WAF pour son application. Vous pouvez configurer le tableau de bord à l'aide d'un service tel qu'Amazon QuickSight. Si de faux positifs sont identifiés ou si d'autres mises à jour des règles AWS WAF sont nécessaires, vous pouvez ajouter des règles AWS WAF au niveau de l'application à la liste ACL Web déployée par Firewall Manager. Les journaux sont répliqués sur le compte d'archivage des journaux et archivés pour les investigations de sécurité.

AWS Global Accelerator

AWS Global Accelerator vous permet de créer des accélérateurs afin d'améliorer les performances de vos applications pour les utilisateurs locaux et internationaux. Global Accelerator vous fournit des adresses IP statiques qui servent de points d'entrée fixes à vos applications hébergées dans une ou plusieurs Régions AWS. Vous pouvez associer ces adresses aux ressources ou points de terminaison AWS régionaux, tels que les Application Load Balancers, les Network Load Balancers, les instances EC2 et les adresses IP Elastic. Cela permet au trafic d'entrer dans le réseau mondial AWS aussi près que possible de vos utilisateurs.

Global Accelerator ne prend actuellement pas en charge les origines entre comptes. Par conséquent, il est déployé sur le même compte que le point de terminaison d'origine. Déployez les accélérateurs dans chaque compte d'application et ajoutez-les en tant que ressources protégées pour AWS Shield Advanced dans le même compte. Les mesures d'atténuation de Shield Advanced ne permettent qu'au trafic valide d'atteindre les points de terminaison d'écouteur de Global Accelerator.

Surveillances de l'état AWS Shield Advanced et AWS Route 53

Pour configurer AWS Shield Advanced afin de protéger vos distributions CloudFront, vous devez abonner chaque compte d'application à Shield Advanced. Vous devez configurer des fonctionnalités telles que l'accès à l'équipe SRT (Shield Response Time) et l'engagement proactif au niveau du compte, car elles doivent être configurées dans le même compte que la ressource. Utilisez Firewall Manager avec correction automatique pour ajouter vos distributions CloudFront en tant que ressources protégées, et appliquez la stratégie à chaque compte. Les surveillances de l'état Route 53 pour chaque distribution CloudFront doivent être déployées dans le même compte et associées à la ressource.

Zones Amazon Route 53 et ACM

Lorsque vous utilisez des services tels qu'Amazon CloudFront, les comptes d'application doivent avoir accès au compte qui héberge le domaine racine afin de créer des sous-domaines personnalisés et d'appliquer des certificats émis par Amazon Certificate Manager (ACM) ou un certificat tiers. Vous pouvez déléguer un domaine public du compte de services partagés central à des comptes d'application individuels en utilisant la délégation de zone Amazon Route 53. La délégation de zone permet à chaque compte de créer et de gérer des sous-domaines spécifiques à une application, tels que des API ou des sous-domaines statiques. L'ACM de chaque compte permet à chaque compte d'application de gérer les processus d'approbation et de vérification des certificats (validation de l'organisation, validation étendue ou validation du domaine) en fonction de ses besoins.

Journaux d'accès CloudFront, journaux de flux Global Accelerator et journaux AWS WAF

Dans ce modèle, nous configurons les journaux d'accès CloudFront et les journaux de flux Global Accelerator dans les compartiments S3 des comptes d'application individuels. Les développeurs qui souhaitent analyser les journaux pour améliorer les performances ou réduire les faux positifs auront un accès direct à ces journaux sans avoir à demander l'accès à une archive de journaux centrale. Les journaux stockés localement peuvent également répondre aux exigences de conformité régionales telles que la résidence des données ou le masquage des données d'identification personnelle.

Les journaux AWS WAF complets sont stockés dans les compartiments S3 du compte d'archivage de journaux à l'aide de la journalisation Firewall Manager. Les équipes chargées des applications peuvent consulter les journaux en utilisant des tableaux de bord configurés à l'aide d'un service tel qu'Amazon QuickSight. En outre, chaque équipe chargée des applications a accès aux journaux AWS WAF échantillonnés depuis son propre compte pour un débogage rapide.

Nous vous recommandons de répliquer les journaux dans un lac de données centralisé situé dans le compte d'archivage de journaux. L'agrégation des journaux dans un lac de données centralisé vous donne une vue complète de l'ensemble du trafic vers vos ressources et distributions AWS WAF. Cela permet aux équipes de sécurité d'analyser et de répondre de manière centralisée aux modèles de menaces de sécurité globales.

Considérations relatives à la conception

- Ce modèle transfère la responsabilité de l'administration du réseau et de la sécurité aux propriétaires de comptes et aux développeurs, ce qui peut alourdir le processus de développement.
- Il peut y avoir des incohérences dans la prise de décisions. Vous devez mettre en place des communications, des modèles et des formations efficaces pour vous assurer que les services sont configurés correctement et suivent les recommandations de sécurité.
- Il existe une dépendance à l'égard de l'automatisation et des attentes claires à l'égard des contrôles de sécurité de base combinés aux contrôles spécifiques à l'application.
- Utilisez des services tels que Firewall Manager et AWS Config pour vous assurer que l'architecture déployée est conforme aux meilleures pratiques de sécurité. Configurez également la surveillance d'AWS CloudTrail pour détecter toute erreur de configuration.
- L'agrégation des journaux et des métriques en un lieu central à des fins d'analyse peut s'avérer complexe.

Services AWS supplémentaires pour les configurations de sécurité périmétrique

Origines dynamiques : Application Load Balancers

Vous pouvez configurer Amazon CloudFront pour utiliser les origines d'Application Load Balancer pour la diffusion de contenu dynamique. Cette configuration vous permet d'acheminer les demandes vers différentes origines d'Application Load Balancer en fonction de divers facteurs tels que le chemin de la demande, le nom d'hôte ou les paramètres de chaîne de requête.

Les origines d'Application Load Balancer sont déployées dans le compte d'application. Si vos distributions CloudFront se trouvent dans le compte réseau, vous devez configurer des autorisations entre comptes pour que la distribution CloudFront puisse accéder à l'origine de l'Application Load

Balancer. Les journaux de l'Application Load Balancer sont envoyés au compte d'archivage de journaux.

Pour empêcher les utilisateurs d'accéder directement à un Application Load Balancer sans passer par CloudFront, suivez ces étapes de haut niveau :

- Configurez CloudFront pour ajouter un en-tête HTTP personnalisé aux demandes qu'il envoie à l'Application Load Balancer et configurez l'Application Load Balancer pour transférer uniquement les demandes contenant l'en-tête personnalisé.
- Utilisez une liste de préfixes gérée par AWS pour CloudFront à partir du groupe de sécurité Application Load Balancer. Cela limite le trafic HTTP/HTTPS entrant dans votre Application Load Balancer aux seules adresses IP appartenant aux serveurs orientés vers l'origine de CloudFront.

Pour plus d'informations, consultez Restriction de l'accès aux Application Load Balancers dans la documentation CloudFront.

Origines statiques : Amazon S3 et AWS Elemental MediaStore

Vous pouvez configurer CloudFront pour utiliser les origines d'Amazon S3 ou d'AWS Elemental MediaStore pour la diffusion de contenu statique. Ces origines sont déployées dans le compte d'application. Si vos distributions CloudFront se trouvent dans le compte réseau, vous devez configurer des autorisations entre comptes pour la distribution CloudFront dans le compte réseau afin d'accéder aux origines.

Pour vérifier que vos points de terminaison d'origine statiques ne sont accessibles que via CloudFront et non directement via l'Internet public, vous pouvez utiliser des configurations de contrôle d'accès d'origine (OAC). Pour plus d'informations sur les restrictions d'accès, consultez Restriction de l'accès à l'origine Amazon S3 et Restriction de l'accès à une origine MediaStore dans la documentation CloudFront.

AWS Firewall Manager

AWS Firewall Manager simplifie les tâches d'administration et de maintenance sur de multiples comptes et ressources, notamment AWS WAF, AWS Shield Advanced, les groupes de sécurité Amazon VPC, AWS Network Firewall et Amazon Route 53 Resolver DNS Firewall, pour une variété de protections.

Déléguez le compte d'outils de sécurité en tant que compte administrateur par défaut de Firewall Manager et utilisez-le pour gérer de manière centralisée les règles AWS WAF et les protections

Shield Advanced au sein des comptes de votre organisation. Utilisez Firewall Manager pour gérer de manière centralisée les règles AWS WAF communes tout en donnant à chaque équipe chargée des applications la flexibilité d'ajouter des règles spécifiques à l'application à la liste ACL Web. Cela permet d'appliquer les stratégies de sécurité à l'échelle de l'organisation, telles que la protection contre les vulnérabilités courantes, tout en permettant aux équipes chargées des applications d'ajouter des règles AWS WAF spécifiques à leur application.

Utilisez la journalisation de Firewall Manager pour centraliser les journaux AWS WAF dans un compartiment S3 du compte d'outils de sécurité, puis répliquez les journaux sur le compte d'archivage de journaux afin de pouvoir les archiver pour des investigations de sécurité. En outre, intégrez Firewall Manager à AWS Security Hub pour visualiser de manière centralisée les détails de configuration et les notifications DDoS dans Security Hub.

Pour des recommandations supplémentaires, consultez AWS Firewall Manager dans la section Compte d'outils de sécurité de ce guide.

AWS Security Hub

L'intégration entre Firewall Manager et Security Hub envoie quatre types de résultats à Security Hub :

- Les ressources qui ne sont pas correctement protégées par les règles AWS WAF
- Les ressources qui ne sont pas correctement protégées par AWS Shield Advanced
- Les résultats de Shield Advanced qui indiquent qu'une attaque DDoS est en cours
- Les groupes de sécurité utilisés de manière incorrecte

Ces résultats provenant de tous les comptes des membres de l'organisation sont regroupés dans le compte de l'administrateur délégué du Security Hub (outils de sécurité). Le compte d'outils de sécurité regroupe, organise et hiérarchise vos alertes de sécurité ou résultats en un seul endroit. Utilisez les règles Amazon CloudWatch Events pour envoyer les résultats aux systèmes de billetterie ou créer des solutions automatiques telles que le blocage de plages d'adresses IP malveillantes.

Pour des recommandations supplémentaires, consultez AWS Security Hub dans la section Compte d'outils de sécurité de ce guide.

Amazon GuardDuty

Vous pouvez utiliser les renseignements sur les menaces fournies par Amazon GuardDuty pour mettre à jour automatiquement les listes ACL Web en réponse aux résultats de GuardDuty. Par

exemple, si GuardDuty détecte une activité suspecte, l'automatisation peut être utilisée pour mettre à jour l'entrée dans les ensembles d'adresses IP AWS WAF et appliquer les listes ACL Web AWS WAF aux ressources concernées afin de bloquer les communications en provenance de l'hôte suspect pendant que vous procédez à des investigations supplémentaires et à des mesures correctives. Le compte d'outils de sécurité est le compte administrateur délégué de GuardDuty. Par conséquent, vous devez utiliser une fonction AWS Lambda avec des autorisations entre comptes pour mettre à jour les ensembles d'adresses IP AWS WAF dans le compte d'application.

Pour des recommandations supplémentaires, consultez Amazon GuardDuty dans la section Compte d'outils de sécurité de ce guide.

AWS Config

AWS Config est un prérequis pour Firewall Manager et est déployé dans les comptes AWS, y compris le compte réseau et le compte d'application. En outre, utilisez les règles AWS Config pour vérifier que les ressources déployées sont conformes aux meilleures pratiques de sécurité. Par exemple, vous pouvez utiliser une règle AWS Config pour vérifier si chaque distribution CloudFront est associée à une liste ACL Web, ou obliger toutes les distributions CloudFront soient configurées pour fournir des journaux d'accès à un compartiment S3.

Pour des recommandations générales, consultez AWS Config dans la section Compte d'outils de sécurité de ce guide.

Informatique légale

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

Dans le contexte de l'AWS SRA, nous utilisons la définition suivante des analyses judiciaires fournie par le National Institute of Standards and Technology (NIST) : « l'application de la science à l'identification, à la collecte, à l'examen et à l'analyse des données tout en préservant l'intégrité des informations et en maintenant une chaîne de contrôle stricte pour les données » (source : NIST Special Publication 800-86 – Guide to Integrating Forensic Techniques into Incident Response).

Les analyses judiciaires dans le contexte de la réponse aux incidents de sécurité

Les conseils en matière de réponse aux incidents (RI) présentés dans cette section ne sont fournis que dans le contexte de l'analyse judiciaire et de la manière dont les différents services et solutions peuvent améliorer le processus de RI.

Le Guide de réponse aux incidents de sécurité AWS répertorie les meilleures pratiques pour répondre aux incidents de sécurité dans le Cloud AWS, sur la base de l'expérience de l'équipe de réponse aux incidents des clients AWS (AWS CIRT). Pour obtenir des conseils supplémentaires de la part de l'équipe AWS CIRT, consultez les ateliers AWS CIRT et les leçons de l'AWS CIRT.

Le cadre de cybersécurité du National Institute of Standards and Technology (NIST CSF) définit quatre étapes dans le cycle de vie des RI : préparation ; détection et analyse ; confinement, éradication et restauration ; et activité post-incident. Ces étapes peuvent être mises en œuvre de manière séquentielle. Cependant, cette séquence est souvent cyclique, car certaines étapes doivent être répétées après le passage à l'étape suivante du cycle. Par exemple, après le confinement et l'éradication, vous devez effectuer une nouvelle analyse pour confirmer que vous avez réussi à éliminer l'adversaire de l'environnement.

Ce cycle répété d'analyse, de confinement, d'éradication et de retour à l'analyse vous permet de recueillir davantage d'informations chaque fois que de nouveaux indicateurs de compromission (IoC) sont détectés. Ces IoC sont utiles à plusieurs égards. Ils vous décrivent les étapes suivies par l'adversaire pour compromettre votre environnement. En outre, en effectuant un examen approprié après l'incident, vous pouvez améliorer vos défenses et vos détections afin de prévenir l'incident à l'avenir ou de détecter les actions de l'adversaire plus rapidement et de réduire ainsi l'impact de l'incident.

Bien que ce processus de RI ne soit pas l'objectif principal des analyses judiciaires, de nombreux outils, techniques et meilleures pratiques sont partagés avec la RI (en particulier l'étape d'analyse). Par exemple, après la détection d'un incident, le processus de collecte judiciaire permet de recueillir les preuves. Ensuite, l'examen et l'analyse des preuves peuvent aider à extraire les IoC. Enfin, les rapports judiciaires peuvent contribuer aux activités postérieures à la RI.

Nous vous recommandons d'automatiser autant que possible le processus d'analyse judiciaire afin d'accélérer la réponse et de réduire la charge de travail des parties prenantes de la RI. En outre, vous pouvez ajouter d'autres analyses automatisées une fois que le processus de collecte judiciaire est terminé et que les preuves ont été stockées en toute sécurité afin d'éviter toute contamination.

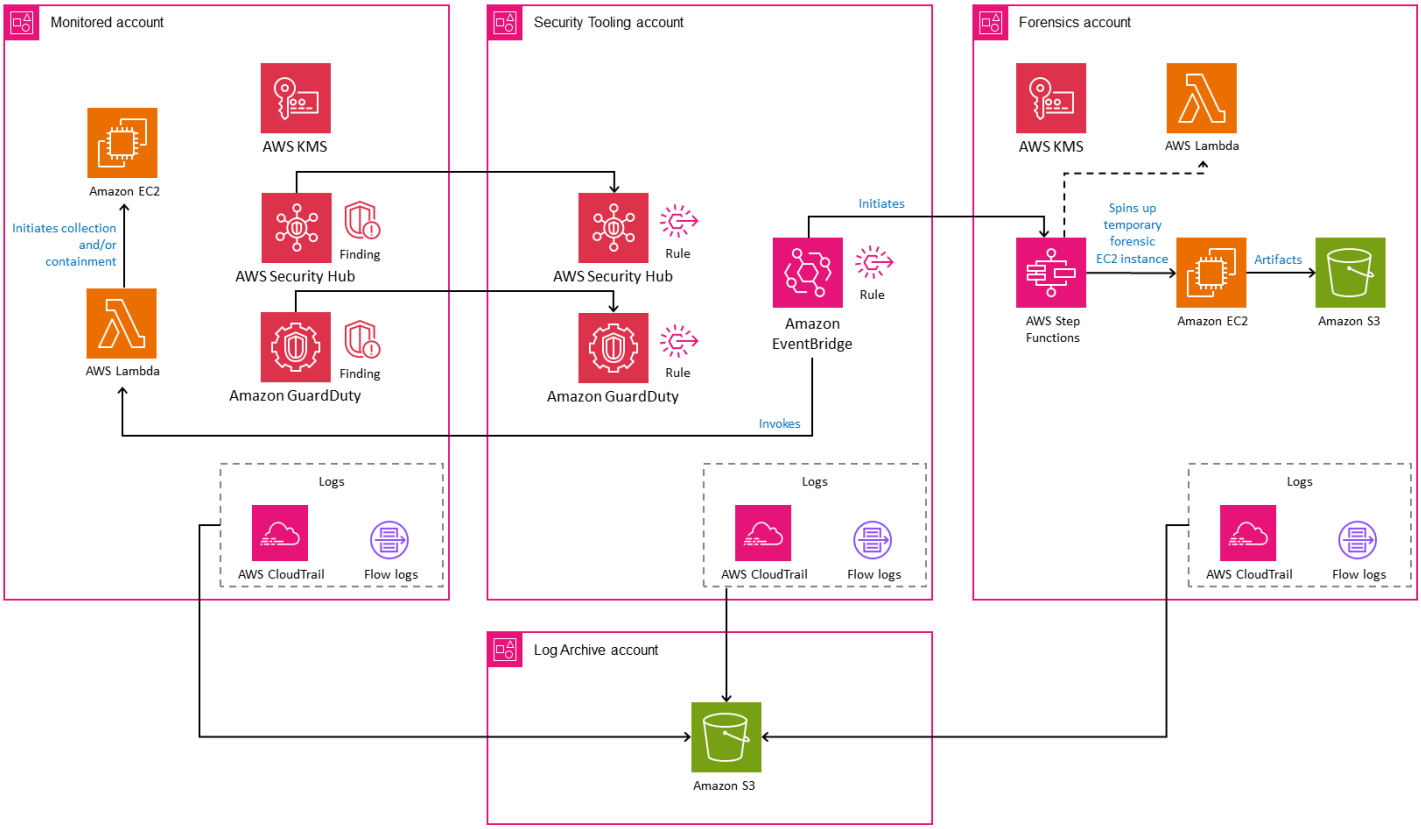
Pour plus d'informations, consultez le modèle Automatiser la réponse aux incidents et les analyses judiciaires sur le site Web des recommandations AWS.

> **Considérations relatives à la conception**
>
> Pour améliorer votre préparation en matière de sécurité RI :
>
> - Activez et stockez en toute sécurité les journaux qui pourraient être nécessaires lors d'une enquête ou d'une réponse à un incident.
> - Prégénérez des requêtes pour des scénarios connus et fournissez des méthodes automatisées de recherche dans les journaux. Envisagez d'utiliser Amazon Detective.
> - Préparez votre outil de RI en effectuant des simulations.
> - Testez régulièrement les processus de sauvegarde et de restauration pour vous assurer qu'ils sont efficaces.
> - Utilisez des manuels basés sur des scénarios, en commençant par les événements potentiels courants liés à AWS, sur la base des résultats d'Amazon GuardDuty. Pour plus d'informations sur la création de vos propres manuels, consultez la section Playbook resources du Guide de réponse aux incidents de sécurité AWS.

Compte d'analyses judiciaires

> **Exclusion de responsabilité**
>
> La description suivante d'un compte d'analyses judiciaires AWS ne doit être utilisée par les organisations que comme point de départ pour développer leurs propres capacités d'analyses judiciaires, en conjonction avec les conseils de leurs conseillers juridiques.
> Nous ne prétendons pas que ce guide soit adapté à la détection ou à l'enquête criminelle ni que les données ou les preuves judiciaires obtenues grâce à l'application de ce guide puissent être utilisées devant un tribunal. Vous devez évaluer de manière indépendante si les meilleures pratiques décrites ici conviennent à votre cas d'utilisation.

Le schéma suivant illustre les services de sécurité AWS qui peuvent être configurés dans un compte d'analyses judiciaires dédié. À des fins de contexte, le schéma montre le compte d'outils de sécurité pour illustrer les services AWS utilisés pour effectuer des détections ou des notifications dans le compte d'analyses judiciaires.



Le compte d'analyses judiciaires est un type distinct et dédié de compte d'outils de sécurité intégré à l'unité d'organisation de sécurité. L'objectif du compte d'analyses judiciaires est de fournir une salle blanche standard, préconfigurée et reproductible pour permettre à l'équipe d'analyses judiciaires d'une organisation de mettre en œuvre toutes les phases du processus d'analyses judiciaires : la collecte, l'examen, l'analyse et l'établissement de rapports. En outre, le processus de quarantaine et d'isolement des ressources concernées est également inclus dans ce compte.

Le fait de regrouper l'ensemble du processus d'analyses judiciaires dans un compte distinct vous permet d'appliquer des contrôles d'accès supplémentaires aux données judiciaires collectées et stockées. Nous vous recommandons de séparer les comptes d'analyses judiciaires et d'outils de sécurité pour les raisons suivantes :

- Les ressources d'analyses judiciaires et de sécurité peuvent appartenir à des équipes différentes ou avoir des autorisations différentes.
- Le compte d'outils de sécurité peut être doté d'une automatisation axée sur la réponse aux événements de sécurité sur le plan de contrôle AWS, tels que l'activation du blocage de l'accès public Amazon S3 pour les compartiments S3, tandis que le compte d'analyses judiciaires inclut également des artefacts du plan de données AWS dont le client peut être responsable, tels que le

système d'exploitation (OS) ou les données spécifiques à une application au sein d'une instance EC2.

- Il se peut que vous deviez mettre en place des restrictions d'accès supplémentaires ou des conservations légales en fonction de vos exigences organisationnelles ou réglementaires.
- Le processus d'analyse judiciaire peut nécessiter l'analyse de codes malveillants tels que des logiciels malveillants dans un environnement sécurisé, conformément aux conditions d'utilisation d'AWS.

Le compte d'analyses judiciaires devrait inclure l'automatisation afin d'accélérer la collecte de preuves à grande échelle tout en minimisant l'interaction humaine dans le processus de collecte judiciaire. L'automatisation de la réponse et de la mise en quarantaine des ressources serait également incluse dans ce compte afin de simplifier les mécanismes de suivi et d'établissement de rapports.

Les fonctionnalités judiciaires décrites dans cette section doivent être déployées dans toutes les Régions AWS disponibles, même si votre organisation ne les utilise pas activement. Si vous ne prévoyez pas d'utiliser des Régions AWS spécifiques, vous devez appliquer une politique de contrôle des services (SCP) afin de limiter le provisionnement des ressources AWS. En outre, le maintien des enquêtes et du stockage des artefacts judiciaires au sein d'une même région permet d'éviter les problèmes liés à l'évolution du paysage réglementaire en matière de résidence et de propriété des données.

Ce guide utilise le compte d'archivage de journaux comme indiqué précédemment pour enregistrer les actions entreprises dans l'environnement via les API AWS, y compris les API que vous exécutez dans le compte d'analyses judiciaires. Le fait de disposer de tels journaux permet d'éviter les allégations de mauvaise manipulation ou d'altération des artefacts. Selon le niveau de détail que vous activez (voir Journalisation des événements de gestion et Journalisation des événements de données dans la documentation AWS CloudTrail), les journaux peuvent inclure des informations sur le compte utilisé pour collecter les artefacts, l'heure à laquelle les artefacts ont été collectés et les mesures prises pour collecter les données. En stockant les artefacts dans Amazon S3, vous pouvez également utiliser des contrôles d'accès avancés et enregistrer des informations sur les personnes qui ont eu accès aux objets. Un journal détaillé des actions permet aux autres utilisateurs de répéter le processus ultérieurement si nécessaire (en supposant que les ressources concernées soient toujours disponibles).

Considérations relatives à la conception

- L'automatisation est utile lorsque vous êtes confronté à de nombreux incidents simultanés, car elle permet d'accélérer et de mettre à l'échelle la collecte de preuves essentielles. Toutefois, il convient d'examiner attentivement ces avantages. Par exemple, en cas d'incident faux positif, une réponse judiciaire entièrement automatisée pourrait avoir un impact négatif sur un processus métier pris en charge par une charge de travail AWS dans le champ d'application. Pour plus d'informations, consultez les considérations de conception pour AWS GuardDuty, AWS Security Hub et AWS Step Functions dans les sections suivantes.
- Nous recommandons des comptes d'outils de sécurité et d'analyses judiciaires distincts, même si les ressources judiciaires et de sécurité de votre organisation appartiennent à la même équipe et que toutes les fonctions peuvent être exécutées par n'importe quel membre de l'équipe. La division des fonctions en comptes distincts permet de renforcer le principe du moindre privilège, d'éviter la contamination par une analyse permanente des événements de sécurité et contribue à garantir l'intégrité des artefacts recueillis.
- Vous pouvez créer une unité d'organisation d'analyses judiciaires distincte pour héberger ce compte si vous souhaitez mettre davantage l'accent sur la séparation des tâches, le moindre privilège et les barrières de protection restrictives.
- Si votre organisation utilise des ressources d'infrastructure immuables, des informations ayant une valeur légale peuvent être perdues si une ressource est automatiquement supprimée (par exemple, lors d'un événement de réduction) et avant qu'un incident de sécurité n'est détecté. Pour éviter cela, envisagez d'exécuter un processus de collecte judiciaire pour chacune de ces ressources. Pour réduire le volume de données collectées, vous pouvez prendre en compte des facteurs tels que les environnements, la criticité de l'activité de la charge de travail, le type de données traitées, etc.
- Envisagez d'utiliser Amazon WorkSpaces pour créer des postes de travail propres. Cela peut aider à distinguer les actions des parties prenantes au cours d'une investigation.

Amazon GuardDuty

Amazon GuardDuty est un service de détection qui surveille en permanence les activités malveillantes et les comportements non autorisés pour protéger vos comptes AWS et vos charges

de travail. Pour obtenir des conseils généraux sur AWS SRA, consultez Amazon GuardDuty dans la section Comptes d'outils de sécurité.

Vous pouvez utiliser les résultats de GuardDuty pour lancer le flux de travail judiciaire qui capture des images de disque et de mémoire des instances EC2 potentiellement compromises. Cela réduit les interactions humaines et peut augmenter considérablement la vitesse de collecte des données judiciaires. Vous pouvez intégrer GuardDuty à Amazon EventBridge pour automatiser les réponses aux nouveaux résultats de GuardDuty.

La liste des types de résultats GuardDuty s'allonge. Vous devez déterminer quels types de résultats (par exemple, Amazon EC2, Amazon EKS, protection contre les programmes malveillants, etc.) doivent lancer le flux de travail judiciaire.

Vous pouvez entièrement automatiser l'intégration du processus de confinement et de collecte de données judiciaires avec les résultats de GuardDuty afin de capturer l'investigation des artefacts de disque et de mémoire et de mettre en quarantaine les instances EC2. Par exemple, si toutes les règles d'entrée et de sortie sont supprimées d'un groupe de sécurité, vous pouvez appliquer une liste ACL réseau pour interrompre la connexion existante et attacher une politique IAM pour refuser toutes les demandes.

Considérations relatives à la conception

- En fonction du service AWS, la responsabilité partagée du client peut varier. Par exemple, la capture de données volatiles sur les instances EC2 n'est possible que sur l'instance elle-même et peut inclure des données précieuses pouvant être utilisées comme preuves judiciaires. À l'inverse, la réponse et l'investigation d'un résultat concernant Amazon S3 impliquent principalement les données CloudTrail ou les journaux d'accès Amazon S3. L'automatisation des réponses doit être organisée à la fois entre les comptes d'outils de sécurité et d'analyses judiciaires en fonction de la responsabilité partagée du client, du flux de processus général et des artefacts capturés qui doivent être sécurisés.
- Avant de mettre en quarantaine une instance EC2, évaluez son impact commercial global et sa criticité. Envisagez d'établir un processus dans lequel les parties prenantes appropriées sont consultées avant d'utiliser l'automatisation pour contenir l'instance EC2.

AWS Security Hub

AWS Security Hub vous offre une vue complète de votre posture de sécurité sur AWS et vous permet de vérifier votre environnement par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Security Hub collecte des données de sécurité à partir des services intégrés AWS, des 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. Pour obtenir des conseils généraux sur AWS SRA, consultez AWS Security Hub dans la section relative Comptes d'outils de sécurité.

En plus de surveiller votre posture de sécurité, Security Hub prend en charge l'intégration avec Amazon EventBridge afin d'automatiser la correction de résultats spécifiques. Par exemple, vous pouvez définir des actions personnalisées qui peuvent être programmées pour exécuter une fonction AWS Lambda ou un flux de travail AWS Step Functions afin de mettre en œuvre un processus d'investigation.

Les actions personnalisées du Security Hub fournissent un mécanisme standardisé permettant aux analystes ou aux ressources de sécurité autorisés de mettre en œuvre l'automatisation du confinement et des analyses judiciaires. Cela réduit les interactions humaines lors du confinement et de la capture des preuves judiciaires. Vous pouvez ajouter un point de contrôle manuel dans le processus automatisé pour confirmer qu'une collecte judiciaire est effectivement nécessaire.

Considération relative à la conception

- Security Hub peut être intégré à de nombreux services, notamment aux solutions de partenaires AWS. Si votre organisation utilise des contrôles de sécurité de détection qui ne sont pas totalement ajustés et qui donnent parfois lieu à des alertes faussement positives, l'automatisation complète du processus de collecte judiciaire entraînerait l'exécution de ce processus inutilement.

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. Pour obtenir des conseils généraux sur AWS SRA, consultez Amazon EventBridge dans la section Comptes d'outils de sécurité.

Par exemple, vous pouvez utiliser EventBridge comme mécanisme pour lancer un flux de travail judiciaire dans Step Functions afin de capturer des images de disque et de mémoire en fonction des détections d'outils de surveillance de la sécurité tels que GuardDuty. Vous pouvez également l'utiliser de manière plus manuelle : EventBridge peut détecter les événements de modification des balises dans CloudTrail, ce qui pourrait lancer le flux de travail d'investigation dans Step Functions.

AWS Step Functions

AWS Step Functions est un service d'orchestration sans serveur que vous pouvez intégrer avec des fonctions AWS Lambda et d'autres services AWS afin de créer des applications métier essentielles. Sur la console graphique Step Functions, vous voyez le flux de travail de votre application comme une série d'étapes pilotées par des événements. Step Functions repose sur les machines d'état et les tâches. Dans Step Functions, un flux de travail est appelé une machine d'état, qui est une série d'étapes pilotées par des événements. Chaque étape d'un flux de travail est appelée un état. Un état de tâche représente une unité de travail exécutée par un autre service AWS, tel que Lambda. Un état de tâche peut appeler n'importe quel service ou API AWS. Vous pouvez utiliser les commandes intégrées dans Step Functions pour examiner l'état de chaque étape de votre flux de travail afin de vous assurer que chaque étape s'exécute dans le bon ordre et comme prévu. Selon votre cas d'utilisation, vous pouvez demander à Step Functions d'appeler des services AWS, tels que Lambda, pour effectuer des tâches. Vous pouvez également créer des flux de travail automatisés à long terme pour les applications qui nécessitent une interaction humaine.

Step Functions est idéal pour une utilisation dans le cadre d'un processus judiciaire, car il prend en charge un ensemble reproductible et automatisé d'étapes prédéfinies qui peuvent être vérifiées à l'aide des journaux d'AWS. Cela vous permet d'exclure toute implication humaine et d'éviter les erreurs dans votre processus judiciaire.

Considérations relatives à la conception

- Vous pouvez lancer un flux de travail Step Functions manuellement ou automatiquement pour capturer et analyser les données de sécurité lorsque GuardDuty ou Security Hub indiquent une compromission. L'automatisation avec une interaction humaine minimale ou nulle permet à votre équipe de se mettre à l'échelle rapidement en cas d'événement de sécurité important affectant de nombreuses ressources.
- Pour limiter les flux de travail entièrement automatisés, vous pouvez inclure des étapes dans le flux d'automatisation pour une intervention manuelle. Par exemple, vous pouvez demander à un analyste de sécurité autorisé ou à un membre de l'équipe d'examiner

les résultats de sécurité générés et de déterminer s'il convient de lancer une collecte de preuves judiciaires, ou de mettre en quarantaine et de contenir les ressources concernées, ou les deux.

- Si vous souhaitez lancer une investigation judiciaire sans qu'un résultat actif ait été créé à partir d'un outil de sécurité (tels que GuardDuty ou Security Hub), vous devez implémenter des intégrations supplémentaires pour invoquer un flux de travail Step Functions judiciaire. Cela peut se faire en créant une règle EventBridge qui recherche un événement CloudTrail spécifique (tel qu'un événement de modification de balise) ou en autorisant un analyste de sécurité ou un membre de l'équipe à lancer un flux de travail Step Functions judiciaire directement depuis la console. Vous pouvez également utiliser Step Functions pour créer des tickets exploitables en les intégrant au système de billetterie de votre organisation.

AWS Lambda

Avec AWS Lambda, vous pouvez exécuter du code sans avoir à allouer ou gérer des serveurs. Vous payez uniquement pour le temps de calcul consommé. Aucuns frais ne sont facturés si votre code n'est pas en cours d'exécution. Lambda exécute le code sur une infrastructure informatique à haute disponibilité et administres toutes les ressources de calcul, y compris la maintenance des serveurs et du système d'exploitation, l'allocation et la mise à l'échelle automatique des capacités, ainsi que la mise à l'échelle automatique et la journalisation. Vous fournissez votre code dans l'une des exécutions de langage pris en charge par Lambda, puis vous organisez votre code en fonctions Lambda. Le service Lambda n'exécute votre fonction qu'en cas de besoin et se met à l'échelle automatiquement.

Dans le contexte d'une investigation judiciaire, l'utilisation des fonctions Lambda vous permet d'obtenir des résultats constants grâce à des étapes reproductibles, automatisées et prédéfinies qui sont définies dans le code Lambda. Lorsqu'une fonction Lambda s'exécute, elle crée un journal qui vous aide à vérifier que le processus approprié a été mis en œuvre.

Considérations relatives à la conception

- Les fonctions Lambda ont un délai d'expiration de 15 minutes, alors qu'un processus judiciaire complet visant à recueillir des preuves pertinentes peut prendre plus de temps. C'est pourquoi nous vous recommandons d'orchestrer votre processus judiciaire en utilisant des fonctions Lambda intégrées dans un flux de travail Step Functions. Le flux de

travail vous permet de créer des fonctions Lambda dans le bon ordre, et chaque fonction Lambda implémente une étape de collecte individuelle.

- En organisant vos fonctions Lambda judiciaires dans un flux de travail Step Functions, vous pouvez exécuter certaines parties de la procédure de collecte judiciaire en parallèle afin d'accélérer la collecte. Par exemple, vous pouvez collecter des informations sur la création d'images de disque plus rapidement lorsque plusieurs volumes sont concernés.

AWS KMS

AWS Key Management Service (AWS KMS) vous aide à créer et à gérer des clés de chiffrement et à contrôler leur utilisation dans un large éventail de services AWS et dans vos applications. Pour obtenir des conseils généraux sur AWS SRA, consultez Amazon KMS dans la section Comptes d'outils de sécurité.

Dans le cadre du processus d'analyses judiciaires, la collecte de données et les investigations doivent être effectuées dans un environnement isolé afin de minimiser l'impact commercial. La sécurité et l'intégrité des données ne peuvent pas être compromises au cours de ce processus, et un processus devra être mis en place pour permettre le partage des ressources chiffrées, telles que les instantanés et les volumes de disque, entre le compte potentiellement compromis et le compte d'analyses judiciaires. Pour ce faire, votre organisation devra s'assurer que la stratégie de ressources AWS KMS associée prend en charge la lecture des données chiffrées ainsi que leur sécurisation en les chiffrant à nouveau avec une clé AWS KMS dans le compte d'analyses judiciaires.

Considération relative à la conception

- Les stratégies de clés KMS d'une organisation doivent autoriser les principaux IAM autorisés à utiliser la clé pour déchiffrer les données dans le compte source et les rechiffrer dans le compte d'analyses judiciaires. Utilisez l'infrastructure en tant que code (IaC) pour gérer de manière centralisée toutes les clés de votre organisation dans AWS KMS afin de garantir que seuls les principaux IAM autorisés disposent de l'accès approprié et du moindre privilège. Ces autorisations doivent exister sur toutes les clés KMS qui peuvent être utilisées pour chiffrer les ressources sur AWS susceptibles d'être collectées lors d'une investigation judiciaire. Si vous mettez à jour la stratégie de clé KMS après un événement de sécurité, la mise à jour ultérieure de la stratégie de ressources pour une clé KMS en cours d'utilisation peut avoir un impact sur votre activité. En outre, les problèmes

d'autorisation peuvent augmenter le temps moyen global de réponse (MTTR) en cas d'événement de sécurité.

AI/ML pour la sécurité

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

L'intelligence artificielle et l'apprentissage automatique (IA/ML) transforment les entreprises. L'IA et le ML sont au cœur des préoccupations d'Amazon depuis plus de 20 ans, et de nombreuses fonctionnalités utilisées par les clients avec AWS, notamment les services de sécurité, sont pilotées par l'IA et le ML. Cela crée une valeur intrinsèque différenciée, car vous pouvez créer en toute sécurité sur 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 la façon dont le programme doit fonctionner 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. De nombreux services AWS utilisent l'intelligence artificielle et le machine learning pour tirer des enseignements 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. Il 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 comptes AWS, vos instances, vos charges de travail sans serveur et de conteneurs, 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 des comportements opérationnels anormaux mais bénins au sein des 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' GuardDutyutilisation 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 dans Amazon GuardDuty (TDR310).

Une sécurité prouvable

AWS développe des outils de raisonnement automatisés qui utilisent la logique mathématique pour répondre à des 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 site Web d'AWS. Les services et fonctionnalités AWS suivants utilisent actuellement un raisonnement automatique pour vous aider à garantir une sécurité prouvable pour vos applications :

- Amazon CodeGuru Security est un outil de test statique de sécurité des applications (SAST) qui combine le machine learning et le raisonnement automatique pour identifier les vulnérabilités de votre code et fournir des recommandations sur la manière de corriger ces vulnérabilités et de suivre leur statut jusqu'à leur fermeture. CodeGuru La sécurité détecte les 10 principaux problèmes

identifiés par l'Open Worldwide Application Security Project (OWASP), les 25 principaux problèmes identifiés par Common Weakness Enumeration (CWE), l'injection de logs, les secrets et l'utilisation non sécurisée des API et SDK AWS. CodeGuru La sécurité s'inspire également des meilleures pratiques de sécurité d'AWS et a été formée sur des millions de lignes de code chez Amazon.

CodeGuru La sécurité peut identifier les vulnérabilités du code avec un taux de vrais positifs très élevé grâce à son analyse sémantique approfondie. Cela permet aux développeurs et aux équipes de sécurité d'avoir confiance dans les conseils, ce qui se traduit par une amélioration de la qualité. Ce service est formé à l'aide de modèles d'exploration de règles et de machine learning supervisée qui utilisent une combinaison de régression logistique et de réseaux neuronaux. Par exemple, lors de la formation sur les fuites de données sensibles, CodeGuru Security effectue une analyse complète du code pour les chemins de code qui utilisent la ressource ou accèdent à des données sensibles, crée un ensemble de fonctionnalités qui les représente, puis utilise les chemins de code comme entrées pour les modèles de régression logistique et les réseaux neuronaux convolutionnels (CNN). La fonction de suivi des bogues de CodeGuru sécurité détecte automatiquement la fermeture d'un bogue. L'algorithme de suivi des bogues garantit que vous disposez up-to-date d'informations sur le niveau de sécurité de votre entreprise sans effort supplémentaire. Pour commencer à réviser le code, vous pouvez associer vos référentiels de code existants sur GitHub Enterprise GitHub, Bitbucket ou AWS CodeCommit sur la CodeGuru console. La conception basée sur l'API de CodeGuru sécurité fournit des fonctionnalités d'intégration que vous pouvez utiliser à n'importe quelle étape du flux de travail de développement.

- 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 (IAM) Access Analyzer vous 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 au niveau du bucket ou du compte (ce qui affecte à la fois les buckets existants et les nouveaux compartiments du compte). Un accès public est accordé aux compartiments et objets via des listes de contrôle d'accès (ACL), des stratégies de compartiment, ou via les 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 réseau AWS. Il produit ensuite des résultats pour les chemins correspondant à vos étendues d'accès réseau, qui définissent les modèles de trafic sortant et entrant. Network Access Analyzer 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 au sein 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 (VPC). 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 (AWSSRA) en répondant à une courte enquête.

L'architecture de sécurité multi-comptes recommandée par l'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. L'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 cloud AWS (AWS CAF) recommande quatre phases itératives et incrémentielles de transformation du cloud : Envision, Align, Launch et Scale. 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. L'AWS SRA vous aide à mettre en place cette architecture de base de sécurité afin que vous puissiez appliquer des contrôles de sécurité de manière uniforme dans l'ensemble de votre organisation en pleine expansion au sein d'AWS Organizations. L'architecture de base comprend plusieurs comptes et services AWS. 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 sécurité d'AWS Well-Architected Framework.

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

Une organisation et une structure de compte AWS 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 de disposer de plusieurs comptes AWS vous 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 vous pouvez utiliser AWS Organizations pour gérer plusieurs comptes AWS, et comment utiliser les fonctionnalités d'accès sécurisé et d'administrateur délégué pour gérer de manière centralisée les services AWS sur ces multiples comptes.

Vous pouvez utiliser AWS Control Tower comme indiqué précédemment dans ce guide pour orchestrer votre zone de landing zone. Si vous utilisez actuellement un seul compte AWS, consultez le guide de transition vers plusieurs comptes AWS pour effectuer la migration vers plusieurs comptes dès que possible. Par exemple, si votre start-up conçoit et prototype actuellement votre produit sur un seul 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 vos unités d'organisation et comptes AWS de base, puis ajoutez vos unités d'organisation et comptes liés à la charge de travail.

Pour les recommandations relatives aux comptes AWS et à la structure de l'unité d'organisation allant au-delà de ce qui est prévu dans l'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 la structure de votre compte, réfléchissez aux contrôles de sécurité de haut niveau à l'échelle de l'organisation que vous souhaiteriez appliquer à l'aide de politiques de contrôle des services (SCP).

Considération de conception

- Ne reproduisez pas la structure hiérarchique de votre entreprise lorsque vous concevez votre unité d'organisation et votre structure de compte. Vos unités d'organisation doivent être basées sur des 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 unités d'organisation de base, puis ajoutez des unités d'organisation de charge de travail selon vos besoins. Vous pouvez déplacer des comptes entre des unités d'organisation

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 des SCP et des conditions IAM basées sur les chemins d'unité d'organisation et de compte.

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 avez créé plusieurs comptes AWS, vous devez donner à vos équipes l'accès aux ressources AWS contenues dans 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 entreprises où les employés et les charges de travail automatisées doivent se connecter à AWS pour effectuer 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 instructions d'AWS SRA pour savoir comment utiliser AWS IAM Identity Center dans les comptes Org Management et Shared Services afin de gérer de manière centralisée l'accès par authentification unique (SSO) à vos 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 ressources AWS, vous devez utiliser AWS 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 de 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 de mise en œuvre

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 l'activité d'AWS, suivez les recommandations d'AWS SRA pour configurer un suivi organisationnel en utilisant AWS CloudTrail et en centralisant vos journaux dans le compte Log Archive. Pour surveiller les événements de sécurité, utilisez AWS Security Hub, Amazon GuardDuty, AWS Config et AWS Security Lake, comme indiqué dans la section relative au compte Security Tooling.

Considération de conception

- Lorsque vous commencez à utiliser les nouveaux 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 de mise en œuvre

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 CloudTrail la duplication de ce qui est configuré par AWS Control Tower. Cette solution fournit des options pour configurer les événements de gestion.
- Le compte de gestion AWS Config Control Tower permet à AWS Config dans le 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 Organization configure Security Hub 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 vos comptes AWS.
- Une structure de compte et d'unité d'organisation bien définie avec des contrôles préventifs définis par le biais de SCP et de rôles et de politiques IAM avec le moindre privilège.

- Possibilité de consigner les activités d'AWS à l'aide d'AWS CloudTrail ; de détecter les événements de sécurité à l'aide d'AWS Security Hub GuardDuty, Amazon et AWS Config ; et d'effectuer des analyses avancées sur un lac de données spécialement conçu à des fins de sécurité à l'aide d'Amazon Security Lake.

Au cours de cette phase, prévoyez d'appliquer la sécurité à d'autres niveaux de votre organisation AWS, comme décrit dans la section Appliquer les services de sécurité au sein de votre organisation AWS. Vous pouvez créer des contrôles de sécurité pour votre couche réseau en utilisant des services tels qu'AWS WAF, AWS Shield, AWS Firewall Manager, AWS Network Firewall, AWS Certificate Manager (ACM), Amazon, 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, Amazon Systems Manager, AWS Secrets Manager et Amazon Cognito comme indiqué dans la section Compte de l'application.

Considération de 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 utilisés par AWS pour adopter une approche de sécurité davantage axée sur la gauche, consultez le billet de blog Comment AWS a créé le programme Security Guardians, un mécanisme de distribution de la propriété des titres.

Exemples de mise en œuvre

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 par défaut d'Amazon Elastic Block Store (Amazon EBS) dans Amazon EC2 afin d'utiliser la clé AWS KMS par défaut dans les régions AWS fournies.
- 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 politique de groupe de sécurité et des politiques AWS WAF 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 AWS 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 l'autorité de certification privée AWS, comme expliqué dans la section Compte de l'application. AWS KMS et AWS CloudHSM vous 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 tout aussi 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 de sécurité ne dégénère. La préparation vous aide à trier rapidement un événement de sécurité afin de comprendre son impact potentiel.

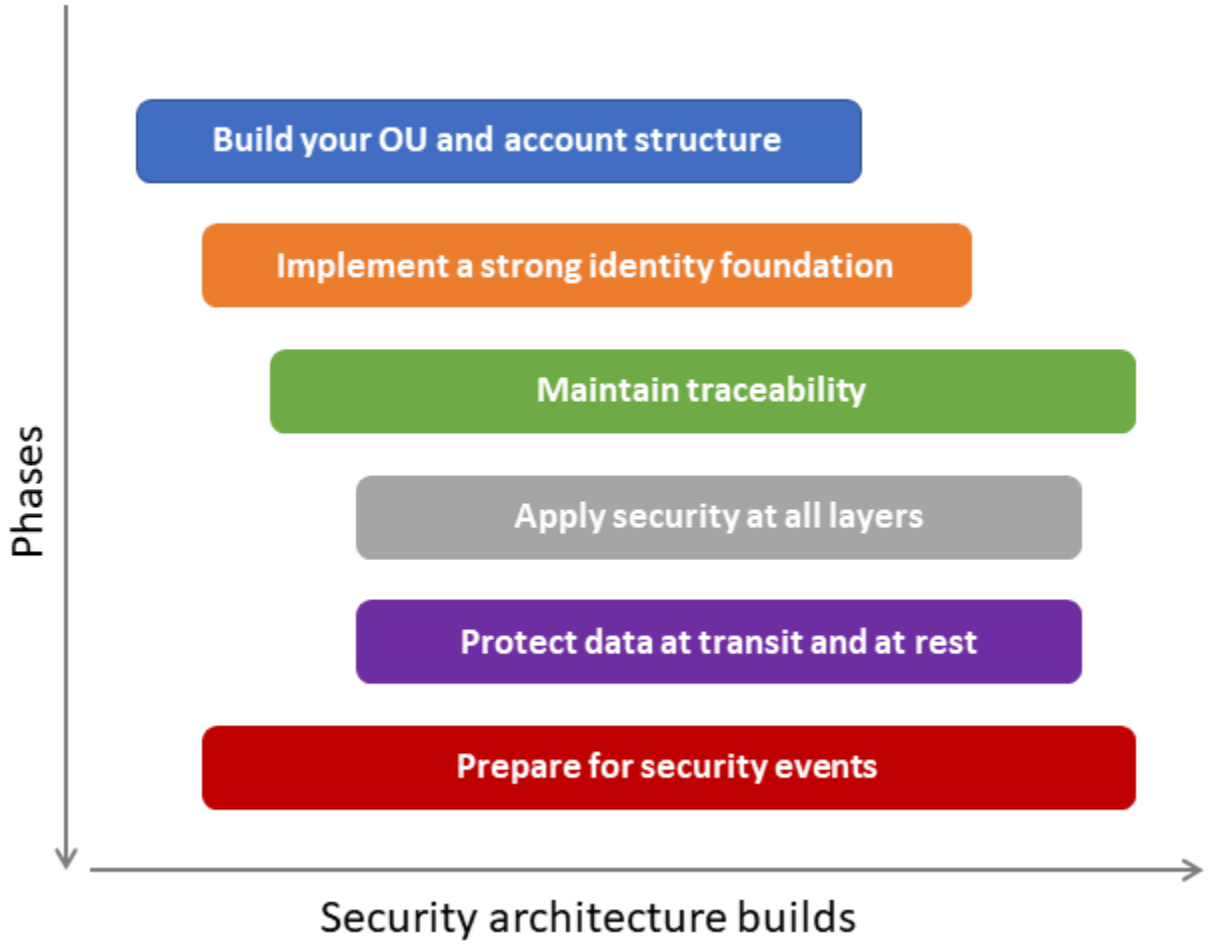
L'AWS SRA, grâce à la conception du compte Security Tooling et au déploiement de services de sécurité communs au sein de tous les comptes AWS, vous permet de détecter les événements de sécurité au sein de votre organisation AWS. AWS Detective, intégré au compte Security Tooling,

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.

L'AWS SRA recommande un compte d'archive de journaux central 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'environnement AWS, 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 l'AWS SRA, pour interroger ces journaux à des fins d'investigation.

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, attribuez des données et une importance commerciale à vos ressources AWS 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 de Detective Organization, qui active automatiquement Detective en déléguant l'administration à un compte (par exemple, Audit ou Security Tooling) et configure Detective pour les comptes AWS Organizations existants et futurs.

Ressources IAM

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

Bien qu'AWS Identity and Access Management (IAM) ne soit pas un service inclus dans un schéma d'architecture traditionnel, il touche tous les aspects de l'organisation AWS, des comptes AWS et des services AWS. Vous ne pouvez déployer aucun service AWS sans créer d'entités IAM et accorder des autorisations au préalable. 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 documentation AWS, les articles IAM sur le blog AWS Security et les présentations AWS re:Invent.
- Le pilier de sécurité d'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 entre comptes, 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
Stratégies de contrôle de service (SCP)	Restrict	Équipe centrale, telle que l'équipe	Garde-corps, gouvernance	Organisation, unité d'organis	Tous les principes de l'organisation, de	Compte de gestion de l'organisation [2]

		chargée de la plateforme ou de la sécurité [1]		ation, compte	l'unité d'organisation et des comptes	
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 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 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 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 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 membres

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 utiliser les SCP, vous devez activer toutes les fonctionnalités d'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, les règles AWS Lambda et AWS Config) 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 d'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 les SCP imposent l'attachement de la limite des autorisations.
8. Cela suppose que des barrières de sécurité suffisantes (par exemple, des SCP 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.

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.
- Utilisez les SCP 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-depth approche (en conjonction avec des politiques basées sur l'identité), utilisez des politiques IAM basées sur les ressources pour refuser un large accès aux ressources.
- Utilisez le conseiller d'accès IAM, AWS CloudTrail, AWS IAM Access Analyzer 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 exemples AWS SRA

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

Pour vous aider à créer et à mettre en œuvre les directives de l'AWS SRA, un référentiel d'infrastructure en tant que code (IaC) disponible à l'adresse 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 AWS Professional Services 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 configurations des services AWS 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 propose deux modèles de solutions : l'un nécessite AWS Control Tower et l'autre utilise AWS Organizations sans AWS Control Tower. Les solutions de ce référentiel qui nécessitent AWS Control Tower ont été déployées et testées dans un environnement AWS Control Tower à l'aide d'AWS CloudFormation et de Customizations for AWS Control Tower (CfCT). Les solutions qui ne nécessitent pas AWS Control Tower ont été testées dans un environnement AWS Organizations à l'aide d'AWS CloudFormation. La solution CfCT aide les clients à configurer rapidement un environnement AWS sécurisé et multi-comptes basé sur les meilleures pratiques d'AWS. 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 fichier README.md contenant des informations détaillées.

- La solution CloudTrail Organization crée un suivi 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. Les événements de données peuvent éventuellement être activés pour les fonctions Amazon S3 et AWS Lambda. Un journal d'organisation enregistre les événements pour tous les comptes AWS de l'organisation AWS tout en empêchant les comptes 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'organisation AWS 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 Organization configure AWS Security Hub en déléguant l'administration au compte Security Tooling. Il configure Security Hub dans le compte Security Tooling pour tous les comptes d'organisation AWS existants et futurs. 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 de Security Hub au sein du compte Security Tooling fournit une vue multicompte de la conformité aux normes de sécurité et des résultats des services AWS et des intégrations de partenaires AWS tiers.
- La solution Inspector configure Amazon Inspector au sein du compte administrateur délégué (Security Tooling) pour tous les comptes et régions régies par l'organisation AWS.
- La solution Firewall Manager configure les politiques de sécurité d'AWS Firewall Manager 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 AWS existants et futurs. 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 agrégateur AWS Config en déléguant l'administration au compte Security Tooling. La solution configure ensuite un agrégateur AWS Config dans le compte Security Tooling pour tous les comptes existants et futurs de l'organisation AWS.
  - La solution Conformance Pack Organization Rules déploie les règles AWS Config 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'organisation AWS. 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 AWS Config dans le compte de gestion AWS Control Tower et met à jour l'agrégateur AWS Config dans le compte Security Tooling en conséquence. La solution utilise le CloudFormation modèle AWS Control Tower pour activer AWS Config comme référence afin de garantir la cohérence avec les autres comptes de l'organisation AWS.
- IAM
  - La solution Access Analyzer active AWS IAM Access Analyzer en déléguant l'administration au compte Security Tooling. Il configure ensuite un analyseur d'accès 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 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 de mot de passe des comptes AWS pour tous les comptes d'une organisation AWS. 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 par défaut EC2 permet le chiffrement Amazon EBS par défaut au niveau du compte au sein de chaque compte AWS et de chaque région AWS 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 active les paramètres au niveau du compte Amazon S3 au sein de chaque compte AWS de l'organisation 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 AWS Organization existants et futurs.

Architecture de référence de confidentialité AWS (AWS PRA)

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

L'AWS SRA vise principalement à vous aider à créer votre architecture de sécurité de base sur AWS dans un environnement multi-comptes. AWS publie également des architectures de référence de sécurité supplémentaires, telles que l'architecture de référence de confidentialité AWS (AWS PRA), qui sont personnalisées pour des types d'applications spécifiques ou aident à répondre aux exigences réglementaires ou de conformité.

Les applications qui traitent des données personnelles doivent respecter des 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). Si vous gérez une telle application sur AWS, vous devez prendre des décisions concernant les personnes, les processus et la conception des technologies afin de préserver la confidentialité. L'AWS PRA fournit un ensemble de directives spécifiques à la conception et à la configuration des contrôles de confidentialité dans les services AWS. Ces contrôles incluent des fonctionnalités de minimisation des données, de chiffrement et de pseudonymisation. L'AWS PRA décrit également les contrôles qui contribuent à préserver la confidentialité lors du partage et du traitement des données. Le guide AWS PRA vous aide à commencer à concevoir et à créer une base garantissant la confidentialité dans le cloud AWS. Il inclut des considérations clés, les meilleures pratiques, des aperçus des services et fonctionnalités AWS liés à la confidentialité, ainsi que des exemples de configuration.

AWS PRA repose sur l'architecture de sécurité de base, telle que fournie par les directives de conception AWS SRA. Afin d'établir des contrôles de confidentialité, l'AWS PRA utilise bon nombre des mêmes services AWS clés que l'AWS SRA et repose sur les mêmes directives fondamentales et la même structure de compte que celles décrites dans l'AWS SRA. Nous vous recommandons de consulter le guide de conception AWS SRA avant de consulter l'AWS PRA.

Remerciements

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

Principaux auteurs

- Avik Mukherjee, AWS Senior Consultant
- Damindra Bandara, AWS Senior Consultant

Collaborateurs

- Scott Conklin, AWS Senior Consultant
- Josh Du Lac, AWS Principal Solutions Architect
- Ilya Epshteyn, AWS Senior Manager, Identity Solutions
- Michae Haken, AWS Principal Technologist
- Paul Hawkins, AWS Principal, Office of CISO
- Jorg Huser, AWS Principal Consultant
- Tomek Jakubowski, AWS Senior Consultant
- Mehial Mendrin, AWS Senior Consultant
- Jonathan Nguyen, AWS Principal Security Architect
- Eric Rose, AWS Principal Consultant
- Handan Selamoglu, AWS Senior Technical Writer
- Arun Thomas, AWS Senior Solution Architect
- Ross Warren, AWS Product Solution Architect
- Andy Wickersham, AWS Senior Security Engineer

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

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

Pour une introduction ou un rappel, consultez la section Sécurité, identité et conformité sur AWS sur le site Web d'AWS pour obtenir la liste des 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 vos modules de sécurité matériels (HSM) dans le cloud AWS.
- AWS Certificate Manager — Fournissez, gérez et déployez des certificats SSL/TLS à utiliser avec les services AWS.
- AWS Secrets Manager : alternez, gérez et récupérez les informations d'identification de base de données, les clés d'API et autres secrets tout au long de leur cycle de vie.

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

- IAM — Contrôlez en toute sécurité l'accès aux services et ressources AWS.
- IAM Identity Center — Gérez de manière centralisée l'accès SSO à plusieurs comptes AWS et 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 cloud AWS.

- AWS Resource Access Manager : partagez les ressources AWS de manière simple et sécurisée.
- AWS Organizations — Mettez en œuvre une gestion basée sur des politiques 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. Les 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 sur AWS grâce à une protection DDoS 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 règles AWS WAF pour les comptes et applications AWS à partir d'un emplacement central.
- AWS Systems Manager — Configurez et gérez les systèmes Amazon EC2 et sur site pour appliquer les correctifs du système d'exploitation, créer des images système sécurisées et configurer des systèmes d'exploitation sécurisés.
- Amazon VPC — Provisionnez une section isolée de manière logique d'AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez.
- AWS Network Firewall : déployez les protections réseau essentielles pour vos VPC.
- Pare-feu DNS Amazon Route 53 : protégez vos requêtes DNS sortantes provenant de vos VPC.
- Accès vérifié AWS — Fournissez un accès sécurisé à vos applications sans avoir besoin de réseaux privés virtuels (VPN).
- Amazon VPC Lattice — Simplifiez la service-to-service connectivité, la sécurité et la surveillance.

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

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

- Amazon GuardDuty — Protégez vos comptes AWS et 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 ressources AWS pour permettre l'audit de conformité, le suivi des modifications des ressources et l'analyse de sécurité.
- Règles AWS Config : 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 CloudTrail — Suivez l'activité des utilisateurs et l'utilisation des API pour permettre la gouvernance et l'audit opérationnel et des risques de votre 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 — AWS vous 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 meilleures pratiques AWS et les normes sectorielles suivies par votre entreprise.

- AWS Artifact : utilisez un portail en libre-service gratuit pour accéder à la demande aux rapports de sécurité et de conformité AWS et à certains accords en ligne.
- AWS Audit Manager — Auditez en permanence votre utilisation d'AWS afin de 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. Si vous souhaitez être informé des futures mises à jour, vous pouvez vous abonner à un flux RSS.

Modification	Description	Date
Mises à jour majeures	• Mise à jour des sections Compte réseau et Compte d'application afin d'ajouter des directives architect urales pour Amazon Verified Permissions, AWS Verified Access et Amazon VPC Lattice. • Ajout de conseils architect uraux approfondis basés sur les fonctionnalités de sécurité. • Ajout de nouvelles directive s sur la manière dont les services AWS utilisent l'intelligence artificielle et le machine learning pour améliorer les 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	Mise à jour des sections relatives au compte Security Tooling et au compte Log	22 septembre 2023

	Archive afin d'ajouter des conseils de conception relatifs à Amazon Security Lake.	
Mises à jour mineures	• Les directives existantes ont été mises à jour pour refléter les nouvelles fonctionnalités des services AWS et les meilleures pratiques. • Consignes architecturales mises à jour pour AWS CloudTrail, AWS IAM Identity Center et Edge Security.	10 mai 2023
Sondage	Ajout d'une courte enquête pour mieux comprendre comment vous utilisez l'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 et les principes de conceptio n de sécurité ont été mises à jour.	27 septembre 2022

Ajouts et mises à jour majeurs	• Ajout d'informations sur l'utilisation de l'AWS SRA et des directives de mise en œuvre clés. • Ajout de conseils architect uraux pour d'autres services AWS tels qu'AWS Artifact, Amazon Inspector, AWS RAM, Amazon Route 53, AWS Control Tower, AWS Audit Manager, AWS Directory Service, Amazon Cognito et Network Access Analyzer. • Les directives existantes ont été mises à jour pour refléter les nouvelles fonctionnalités des services AWS et les meilleures pratiques.	25 juillet 2022
—	Publication initiale. Cette version n'inclut pas plusieurs AWS services (tels qu'AWS Directory ServiceAmazon Cognito et AWS Audit Manager)AWS Resource Access Manager, que nous prévoyons d'ajouter dans les futures versions.	23 Juin 2021

AWSGlossaire 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 Fournir des commentaires à la fin du glossaire.

Termes de sécurité

anonymisation

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

anti-motif

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

contrôle d'accès basé sur les attributs (ABAC)

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

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.

graphe de comportement

Une vue unifiée et interactive du comportement et des interactions des ressources au fil du temps. Vous pouvez utiliser un graphe 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, consultez la section Données d'un graphe de comportement dans la documentation Detective.

chiffrement côté client

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

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.

données au repos

Les données stationnaires sur votre réseau, telles que les données stockées.

classification des données

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

données en transit

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

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.

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.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement intégrés dans 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 stratégieAWS, vous ajoutez plusieurs contrôles à différentes couches de la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

DansAWS 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, consultez la section Services compatibles AWS Organizations dans la AWS Organizations documentation.

contrôle de détective

Contrôle de sécurité conçu pour détecter, consigner 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, voir Detective controls dans Implementation des contrôles de sécurité sur AWS.

clé de chiffrement

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

service de point final

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

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).

contrôle d'accès détaillé (FGAC)

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

restrictions géographiques (blocage géographique)

Dans 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.

rambarde

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (UO). Des garde-fous préventifs appliquent des politiques visant à garantir l'alignement sur les normes de conformité. Ils sont mis en œuvre à l'aide de politiques de contrôle des services et de limites d'autorisations IAM. Les garde-corps Detective 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 GuardDutyAWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

politique basée sur l'identité

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

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 AWS de référence de sécurité recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

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 AWS de référence de sécurité recommande de configurer votre compte réseau avec des VPC entrants, sortants et d'inspection afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

moindre privilège

La meilleure pratique en matière de sécurité qui consiste à accorder les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez la section Appliquer les autorisations de moindre privilège dans la documentation IAM.

compte membre

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

parcours d'organisation

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

VPC sortant (de sortie)

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

contrôle d'accès à l'origine (OAC)

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

identité d'accès à l'origine (OAI)

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

limite d'autorisations

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

politique

Objet capable de définir des autorisations (voirpolitique basée sur l'identité), de spécifier des conditions d'accès (voirpolitique 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).

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, consultez la section Contrôles préventifs dans Implémentation des contrôles de sécurité sur AWS.

principal

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

Confidentialité dès la conception

Une approche de l'ingénierie des systèmes qui prend en compte la confidentialité tout au long du processus d'ingénierie.

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.

ransomware

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

politique basée sur les ressources

Politique attachée à une ressource, telle qu'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.

commande réactive

Un contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre base de référence en matière de sécurité. Pour plus d'informations, voir Contrôles réactifs dans Implémentation des contrôles de sécurité sur AWS.

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'AWSAPI sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération basée sur SAML 2.0, voir À propos de la fédération basée sur SAML 2.0 dans la documentation IAM.

contrôle de sécurité

Un garde-fou technique ou administratif qui empêche, détecte ou réduit la capacité d'un acteur menaçant d'exploiter une faille de sécurité. Il existe trois principaux types de contrôles de sécurité : préventifs, détectifs et réactifs.

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 nécessaires, la mise en œuvre des meilleures pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

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

Outils et services qui combinent des systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un 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 et de générer des alertes.

chiffrement côté serveur

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

politique de contrôle des services (SCP)

Politique qui fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dansAWS Organizations. Les SCP définissent des garde-fous 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 spécifier quels services ou actions sont autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWSest 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.

chiffrement symétrique

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

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 pour vous. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

vulnérabilité

Défaut logiciel ou matériel qui compromet la sécurité du système.

charge de travail

Ensemble de ressources et de code apportant une valeur commerciale, tel qu'une application destinée aux clients ou un processus principal.

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'unvulnérabilité 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.

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.