Guide de GuardDuty l'utilisateur Amazon

Amazon GuardDuty

Amazon GuardDuty: Guide de GuardDuty l'utilisateur Amazon

Table of Contents

Qu'est-ce qu'Amazon GuardDuty ?

Amazon GuardDuty est un service de détection des menaces qui surveille, analyse et traite en permanence les sources de AWS données et les journaux de votre AWS environnement. GuardDuty utilise des flux de renseignements sur les menaces, tels que des listes d'adresses IP et de domaines malveillants, des hachages de fichiers et des modèles d'apprentissage automatique (ML) pour identifier les activités suspectes et potentiellement malveillantes dans votre AWS environnement. La liste suivante fournit une vue d'ensemble des scénarios de menaces potentiels qui GuardDuty peuvent vous aider à les détecter :

- Informations d'identification compromises et exfiltrées. AWS
- Exfiltration et destruction de données susceptibles de provoquer un ransomware. Des modèles inhabituels d'événements de connexion dans les versions du moteur prises en charge des RDS bases de données Amazon Aurora et Amazon, qui indiquent un comportement anormal.
- Activité de cryptomining non autorisée dans vos instances Amazon Elastic Compute Cloud EC2 (Amazon) et vos charges de travail de conteneurs.
- Présence de logiciels malveillants dans vos EC2 instances Amazon et vos charges de travail de conteneur, ainsi que de fichiers récemment chargés dans vos compartiments Amazon Simple Storage Service (Amazon S3).
- Événements au niveau du système d'exploitation, du réseau et des fichiers indiquant un comportement non autorisé sur vos clusters Amazon Elastic Kubernetes Service (Amazon), sur vos tâches EKS Amazon Elastic Container Service ECS (Amazon), EC2 sur vos instances Amazon et sur vos AWS Fargate (Fargate) charges de travail de conteneur.

Qu'est-ce qu'Amazon GuardDuty

Table des matières

Caractéristiques de GuardDuty

Voici quelques-uns des principaux moyens par lesquels Amazon GuardDuty peut vous aider à surveiller, détecter et gérer les menaces potentielles dans votre AWS environnement.

Surveille en permanence des sources de données et des journaux d'événements spécifiques

- Détection des menaces fondamentales : lorsque vous activez un Compte AWS, commence GuardDuty automatiquement GuardDuty à ingérer les sources de données de base associées à ce compte. Ces sources de données incluent les événements AWS CloudTrail de gestion, les journaux de VPC flux (provenant EC2 des instances Amazon) et DNS les journaux. Vous n'avez rien d'autre à activer pour commencer GuardDuty à analyser et à traiter ces sources de données afin de générer les résultats de sécurité associés. Pour de plus amples informations, veuillez consulter GuardDuty sources de données de base.
- Plans de GuardDuty protection axés sur les cas d'utilisation : pour une meilleure visibilité de la détection des menaces sur la sécurité de votre AWS environnement, GuardDuty propose des plans de protection dédiés que vous pouvez choisir d'activer. Les plans de protection vous aident à surveiller les journaux et les événements provenant d'autres AWS services. Ces sources incluent les journaux EKS d'audit, l'activité de RDS connexion, les événements liés aux données Amazon S3, les EBS volumes CloudTrail, la surveillance du temps d'exécution sur AmazonEKS, Amazon et Amazon ECS -FargateEC2, ainsi que les journaux d'activité du réseau Lambda. GuardDutyconsolide ces sources de journaux et d'événements sous le terme « Fonctionnalités ». Vous pouvez activer à tout moment un ou plusieurs plans de protection dédiés dans un Région AWS programme pris en charge. GuardDuty commencera à surveiller, traiter et analyser les activités en fonction du plan de protection que vous activez. Pour plus d'informations sur chaque plan de protection et son fonctionnement, consultez le document du plan de protection correspondant.

Plan de protection	Description
Protection S3	Identifie les risques de sécurité potentiels tels que l'exfiltr ation de données et les tentatives de destruction dans vos compartiments Amazon S3.
EKSProtection	EKSLa surveillance des journaux d'audit analyse les journaux d'audit Kubernetes de vos EKS clusters Amazon

Plan de protection	Description
	pour détecter les activités potentiellement suspectes et malveillantes.
Surveillance d'exécution	Surveille et analyse les événements au niveau du système d'exploitation sur Amazon, EKS Amazon et Amazon ECS (y compris AWS Fargate)EC2, afin de détecter les menaces potentielles liées à l'exécution.
Protection contre les logiciels malveillants pour EC2	Détecte la présence potentielle de logiciels malveillants en analysant les EBS volumes Amazon associés à vos EC2 instances Amazon. Il existe une option permettant d'utiliser cette fonctionnalité à la demande.
Protection contre les logiciels malveillants pour S3	Détecte la présence potentielle de logiciels malveillants dans les objets récemment chargés dans vos compartiments Amazon S3.
RDSProtection	Analyse et établit le profil de votre activité de RDS connexion pour détecter les menaces d'accès potentielles aux RDS bases de données Amazon Aurora et Amazon prises en charge.
Protection Lambda	Surveille les journaux d'activité du réseau Lambda, en commençant par les journaux de VPC flux, afin de détecter les menaces qui pèsent sur vos AWS Lambda fonctions. Le minage de cryptomonnaies et la communication avec des serveurs malveillants sont des exemples de ces menaces potentielles.

Activez la protection contre les programmes malveillants pour S3 de manière indépendante

GuardDuty offre la possibilité d'utiliser Malware Protection for S3 de manière indépendante, sans activer le GuardDuty service Amazon. Pour plus d'informations sur la mise en route uniquement avec Malware Protection pour S3, consultezGuardDuty

Protection contre les logiciels malveillants pour S3. Pour utiliser tous les autres plans de protection, vous devez activer le GuardDuty service.

Gestion d'un environnement à comptes multiples

Vous pouvez gérer un AWS environnement à comptes multiples en utilisant une méthode d'invitation AWS Organizations (recommandée) ou une ancienne méthode d'invitation. Pour de plus amples informations, veuillez consulter Gestion de plusieurs comptes .

Génère des résultats de sécurité pour les menaces détectées

Lorsqu'il GuardDuty détecte des menaces de sécurité potentielles associées à vos AWS ressources, il commence à générer des résultats de sécurité fournissant des informations sur la ressource potentiellement compromise. Une fois que vous l'avez activé GuardDuty dans votre compte, générez Exemples de résultats pour afficher les informations associéesDétails d'un résultat. Pour une liste complète des résultats de sécurité, voirTypes de résultats.

Avec GuardDuty, vous pouvez également utiliser un script de test qui génère des résultats GuardDuty de sécurité spécifiques pour comprendre comment examiner les GuardDuty résultats et y répondre. Pour de plus amples informations, veuillez consulter GuardDuty Résultats des tests dans des comptes dédiés.

Évaluation et gestion des résultats de sécurité

GuardDuty consolide vos résultats de sécurité sur l'ensemble des comptes et affiche les résultats dans le tableau de bord récapitulatif de la GuardDuty console. Vous pouvez également récupérer les résultats via le AWS Security Hub API AWS Command Line Interface, ou AWS SDK. Grâce à une vision globale de votre état de sécurité actuel, vous pouvez identifier les tendances et les problèmes potentiels, et prendre les mesures correctives nécessaires. Pour de plus amples informations, veuillez consulter Gérer GuardDuty les résultats.

Intégrez les services AWS de sécurité connexes

Pour vous aider à analyser et à étudier les tendances en matière de sécurité dans votre AWS environnement, pensez à utiliser les services AWS liés à la sécurité suivants en combinaison avec. GuardDuty

- AWS Security Hub— Ce service vous donne une vue complète de l'état de sécurité de vos AWS ressources et vous aide à vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Pour ce faire, il utilise, agrège, organise et hiérarchise les résultats de sécurité provenant de multiples AWS services (y

compris Amazon Macie) et de produits AWS pris en charge par le réseau APN de partenaires (). Security Hub vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires dans votre AWS environnement.

Pour plus d'informations sur GuardDuty l'utilisation conjointe de Security Hub, consultezIntégration GuardDuty avec AWS Security Hub. Pour en savoir plus sur Security Hub, consultez le guide de AWS Security Hub l'utilisateur.

- Amazon Detective : ce service vous permet d'analyser, d'enquêter et d'identifier rapidement la cause première des problèmes de sécurité ou des activités suspectes. Detective collecte automatiquement les données du journal à partir de vos AWS ressources. Detective utilise ensuite le machine learning, l'analyse statistique et la théorie des graphes pour générer des visualisations qui vous aideront à mener des investigations de sécurité plus rapides et plus efficaces. Les agrégations de données prédéfinies, les résumés et le contexte du Detective vous aident à analyser et à déterminer la nature et l'étendue des problèmes de sécurité potentiels.

  Pour plus d'informations sur l'utilisation conjointe de Detective GuardDuty et de Detective, consultezIntégration GuardDuty à Amazon Detective. Pour en savoir plus sur Detective, consultez le guide de l'utilisateur d'Amazon Detective.
- Amazon EventBridge — Ce service vous permet de recevoir des notifications et de répondre aux GuardDuty problèmes de sécurité en temps quasi réel. GuardDutycrée un événement en cas de modification des résultats. Vous pouvez choisir la fréquence à laquelle vous souhaitez recevoir les notifications EventBridge. Pour plus d'informations, consultez la section Qu'est-ce qu'Amazon EventBridge dans le guide de EventBridge l'utilisateur Amazon.

PCIDSSConformité

GuardDuty prend en charge le traitement, le stockage et la transmission des données de carte de crédit par un commerçant ou un fournisseur de services, et sa conformité à la norme de sécurité des données de l'industrie des cartes de paiement (PCI) a été validée (DSS). Pour plus d'informations PCIDSS, notamment sur la manière de demander une copie du Package de AWS PCI conformité, consultez le PCIDSSniveau 1.

Pour plus d'informations, consultez la section Nouveau test tiers comparant Amazon GuardDuty aux systèmes de détection d'intrusion sur le réseau dans le blog sur la AWS sécurité.

Tarification en GuardDuty

Niveau gratuit d'AWS vous permet d'explorer et d'essayer AWS services gratuitement jusqu'à des limites spécifiées pour chaque service. Il existe trois catégories : 12 mois gratuits, toujours gratuits et essais gratuits de courte durée. Amazon GuardDuty appartient à la catégorie des essais gratuits de courte durée et propose un essai gratuit de 30 jours. Lorsque vous continuez à utiliser ce GuardDuty service après la fin de cet essai gratuit, vous commencez à encourir des frais en fonction de la façon dont vous utilisez ce service.

L'analyse des programmes malveillants à la demande (sous Protection contre les programmes malveillants pourEC2) et la protection contre les logiciels malveillants pour S3 n'entrent pas dans la catégorie des essais gratuits de courte durée de GuardDuty 30 jours. La protection contre les programmes malveillants pour S3 entre dans la catégorie des 12 mois gratuits, Niveau gratuit d'AWS tandis que l'analyse des programmes malveillants à la demande suit un modèle de pay-as-you-use coût. Il n'existe pas d'essai gratuit de 30 jours ni de modèle de coût gratuit de 12 mois avec analyse des programmes malveillants à la demande. Pour plus d'informations, consultez GuardDuty les tarifs.

Utilisation de l' GuardDuty essai gratuit de 30 jours

Lorsque vous l'utilisez GuardDuty pour la première fois depuis une Région AWS, vous Compte AWS êtes automatiquement inscrit à un essai gratuit de 30 jours dans cette région. Certains plans de protection seront également activés automatiquement et sont inclus dans l'essai gratuit de 30 jours. Comme il GuardDuty s'agit d'un service régional, lorsque vous l'activez pour la première fois dans une autre région, votre compte bénéficie d'un essai gratuit de 30 jours GuardDuty et de certains plans de protection pris en charge dans cette région.

Lorsque vous travaillez avec plusieurs comptes au GuardDuty sein d'une entreprise, chaque compte bénéficie de son propre essai gratuit de 30 jours GuardDuty et de plans de protection.

Le tableau suivant indique quels plans de protection sont activés automatiquement lorsque vous GuardDuty les activez pour la première fois.

Plan de protection	Inclus dans l' GuardDuty essai gratuit de 30 jours	Possède son propre essai gratuit de 30 jours [1]	
EKSProtection	Oui	Oui	

Plan de protection	Inclus dans l' GuardDuty essai gratuit de 30 jours	Possède son propre essai gratuit de 30 jours [1]
Protection Lambda	Oui	Oui
Protection contre les logiciels malveillants pour EC2 – GuardDuty-analyse des logiciels malveillants initiée	Oui	Oui
Protection contre les logiciels malveillants pour EC2 – Analyse des logiciels malveillants à la demande	Non	Non
GuardDuty Protection contre les logiciels malveillants pour S3	Non	Non
RDSProtection	Oui	Oui
Surveillance d'exécution	Non	Oui
Protection S3	Oui	Oui

[1] Chaque plan de protection dispose de son propre essai gratuit. Par exemple, lorsque vous activez un plan de protection après l'expiration de l'essai gratuit de GuardDuty 30 jours pour votre compte et qu'un nouveau plan de protection est publié, vous pouvez activer ce plan de protection avec son propre essai gratuit. Pour plus d'informations sur les essais gratuits des plans de protection, consultez le document associé à chaque plan de protection.

Afficher le coût d'utilisation estimé pendant l'essai gratuit — Au cours de l'essai gratuit de 30 jours GuardDuty et éventuellement d'un plan de protection, GuardDuty fournit une estimation du coût

d'utilisation de votre compte. Si vous êtes un compte d' GuardDuty administrateur délégué, vous pouvez consulter le coût d'utilisation total estimé et la répartition au niveau du compte pour tous les comptes membres qui ont été activés. GuardDuty Pour de plus amples informations, veuillez consulter Estimation des GuardDuty coûts.

Coût d'utilisation après la fin de l'essai gratuit — Lorsque vous continuez à utiliser l' GuardDuty un de ses plans de protection après la fin de l'essai gratuit, vous commencerez à encourir des frais d'utilisation associés. Pour consulter votre facture, accédez à Cost Explorer dans la https://console.aws.amazon.com/billing/console. Pour plus d'informations sur la facturation du AWS compte, consultez le guide de AWS Billing l'utilisateur.

Utilisation de la protection contre les programmes malveillants pour S3 avec un niveau gratuit de 12 mois

Malware Protection for S3 utilise un plan gratuit associé à votre abonnement, Comptes AWS qu'il s'agisse d'un nouveau forfait, d'un niveau gratuit permanent ou d'un plan gratuit expiré de 12 mois. Pour de plus amples informations, veuillez consulter Tarification de la protection contre les programmes malveillants pour S3.

Accès GuardDuty

Vous pouvez l'utiliser GuardDuty de l'une des manières suivantes :

GuardDuty console

https://console.aws.amazon.com/guardduty/

La console est une interface basée sur un navigateur permettant d'y accéder et de l'utiliser. GuardDuty La GuardDuty console permet d'accéder à votre GuardDuty compte, à vos données et à vos ressources.

AWS outils de ligne de commande

Avec les outils de ligne de AWS commande, vous pouvez émettre des commandes sur la ligne de commande de votre système pour effectuer GuardDuty des tâches et AWS des tâches. Les outils de ligne de commande sont utiles si vous souhaitez créer des scripts exécutant des tâches.

Pour plus d'informations sur l'installation et l'utilisation AWS CLI, consultez le Guide de AWS Command Line Interface l'utilisateur. Pour consulter les AWS CLI commandes disponibles pour GuardDuty, consultez la référence des CLI commandes.

GuardDuty HTTPS API

Vous pouvez y accéder GuardDuty et par AWS programmation en utilisant le GuardDuty HTTPSAPI, qui vous permet d'envoyer des HTTPS demandes directement au service. Pour plus d'informations, consultez la GuardDuty APIréférence.

AWS SDKs

AWS fournit des kits de développement logiciel (SDKs) composés de bibliothèques et d'exemples de code pour divers langages de programmation et plateformes (Java, Python, Ruby,. NET, iOS, Android, etc.). Ils SDKs fournissent un moyen pratique de créer un accès programmatique à GuardDuty. Pour plus d'informations AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour Amazon Web Services.

Concepts et terminologie

Lorsque vous débutez avec Amazon GuardDuty, vous pouvez bénéficier de l'apprentissage de ses concepts clés.

Compte

Un compte Amazon Web Services (AWS) standard contenant vos AWS ressources. Vous pouvez vous connecter AWS à votre compte et l'activer GuardDuty.

Vous pouvez également inviter d'autres comptes à activer votre AWS compte GuardDuty et à s'y associer dans GuardDuty. Si vos invitations sont acceptées, votre compte est désigné comme GuardDuty compte administrateur et les comptes ajoutés deviennent vos comptes de membre. Vous pouvez ensuite consulter et gérer les GuardDuty résultats de ces comptes en leur nom.

Les utilisateurs du compte administrateur peuvent configurer GuardDuty , consulter et gérer les GuardDuty résultats pour leur propre compte et pour tous leurs comptes membres. Vous pouvez avoir jusqu'à 10 000 comptes de membres GuardDuty.

Les utilisateurs des comptes membres peuvent configurer GuardDuty , consulter et gérer les GuardDuty résultats de leur compte (via la console GuardDuty de gestion ou GuardDuty API). Les utilisateurs de comptes membres ne peuvent pas afficher ou gérer des résultats dans les comptes d'autres membres.

An ne Compte AWS peut pas être un compte GuardDuty administrateur et un compte membre en même temps. An ne Compte AWS peut accepter qu'une seule invitation d'adhésion. L'acceptation d'une invitation d'adhésion est facultative.

Pour de plus amples informations, veuillez consulter Gestion de plusieurs comptes sur Amazon GuardDuty.

Détecteur

Amazon GuardDuty est un service régional. Lorsque vous l'activez GuardDuty dans un domaine spécifique Région AWS, vous Compte AWS êtes associé à un identifiant de détecteur. Cet identifiant alphanumérique à 32 caractères est unique à votre compte dans cette région. Par exemple, lorsque vous activez GuardDuty le même compte dans une région différente, votre compte sera associé à un identifiant de détecteur différent. Le format de a detectorId est`12abc34d567e8fa901bc2d34e56789f0`.

Tous les GuardDuty résultats, comptes et actions relatifs à la gestion des résultats et au GuardDuty service utilisent l'identifiant du détecteur pour exécuter une API opération.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

> **Note**
>
> Dans des environnements à plusieurs comptes, tous les résultats destinés aux comptes membres sont associés au détecteur du compte administrateur.

Certaines GuardDuty fonctionnalités sont configurées via le détecteur, telles que la configuration de la fréquence de notification des CloudWatch événements et l'activation ou la désactivation de plans de protection facultatifs GuardDuty à traiter.

Utilisation de la protection contre les programmes malveillants pour S3 dans GuardDuty

Lorsque vous activez la protection contre les programmes malveillants pour S3 dans un compte où cette option GuardDuty est activée, les actions de protection contre les programmes malveillants pour S3 telles que l'activation, la modification et la désactivation d'une ressource protégée ne sont pas associées à l'ID du détecteur.

Lorsque vous n'activez pas GuardDuty et ne choisissez pas l'option de détection des menaces Malware Protection for S3, aucun identifiant de détecteur n'est créé pour votre compte.

Sources de données de base

Origine ou emplacement d'un ensemble de données. Pour détecter une activité non autorisée ou inattendue dans votre AWS environnement. GuardDuty analyse et traite les données provenant des journaux d' AWS CloudTrail événements, AWS CloudTrail des événements de gestion, AWS CloudTrail des événements de données pour S3, des journaux de VPC flux, DNS des journaux, voirGuardDuty sources de données de base.

Fonctionnalité

Un objet fonctionnel configuré pour votre plan de GuardDuty protection permet de détecter une activité non autorisée ou inattendue dans votre AWS environnement. Chaque plan de GuardDuty protection configure l'objet fonctionnel correspondant pour analyser et traiter les données. Certains des objets de fonctionnalité incluent les journaux EKS d'audit, la surveillance des

activités de RDS connexion, les journaux d'activité du réseau Lambda et EBS les volumes. Pour de plus amples informations, veuillez consulter Activation des fonctionnalités dans GuardDuty.

Résultat

Un problème potentiel de sécurité a été détecté par GuardDuty. Pour de plus amples informations, veuillez consulter Comprendre les GuardDuty résultats d'Amazon.

Les résultats sont affichés dans la GuardDuty console et contiennent une description détaillée du problème de sécurité. Vous pouvez également récupérer les résultats que vous avez générés en appelant les ListFindingsAPIopérations GetFindingset.

Vous pouvez également consulter vos GuardDuty résultats par le biais CloudWatch des événements Amazon. GuardDuty envoie les résultats à Amazon CloudWatch via un HTTPS protocole. Pour de plus amples informations, veuillez consulter Création de réponses personnalisées aux GuardDuty résultats avec Amazon CloudWatch Events.

IAMrôle

Il s'agit du IAM rôle disposant des autorisations requises pour scanner l'objet S3. Lorsque le balisage des objets numérisés est activé, les IAM PassRole autorisations permettent d' GuardDuty ajouter des balises à l'objet numérisé.

Ressource du plan de protection contre les logiciels

Une fois que vous avez activé la protection contre les programmes malveillants pour S3 pour un compartiment, vous GuardDuty créez une ressource de protection contre les programmes malveillants pour le EC2 plan. Cette ressource est associée à Malware Protection for EC2 plan ID, un identifiant unique pour votre compartiment protégé. Utilisez la ressource du plan Malware Protection pour effectuer API des opérations sur une ressource protégée.

Compartiment protégé (ressource protégée)

Un compartiment Amazon S3 est considéré comme protégé lorsque vous activez Malware Protection for S3 pour ce compartiment et que son statut de protection passe à Active.

GuardDuty prend uniquement en charge un compartiment S3 en tant que ressource protégée.

État de protection

État associé à la ressource de votre plan de protection contre les programmes malveillants. Une fois que vous avez activé Malware Protection for S3 pour votre compartiment, cet état indique si votre compartiment est correctement configuré ou non.

Préfixe d'objet S3

Dans un bucket Amazon Simple Storage Service (Amazon S3), vous pouvez utiliser des préfixes pour organiser votre stockage. Un préfixe est un regroupement logique des objets d'un compartiment S3. Pour plus d'informations, consultez la section Organisation et mise en liste des objets dans le guide de l'utilisateur Amazon S3.

Options de numérisation

Lorsque GuardDuty Malware Protection for EC2 est activée, elle vous permet de spécifier les EC2 instances Amazon et les volumes Amazon Elastic Block Store (EBS) à scanner ou à ignorer. Cette fonctionnalité vous permet d'ajouter les balises existantes associées à vos EC2 instances et à votre EBS volume à une liste de balises d'inclusion ou à une liste de balises d'exclusion. Les ressources associées aux balises que vous ajoutez à une liste de balises d'inclusion sont analysées pour détecter les logiciels malveillants, et celles ajoutées à une liste de balises d'exclusion ne sont pas analysées. Pour de plus amples informations, veuillez consulter Options d'analyse avec balises définies par l'utilisateur.

Conservation des instantanés

Lorsque la protection contre les GuardDuty logiciels malveillants EC2 est activée, elle propose une option permettant de conserver les instantanés de vos EBS volumes dans votre AWS compte. GuardDuty génère les EBS volumes de réplication en fonction des instantanés de vos EBS volumes. Vous ne pouvez conserver les instantanés de vos EBS volumes que si la protection contre les programmes malveillants à des fins d'EC2analyse détecte des logiciels malveillants dans les EBS volumes répliqués. Si aucun logiciel malveillant n'est détecté dans les EBS volumes de réplication, supprime GuardDuty automatiquement les instantanés de vos EBS volumes, quel que soit le paramètre de conservation des instantanés. Pour de plus amples informations, veuillez consulter Conservation des instantanés.

Règle de suppression

Les règles de suppression vous permettent de créer des combinaisons d'attributs très spécifiques pour supprimer des résultats. Par exemple, vous pouvez définir une règle via le GuardDuty filtre pour archiver automatiquement `Recon:EC2/Portscan` uniquement les instances d'une balise spécifiqueVPC, en cours d'exécution ou avec une EC2 balise spécifique. AMI Cette règle entraînerait l'archivage automatique des résultats d'analyse de port depuis les instances qui répondent aux critères. Cependant, il permet toujours d'émettre des alertes s'il GuardDuty détecte des instances menant d'autres activités malveillantes, telles que le minage de cryptomonnaies.

Les règles de suppression définies dans le compte GuardDuty administrateur s'appliquent aux comptes des GuardDuty membres. GuardDuty les comptes membres ne peuvent pas modifier les règles de suppression.

Avec les règles de suppression, génère GuardDuty toujours tous les résultats. Les règles de suppression permettent de supprimer des résultats tout en conservant un historique immuable et complet de toute l'activité.

En général, les règles de suppression sont utilisées pour masquer les résultats que vous avez déterminés comme faux positifs pour votre environnement et limitent les perturbations provenant des résultats de faible valeur afin de vous permettre de vous concentrer sur les menaces plus importantes. Pour de plus amples informations, veuillez consulter Règles de suppression.

Liste d'adresses IP approuvées

Une liste d'adresses IP fiables pour une communication hautement sécurisée avec votre AWS environnement. GuardDuty ne génère pas de résultats basés sur des listes d'adresses IP fiables. Pour de plus amples informations, veuillez consulter Utilisation de listes d'adresses IP approuvées et de listes de menaces.

Liste d'adresses IP de menaces

Liste d'adresses IP malveillantes. En plus de générer des résultats en raison d'une activité potentiellement suspecte, il génère GuardDuty également des résultats basés sur ces listes de menaces. Pour de plus amples informations, veuillez consulter Utilisation de listes d'adresses IP approuvées et de listes de menaces.

Commencer avec GuardDuty

Ce didacticiel fournit une introduction pratique à GuardDuty. Les exigences minimales pour l'activation GuardDuty en tant que compte autonome ou en tant qu' GuardDuty administrateur AWS Organizations sont décrites à l'étape 1. Les étapes 2 à 5 couvrent l'utilisation des fonctionnalités supplémentaires recommandées par GuardDuty pour tirer le meilleur parti de vos résultats.

Rubriques

Avant de commencer

GuardDuty est un service de détection des menaces qui surveille GuardDuty sources de données de base notamment les journaux d' AWS CloudTrail événements, les événements AWS CloudTrail de gestion, les journaux Amazon VPC Flow et DNS les journaux. GuardDuty analyse également les fonctionnalités associées à ses types de protection uniquement si vous les activez séparément. Les fonctionnalités incluent les journaux d'audit Kubernetes, l'activité de RDS connexion, les journaux S3, les EBS volumes, la surveillance du temps d'exécution et les journaux d'activité réseau Lambda. L'utilisation de ces sources de données et de ces fonctionnalités (si elles sont activées) GuardDuty génère des résultats de sécurité pour votre compte.

Une fois que vous l'avez activé GuardDuty, il commence à surveiller votre environnement. Vous pouvez le désactiver GuardDuty pour n'importe quel compte dans n'importe quelle région, à tout moment. Cela GuardDuty empêchera le traitement des sources de données de base et de toutes les fonctionnalités activées séparément.

Vous n'avez pas besoin d'activer l'une des options des GuardDuty sources de données de base de manière explicite. Amazon GuardDuty extrait des flux de données indépendants directement à partir de ces services. Pour un nouveau GuardDuty compte, tous les types de protection disponibles pris en charge dans un Région AWS sont activés et inclus par défaut dans la période d'essai gratuite de 30 jours. Vous pouvez choisir de toutes les refuser ou seulement l'une d'entre elles. Si vous êtes déjà

GuardDuty client, vous pouvez choisir d'activer tout ou partie des plans de protection disponibles dans votre Région AWS. Pour plus d'informations, consultez la section Fonctionnalités associées à chaque type de protection dans GuardDuty.

Lors de l'activation GuardDuty, tenez compte des points suivants :

- GuardDuty est un service régional, ce qui signifie que toutes les procédures de configuration que vous suivez sur cette page doivent être répétées dans chaque région que vous souhaitez surveiller GuardDuty.

  Nous vous recommandons vivement de l'activer GuardDuty dans toutes les AWS régions prises en charge. Cela permet GuardDuty de générer des informations sur des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. Cela permet également GuardDuty de surveiller les AWS CloudTrail événements pour AWS des services mondiaux tels queIAM. S'il n' GuardDuty est pas activé dans toutes les régions prises en charge, sa capacité à détecter les activités impliquant des services internationaux est réduite. Pour une liste complète des régions où cette GuardDuty offre est disponible, voirRégions et points de terminaison.
- Tout utilisateur disposant de privilèges d'administrateur sur un AWS compte peut l'activer. Toutefois GuardDuty, conformément à la meilleure pratique de sécurité du privilège minimal, il est recommandé de créer un IAM rôle, un utilisateur ou un groupe à gérer GuardDuty spécifiquement. Pour plus d'informations sur les autorisations requises pour l'activation, GuardDuty consultezAutorisations requises pour activer GuardDuty.
- Lorsque vous l'activez GuardDuty pour la première fois Région AWS, par défaut, tous les types de protection disponibles pris en charge dans cette région sont également activés, y compris la protection contre les programmes malveillants pourEC2. GuardDuty crée un rôle lié à un service pour votre compte appelé. `AWSServiceRoleForAmazonGuardDuty` Ce rôle inclut les autorisations et les politiques de confiance qui permettent de GuardDuty consommer et d'analyser les événements directement à partir du GuardDuty sources de données de base pour générer des résultats de sécurité. Malware Protection for EC2 crée un autre rôle lié à un service pour votre compte appelé. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Ce rôle inclut les autorisations et les politiques de confiance qui permettent à Malware Protection d'EC2effectuer des analyses sans agent afin de détecter les logiciels malveillants dans votre GuardDuty compte. Il permet GuardDuty de créer un instantané EBS du volume dans votre compte et de partager cet instantané avec le compte GuardDuty de service. Pour de plus amples informations, veuillez consulter Autorisations de rôle liées à un service pour GuardDuty. Pour de plus amples informations sur les rôles liés à un service, veuillez consulter Utilisation des rôles liés à un service.

- Lorsque vous l'activez GuardDuty pour la première fois dans une région, votre AWS compte est automatiquement inscrit à un essai GuardDuty gratuit de 30 jours pour cette région.

Mise en route : activation d'Amazon GuardDuty pour les environnements autonomes ou multi-comptes

Étape 1 : activer Amazon GuardDuty

La première étape pour l'utiliser GuardDuty est de l'activer dans votre compte. Une fois activé, GuardDuty il commencera immédiatement à surveiller les menaces de sécurité dans la région actuelle.

Si vous souhaitez gérer les GuardDuty résultats d'autres comptes au sein de votre organisation en tant qu' GuardDuty administrateur, vous devez ajouter des comptes membres et GuardDuty les activer également.

> **Note**
>
> Si vous souhaitez activer la protection contre les GuardDuty programmes malveillants pour S3 sans l'activer GuardDuty, consultez la procédure à suivreGuardDuty Protection contre les logiciels malveillants pour S3.

Standalone account environment

1. Ouvrez la GuardDuty console à https://console.aws.amazon.com/guardduty/
2. Sélectionnez l'option Amazon GuardDuty - Toutes les fonctionnalités.
3. Choisissez Démarrer.
4. Sur la GuardDuty page Bienvenue, consultez les conditions de service. Choisissez Activer GuardDuty.

Multi-account environment

> **Important**
>
> Comme condition préalable à ce processus, vous devez appartenir à la même organisation que tous les comptes que vous souhaitez gérer et avoir accès au compte de AWS Organizations gestion afin de déléguer un administrateur GuardDuty au sein de votre organisation. Des autorisations supplémentaires peuvent être nécessaires pour déléguer un administrateur. Pour plus d'informations, veuillez consulter Autorisations requises pour désigner un compte d' GuardDuty administrateur délégué.

Pour désigner un compte d' GuardDuty administrateur délégué

1. Ouvrez la AWS Organizations console à l'adresse https://console.aws.amazon.com/organizations/, à l'aide du compte de gestion.
2. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Est-ce GuardDuty déjà activé dans votre compte ?

   - Si GuardDuty ce n'est pas déjà fait, vous pouvez sélectionner Commencer, puis désigner un administrateur GuardDuty délégué sur la GuardDuty page Bienvenue sur la page de bienvenue.
   - Si cette option GuardDuty est activée, vous pouvez désigner un administrateur GuardDuty délégué sur la page Paramètres.
3. Entrez l'identifiant de AWS compte à douze chiffres du compte que vous souhaitez désigner comme administrateur GuardDuty délégué de l'organisation et choisissez Déléguer.

   > **Note**
   >
   > Si GuardDuty ce n'est pas déjà fait, la désignation d'un administrateur délégué sera activée GuardDuty pour ce compte dans votre région actuelle.

Pour ajouter un compte membre

Cette procédure couvre l'ajout de comptes de membres à un compte d'administrateur GuardDuty délégué via AWS Organizations. Il est également possible d'ajouter des membres sur

invitation. Pour en savoir plus sur les deux méthodes d'association de membres GuardDuty, consultezGestion de plusieurs comptes sur Amazon GuardDuty.

1. Connexion au compte administrateur délégué
2. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
3. Dans le panneau de navigation, choisissez Settings (Paramètres), puis Accounts (Comptes).

   La table des comptes répertorie tous les comptes de l'organisation.
4. Choisissez les comptes que vous souhaitez ajouter en tant que membres en cochant la case située à côté de l'ID du compte. Ensuite, dans le menu Action, sélectionnez Ajouter un membre.

> **Tip**
>
> Vous pouvez automatiser l'ajout de nouveaux comptes en tant que membres en activant la fonctionnalité Activation automatique. Toutefois, cela ne s'applique qu'aux comptes qui rejoignent votre organisation une fois cette fonctionnalité activée.

Étape 2 : générer des exemples de résultats et explorer les opérations de base

Lorsqu'il GuardDuty découvre un problème de sécurité, il génère une constatation. Une GuardDuty constatation est un ensemble de données contenant des informations relatives à ce problème de sécurité unique. Les détails du résultat peuvent être utilisés pour vous aider à examiner le problème.

GuardDuty permet de générer des exemples de résultats à l'aide de valeurs d'espace réservé, qui peuvent être utilisées pour tester les GuardDuty fonctionnalités et vous familiariser avec les résultats avant de devoir répondre à un véritable problème de sécurité découvert par GuardDuty. Suivez le guide ci-dessous pour générer des exemples de résultats pour chaque type de recherche disponible dans GuardDuty. Pour découvrir d'autres méthodes de génération d'échantillons de résultats, notamment la génération d'un événement de sécurité simulé dans votre compte, voirExemples de résultats.

Pour créer et explorer des exemples de résultats

1. Dans le panneau de navigation, sélectionnez Settings (Paramètres).

2. Sur la page Settings, sous Sample findings, choisissez Generate sample findings.
3. Dans le volet de navigation, choisissez Résumé pour afficher les informations relatives aux résultats générés dans votre AWS environnement. Pour de plus amples informations sur les composants du tableau de bord récapitulatif, veuillez consulter Tableau de bord récapitulatif.
4. Dans le volet de navigation, choisissez Conclusions. Les exemples de résultats sont affichés sur la page Résultats actuels avec le préfixe [SAMPLE].
5. Sélectionnez un résultat dans la liste pour en afficher les détails.

    - Vous pouvez consulter les différents champs d'informations disponibles dans le volet des informations du résultat. Les différents types de résultat peuvent avoir différents champs. Pour de plus amples informations sur les champs disponibles dans tous les types de résultat, veuillez consulter Détails d'un résultat. Depuis le volet des détails, vous pouvez effectuer les actions suivantes :

        - Sélectionnez l'ID de recherche en haut du volet pour ouvrir les JSON détails complets de la recherche. Le JSON dossier complet peut également être téléchargé depuis ce panneau. Le JSON contient des informations supplémentaires non incluses dans l'affichage de la console et est le format qui peut être ingéré par d'autres outils et services.
        - Veuillez consulter la section Ressource affectée. En cas de véritable découverte, les informations présentées ici vous aideront à identifier une ressource de votre compte qui devrait faire l'objet d'une enquête et incluront des liens vers les ressources appropriées AWS Management Console pour des actions.
        - Sélectionnez les icônes de loupe + ou - afin de créer un filtre inclusif ou exclusif pour chaque détail. Pour plus d'informations sur la recherche de filtres, veuillez consulter Filtrage des résultats.
6. Archivage de tous vos exemples de résultats

    a. Sélectionnez tous les résultats en cochant la case en haut de la liste.

    b. Désélectionnez les résultats que vous souhaitez conserver.

    c. Sélectionnez le menu Actions, puis Archiver pour masquer les exemples de résultats.

    > **Note**
    >
    > Pour afficher les résultats archivés, sélectionnez Actuel, puis Archivé pour changer d'affichage des résultats.

Étape 3 : configurer l'exportation GuardDuty des résultats vers un compartiment Amazon S3

GuardDuty recommande de configurer les paramètres pour exporter les résultats, car cela vous permet d'exporter vos résultats vers un compartiment S3 pour un stockage indéfini au-delà de la période de conservation de GuardDuty 90 jours. Cela vous permet de conserver des enregistrements des résultats ou de suivre les problèmes rencontrés dans votre AWS environnement au fil du temps. Le processus décrit ici vous explique comment configurer un nouveau compartiment S3 et créer une nouvelle KMS clé pour chiffrer les résultats depuis la console. Pour plus d'informations à ce sujet, notamment sur la façon d'utiliser votre propre compartiment existant ou un compartiment d'un autre compte, veuillez consulter Exportation des résultats.

Pour configurer l'option d'exportation des résultats dans S3

1. Pour chiffrer les résultats, vous aurez besoin d'une KMS clé dotée d'une politique autorisant l'utilisation GuardDuty de cette clé pour le chiffrement. Les étapes suivantes vous aideront à créer une nouvelle KMS clé. Si vous utilisez une KMS clé d'un autre compte, vous devez appliquer la politique en matière de clés en vous connectant au Compte AWS propriétaire de la clé. La région de votre KMS clé et de votre compartiment S3 doit être identique. Toutefois, vous pouvez utiliser ce même compartiment et cette même paire de clés pour chaque région à partir de laquelle vous souhaitez exporter les résultats.

   a. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.

   b. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.

   c. Dans le volet de navigation, sélectionnez Clés gérées par le client.

   d. Choisissez Create key.

   e. Choisissez Symétrique sous Type de clé, puis Suivant.

      > **Note**
      >
      > Pour connaître les étapes détaillées relatives à la création de votre KMS clé, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.

   f. Fournissez un alias pour votre clé, puis choisissez Suivant.

g. Choisissez Suivant, puis à nouveau Suivant pour accepter les autorisations d'administration et d'utilisation par défaut.

h. Une fois que vous avez fini de vérifier la configuration, choisissez Terminer pour créer la clé.

i. Sur la page Clés gérées par le client, choisissez votre alias de clé.

j. Dans la section Stratégie de clé, sélectionnez Passer à la vue de stratégie.

k. Choisissez Modifier et ajoutez la politique clé suivante à votre KMS clé, en accordant l' GuardDuty accès à votre clé. Cette instruction permet GuardDuty d'utiliser uniquement la clé à laquelle vous ajoutez cette politique. Lorsque vous modifiez la politique clé, assurez-vous que la JSON syntaxe est valide. Si vous ajoutez l'instruction avant la dernière instruction, vous devez ajouter une virgule après le crochet de fermeture.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
}
```

Remplacez *Region1* avec la région de votre KMS clé. Remplacez *444455556666* avec celui Compte AWS qui détient la KMS clé. Remplacez *KMSKeyId* avec l'ID de la KMS clé que vous avez choisie pour le chiffrement. Pour identifier toutes ces valeurs (région et identifiant de clé), consultez le code ARNde votre KMS clé. Compte AWS Pour localiser la cléARN, voir Trouver l'identifiant de la clé et ARN.

De même, remplacez *111122223333* avec Compte AWS le GuardDuty compte. Remplacez *Region2* avec la région du GuardDuty compte. Remplacez *SourceDetectorID* avec l'identifiant du détecteur du GuardDuty compte pour *Region2*.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

l. Choisissez Save (Enregistrer).

2. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
3. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
4. Sous Options d'exportation des résultats, choisissez Configurer maintenant.
5. Choisissez Nouveau compartiment. Indiquez un nom unique pour votre compartiment S3.
6. (Facultatif) Vous pouvez tester vos nouveaux paramètres d'exportation en générant des exemples de résultats. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
7. Sous la section Exemples de résultats, choisissez Générer des exemples de résultats. Les nouveaux échantillons de résultats apparaîtront sous forme d'entrées dans le compartiment S3 créé GuardDuty dans un délai maximum de cinq minutes.

Étape 4 : Configurez les alertes de GuardDuty recherche via SNS

GuardDuty s'intègre à Amazon EventBridge, qui peut être utilisé pour envoyer les données des résultats à d'autres applications et services à des fins de traitement. EventBridge Vous pouvez utiliser GuardDuty les résultats pour initier des réponses automatiques à vos résultats en connectant les événements de recherche à des cibles telles que AWS Lambda les fonctions, l'automatisation d'Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS), etc.

Dans cet exemple, vous allez créer un SNS sujet qui sera la cible d'une EventBridge règle, puis vous l'utiliserez EventBridge pour créer une règle qui capture les données de résultats GuardDuty. La règle qui en résulte transmet les détails du résultat à une adresse e-mail. Pour savoir comment envoyer des résultats à Slack ou Amazon Chime, et comment modifier les types de résultat pour lesquels les alertes sont envoyées, veuillez consulter Configurer une rubrique Amazon SNS et un point de terminaison.

Pour créer un SNS sujet pour vos alertes de résultats

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans le volet de navigation, choisissez Rubriques.
3. Choisissez Créer la rubrique.

4. Pour Type, sélectionnez Standard.
5. Pour Name (Nom), saisissez **`GuardDuty`**.
6. Choisissez Créer la rubrique. Les détails de la rubrique pour votre nouvelle rubrique s'ouvrent.
7. Dans la section Abonnements, choisissez Créer un abonnement.
8. Pour Protocole, choisissez E-mail.
9. Pour Point de terminaison, saisissez l'adresse e-mail à laquelle vous souhaitez envoyer des notifications.
10. Choisissez Create subscription (Créer un abonnement).

    Vous devez confirmer votre abonnement par e-mail après avoir créé l'abonnement.
11. Pour vérifier la présence d'un message d'abonnement, accédez à votre boîte de réception et, dans le message d'abonnement, sélectionnez Confirmer l'abonnement.

> **Note**
>
> Pour vérifier le statut de l'e-mail de confirmation, accédez à la SNS console et choisissez Abonnements.

Pour créer une EventBridge règle permettant de saisir les GuardDuty résultats et de les mettre en forme

1. Ouvrez la EventBridge console à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Règles.
3. Choisissez Créer une règle.
4. Saisissez un nom et une description pour la règle.

   Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.
5. Pour Event bus (Bus d'événement), choisissez default (défaut).
6. Pour Type de règle, choisissez Règle avec un modèle d'événement.
7. Choisissez Suivant.
8. Pour Event source (Source de l'événement), choisissez AWS events (Événements).
9. Pour Modèle d'événement, choisissez Formulaire de modèle d'événement.

10. Pour Source d'événement, choisissez Services AWS .
11. Pour Service AWS , choisissez GuardDuty.
12. Dans Type d'événement, choisissez GuardDutyRechercher.
13. Choisissez Suivant.
14. Pour Types de cibles, choisissez service AWS .
15. Pour Sélectionner une cible, choisissez un SNSsujet, et pour Sujet, choisissez le nom du SNS sujet que vous avez créé précédemment.
16. Dans la section Paramètres supplémentaires, pour Configurer l'entrée cible, choisissez Transformateur d'entrée.

    L'ajout d'un transformateur d'entrée formate les données de JSON recherche envoyées GuardDuty en un message lisible par l'homme.
17. Choisissez Configure input transformer (Configurer le transformateur d'entrée).
18. Dans la section Transformateur d'entrée cible, pour Chemin d'entrée, collez le code suivant :

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. Pour formater l'e-mail, dans Modèle, collez le code suivant et assurez-vous de remplacer le texte en rouge par les valeurs appropriées à votre région :

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Choisissez Confirmer.
21. Choisissez Suivant.

22. (Facultatif) Saisissez une ou plusieurs balises pour la règle. Pour plus d'informations, consultez les EventBridge balises Amazon dans le guide de EventBridge l'utilisateur Amazon.
23. Choisissez Suivant.
24. Consultez les détails de la règle et choisissez Create rule (Créer une règle).
25. (Facultatif) Testez votre nouvelle règle en générant des exemples de résultats à l'aide du processus de l'étape 2. Vous recevrez un e-mail pour chaque exemple de résultat généré.

Étapes suivantes

Au fur et à mesure que vous continuerez à l'utiliser GuardDuty, vous comprendrez quels types de résultats sont pertinents pour votre environnement. Chaque fois que vous recevez un nouveau résultat, vous pouvez trouver des informations, notamment des recommandations de correction concernant ce résultat, en sélectionnant En savoir plus dans la description du résultat dans le volet des détails du résultat, ou en recherchant le nom du résultat sur Types de résultats.

Les fonctionnalités suivantes vous aideront à le régler de GuardDuty manière à ce qu'il puisse fournir les résultats les plus pertinents pour votre AWS environnement :

- Pour trier facilement les résultats en fonction de critères spécifiques, tels que l'ID d'instance, l'ID de compte, le nom du compartiment S3, etc., vous pouvez créer et enregistrer des filtres à l'intérieur de celui-ci GuardDuty. Pour de plus amples informations, veuillez consulter Filtrage des résultats.
- Si vous recevez des résultats concernant le comportement attendu dans votre environnement, vous pouvez automatiquement archiver les résultats en fonction des critères que vous définissez à l'aide des règles de suppression.
- Pour éviter que des résultats ne soient générés à partir d'un sous-ensemble de sites fiablesIPs, ou pour que le GuardDuty monitoring IPs sorte de son champ de surveillance normal, vous pouvez configurer des adresses IP fiables et des listes de menaces.

GuardDuty sources de données de base

GuardDuty utilise les sources de données de base pour détecter les communications avec des domaines et adresses IP malveillants connus, et identifier les comportements potentiellement anormaux et les activités non autorisées. Pendant le transfert entre ces sources et GuardDuty, toutes les données du journal sont cryptées. GuardDutyextrait différents champs de ces sources de journaux à des fins de profilage et de détection d'anomalies, puis supprime ces journaux.

Lorsque vous l'activez GuardDuty pour la première fois dans une région, un essai gratuit de 30 jours inclut la détection des menaces pour toutes les sources de données de base. Au cours de cet essai gratuit, vous pouvez suivre une estimation de l'utilisation mensuelle ventilée par source de données de base. En tant que compte d' GuardDuty administrateur délégué, vous pouvez consulter le coût d'utilisation mensuel estimé ventilé par compte de membre qui appartient à votre organisation et qui a été activé GuardDuty. Une fois la période d'essai de 30 jours terminée, vous pouvez AWS Billing demander des informations sur le coût d'utilisation.

Il n'y a aucun coût supplémentaire pour GuardDuty accéder aux événements et aux journaux à partir de ces sources de données fondamentales.

Une fois que vous l'avez activé GuardDuty dans votre Compte AWS, il commence automatiquement à surveiller les sources de journaux expliquées dans les sections suivantes. Vous n'avez rien d'autre à activer pour commencer GuardDuty à analyser et à traiter ces sources de données afin de générer les résultats de sécurité associés.

Rubriques

AWS CloudTrail événements de gestion

AWS CloudTrail vous fournit un historique des AWS API appels relatifs à votre compte, y compris les API appels passés à l' AWS Management Console aide des outils de ligne de commande et de certains AWS services. AWS SDKs CloudTrail vous aide également à identifier les utilisateurs et les comptes invoqués AWS APIs pour les services pris en charge CloudTrail, l'adresse IP source à partir de laquelle les appels ont été appelés et l'heure à laquelle les appels ont été appelés. Pour de plus

amples informations, veuillez consulter Présentation de AWS CloudTrail dans le Guide de l'utilisateur AWS CloudTrail .

GuardDuty surveille les événements CloudTrail de gestion, également appelés événements du plan de contrôle. Ces événements fournissent un aperçu des opérations de gestion effectuées sur les ressources de votre AWS compte.

Voici des exemples d'événements de CloudTrail gestion GuardDuty surveillés :

- Configuration de la sécurité (IAM`AttachRolePolicy`APIopérations)
- Configuration des règles pour les données de routage (EC2`CreateSubnet`APIopérations Amazon)
- Configuration de la journalisation (AWS CloudTrail `CreateTrail`APIopérations)

Lorsque vous l'activez GuardDuty, il commence à consommer CloudTrail des événements de gestion directement CloudTrail via un flux d'événements indépendant et dupliqué et analyse vos CloudTrail journaux d'événements.

GuardDuty ne gère pas vos CloudTrail événements et n'affecte pas vos CloudTrail configurations existantes. De même, vos CloudTrail configurations n'affectent pas la façon dont les journaux d'événements sont GuardDuty consommés et traités. Pour gérer l'accès et la rétention de vos CloudTrail événements, utilisez la console CloudTrail de service ouAPI. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements dans le Guide de AWS CloudTrail l'utilisateur.

Comment GuardDuty gère les événements AWS CloudTrail mondiaux

Pour la plupart AWS des services, les CloudTrail événements sont enregistrés Région AWS là où ils ont été créés. Pour les services internationaux tels que AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon et CloudFront Amazon Route 53 (Route 53), les événements ne sont générés que dans la région où ils se produisent, mais ils ont une importance mondiale.

Lorsqu'il GuardDuty consomme des événements de service CloudTrail globaux ayant une valeur de sécurité, tels que des configurations réseau ou des autorisations utilisateur, il reproduit ces événements et les traite dans chaque région où vous les avez activés GuardDuty. Ce comportement permet de GuardDuty maintenir les profils des utilisateurs et des rôles dans chaque région, ce qui est essentiel pour détecter les événements anormaux.

Nous vous recommandons vivement d'activer GuardDuty tous ceux Régions AWS qui sont activés pour votre Compte AWS. Cela permet GuardDuty de détecter des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez peut-être pas activement.

Journaux de flux VPC

La fonctionnalité VPC Flow Logs d'Amazon VPC capture des informations sur le trafic IP en provenance et à destination des interfaces réseau connectées aux instances Amazon Elastic Compute Cloud (AmazonEC2) au sein de votre AWS environnement.

Lorsque vous l'activez GuardDuty, il commence immédiatement à analyser vos journaux de VPC flux à partir EC2 des instances Amazon de votre compte. Il consomme les événements des journaux de VPC flux directement depuis la fonctionnalité VPC Flow Logs via un flux indépendant et dupliqué de journaux de flux. Ce processus n'affecte pas les éventuelles configurations de journaux de flux existantes.

Protection Lambda

La protection Lambda est une amélioration facultative d'Amazon. GuardDuty À l'heure actuelle, Lambda Network Activity Monitoring inclut les journaux de VPC flux Amazon relatifs à toutes les fonctions Lambda de votre compte, même ceux qui n'utilisent pas le réseau. VPC Pour protéger votre fonction Lambda contre les menaces de sécurité potentielles, vous devez configurer la protection Lambda dans votre compte. GuardDuty Pour de plus amples informations, veuillez consulter Protection Lambda.

GuardDuty Surveillance du temps d'exécution

Lorsque vous gérez l'agent de sécurité (manuellement ou via GuardDuty) dans EKS Runtime Monitoring ou Runtime Monitoring pour les EC2 instances, et qu'GuardDuty il est actuellement déployé sur une EC2 instance Amazon et que vous le recevez Types d'événement d'exécution collectés de cette instance, l'analyse Compte AWS des journaux de VPC flux provenant de cette EC2 instance Amazon ne vous GuardDuty sera pas facturée. Cela permet GuardDuty d'éviter le double coût d'utilisation sur le compte.

GuardDuty ne gère pas vos journaux de flux et ne les rend pas accessibles dans votre compte. Pour gérer l'accès à vos journaux de flux et leur conservation, vous devez configurer la fonctionnalité VPC Flow Logs.

Journaux de requêtes du résolveur DNS Route53

Si vous utilisez des AWS DNS résolveurs pour vos EC2 instances Amazon (paramètre par défaut), vous GuardDuty pouvez accéder aux journaux de DNS requêtes Route53 Resolver et les traiter via les résolveurs internes. AWS DNS Si vous utilisez un autre DNS résolveur, tel qu'Open DNS ou GoogleDNS, ou si vous configurez vos propres DNS résolveurs, vous GuardDuty ne pourrez pas accéder aux données de cette source de données et les traiter.

Lorsque vous l'activez GuardDuty, il commence immédiatement à analyser vos journaux de DNS requêtes Route53 Resolver à partir d'un flux de données indépendant. Ce flux de données est distinct des données fournies par le biais de la fonctionnalité Journalisation des requêtes de résolveur de Route 53. La configuration de cette fonctionnalité n'affecte pas GuardDuty l'analyse.

> **Note**
>
> GuardDuty ne prend pas en charge DNS les journaux de surveillance pour les EC2 instances Amazon lancées AWS Outposts car la fonctionnalité de journalisation des Amazon Route 53 Resolver requêtes n'est pas disponible dans cet environnement.

Activation des fonctionnalités dans GuardDuty

Lorsque vous activez Amazon GuardDuty pour la première fois ou que vous activez un type de protection dans celui-ci GuardDuty, GuardDuty commence à traiter le type correspondant Source de données de base dans votre AWS environnement. GuardDuty utilise ces sources de données pour traiter un flux d'événements, tels que les journaux de VPC flux, les DNS journaux et les journaux d' AWS CloudTrail événements et de gestion. Il analyse ensuite ces événements pour identifier les menaces de sécurité potentielles et génère des résultats dans votre compte.

Outre les sources de données de journalisation, GuardDuty vous pouvez utiliser des données supplémentaires provenant d'autres AWS services de votre AWS environnement pour surveiller et analyser les menaces de sécurité potentielles.

Activation de fonctionnalité

Lorsque vous ajoutez des GuardDuty protections supplémentaires, par exemple S3 Protection, Runtime Monitoring ou EKS Protection, vous pouvez configurer la GuardDuty fonctionnalité correspondant au type de protection. Historiquement, GuardDuty les protections étaient appelées `dataSources` dans leAPIs. Cependant, après mars 2023, les nouveaux types de GuardDuty protection sont désormais configurés comme tels `features` ou non`dataSources`. GuardDuty prend toujours en charge la configuration des types de protection lancés avant mars 2023, comme `dataSources` par le biais duAPI, mais les nouveaux types de protection ne sont disponibles que sous forme de`features`.

Si vous gérez les types de GuardDuty configuration et de protection par le biais de la console, vous n'êtes pas directement concerné par cette modification et vous n'avez aucune action à entreprendre. L'activation des fonctionnalités affecte le comportement des types APIs invoqués pour activer GuardDuty ou protéger les types de protection qu'ils contiennent GuardDuty. Pour de plus amples informations, veuillez consulter GuardDuty APImodifications.

GuardDuty APImodifications en mars 2023

Les fonctionnalités de protection GuardDuty APIs configurées qui ne figurent pas dans la liste desGuardDuty sources de données de base. Un objet de fonctionnalité contient les détails des fonctionnalités, tels que le nom et l'état de la fonctionnalité, et peut contenir une configuration supplémentaire pour certaines fonctionnalités. Cette migration affecte les éléments suivants APIs dans la GuardDuty APIréférence Amazon :

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Activation des fonctionnalités par rapport aux sources de données

Historiquement, toutes les GuardDuty fonctionnalités passaient par un `dataSources` objet dans leAPI. À partir de mars 2023, GuardDuty préfère `features` l'objet au lieu de l'`dataSources`objet dans leAPI. Toutes les sources de données antérieures possèdent des fonctionnalités correspondantes, mais il se peut que les fonctionnalités plus récentes n'en aient pas.

La liste suivante montre la comparaison entre `dataSources` un `features` objet lorsqu'il est passé par un API :

- L'objet `dataSources` contient des objets pour chaque type de protection et son état. L'`features`objet est une liste des fonctionnalités disponibles correspondant à chaque type de protection qu'il contient GuardDuty.

  À compter de mars 2023, l'activation des fonctionnalités sera le seul moyen de configurer de nouvelles GuardDuty fonctionnalités dans votre AWS environnement.
- Le `dataSources` schéma de la API demande ou de la réponse est le même dans chaque Région AWS endroit où GuardDuty cela est disponible. Cependant, il se peut que toutes les fonctionnalités ne soient pas disponibles dans chaque région. Par conséquent, les noms des fonctionnalités disponibles peuvent varier en fonction de la région.

Comprendre le fonctionnement de l'activation des fonctionnalités

Ils GuardDuty APIs continueront à renvoyer un `dataSources` objet le cas échéant, et ils renverront également un `features` objet contenant les mêmes informations dans un format différent.

GuardDuty les fonctionnalités lancées avant mars 2023 seront disponibles via `dataSources` object et `features` object. GuardDuty les fonctionnalités lancées depuis mars 2023 ne seront disponibles que via l'`features`objet. Vous ne pouvez pas créer ou mettre à jour un détecteur, ni décrire votre AWS Organizations utilisation à la fois `dataSources` et de la notation d'`features`objets dans la même API demande. Pour activer les types de GuardDuty protection, vous devez migrer vos sources de données existantes vers l'`features`objet en utilisant celles APIs qui incluent désormais également l'`features`objet.

> **Note**
>
> GuardDuty n'ajoutera pas de nouvelle source de données après cette modification.

GuardDuty a déconseillé l'utilisation de sources de données. Cependant, il prend toujours en charge les GuardDuty sources de données de base. Les GuardDuty meilleures pratiques recommandent d'utiliser l'activation des fonctionnalités pour tous les types de protection déjà activés pour votre compte. Les meilleures pratiques exigent également l'activation des fonctionnalités lorsque vous activez un nouveau type de protection pour votre compte.

Intégration des modifications d'activation des fonctionnalités

- Si vous gérez des GuardDuty configurations par le biais de APIsSDKs, ou d'un AWS CloudFormation modèle, et que vous souhaitez activer de nouvelles GuardDuty fonctionnalités potentielles, vous devrez modifier votre code et votre modèle, respectivement. Pour plus d'informations, consultez la mise à jour APIs dans le Amazon GuardDuty API Reference.
- Pour les GuardDuty fonctionnalités configurées avant cette mise à niveau, vous pouvez continuer à utiliser le AWS CloudFormation modèle APIsSDKs, ou. Toutefois, nous vous recommandons de passer à l'utilisation de l'objet `feature`.

  Toutes les sources de données ont un objet de fonctionnalité équivalent. Pour de plus amples informations, veuillez consulter Mappage de `dataSources` aux `features`.
- Actuellement, `additionalConfiguration` dans l'objet `features` n'est disponible que pour certains types de protection.
  - Pour de tels types de protection, si votre fonctionnalité `AdditionalConfiguration` `status` est définie sur `ENABLED` mais que la configuration de votre fonctionnalité n'`status`est pas définie sur`ENABLED`, GuardDuty aucune action n'est entreprise dans ce cas.
  - Ceci a APIs une incidence sur les éléments suivants :

- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration

Mappage de **`dataSources`** aux **`features`**

Le tableau suivant montre le mappage des types de protection, `dataSources` et `features`.

GuardDuty type de protection	Nom de la source de données *	Nom de la fonctionnalité
Journaux de flux VPC	`flowLogs` (lecture seule ; modification impossible)	`FLOW_LOGS` (lecture seule ; modification impossible)
Journaux de requêtes du résolveur DNS Route53	`dnsLogs` (lecture seule ; modification impossible)	`DNS_LOGS` (lecture seule ; modification impossible)
CloudTrail événements	`cloudTrail` (lecture seule ; modification impossible)	`CLOUD_TRAIL` (lecture seule ; modification impossible)
S3	`s3Logs`	`S3_DATA_EVENTS`
EKSSurveillance du journal d'audit	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Protection contre les logiciels malveillants pour EC2	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
RDSÉvénements de connexion	GuardDuty fournit uniquement un support d'activation des fonctionnalités pour ces types de protection.	`RDS_LOGIN_EVENTS`

GuardDuty type de protection	Nom de la source de données *	Nom de la fonctionnalité
EKSSurveillance du temps d'exécution		`EKS_RUNTIME_MONITORING`
Surveillance du temps d'exécution		`RUNTIME_MONITORING`

GuardDuty agent de sécurité pour les EKS clusters Amazon		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty agent de sécurité pour les clusters Amazon ECS -Fargate		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`

GuardDuty type de protection	Nom de la source de données *	Nom de la fonctionnalité
GuardDuty agent de sécurité pour les EC2 instances Amazon		`RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT`
Protection Lambda		`LAMBDA_NETWORK_LOGS`

* GetUsageStatistics utilise ses propres noms de `dataSource`. Pour plus d'informations, consultez Estimation des GuardDuty coûts ou GetUsageStatistics.

GuardDuty Protection S3

S3 Protection aide Amazon à GuardDuty surveiller les événements liés aux AWS CloudTrail données pour Amazon Simple Storage Service (Amazon S3), notamment les opérations API au niveau des objets, afin d'identifier les risques de sécurité potentiels pour les données contenues dans vos compartiments Amazon S3.

GuardDuty surveille à la fois les événements de AWS CloudTrail gestion et les événements relatifs aux données AWS CloudTrail S3 afin d'identifier les menaces potentielles pesant sur vos ressources Amazon S3. Les deux sources de données surveillent différents types d'activité. Les exemples d'événements de CloudTrail gestion pour S3 incluent les opérations qui répertorient ou configurent des compartiments Amazon S3, telles que `ListBucketsDeleteBuckets`, et`PutBucketReplication`. Les exemples d'événements de CloudTrail données pour S3 incluent les API opérations au niveau des objets, telles que`GetObject`, `ListObjectsDeleteObject`, et. `PutObject`

Lorsque vous activez Amazon GuardDuty pour un Compte AWS, GuardDuty commence à surveiller les événements CloudTrail de gestion. Il n'est pas nécessaire d'activer ou de configurer explicitement la connexion aux événements de données S3 AWS CloudTrail pour utiliser S3 Protection. Vous pouvez activer la fonctionnalité S3 Protection (qui surveille les événements CloudTrail liés aux données pour S3) pour n'importe quel compte, partout Région AWS où cette fonctionnalité est disponible sur Amazon GuardDuty, à tout moment. Une Compte AWS version déjà activée GuardDuty peut activer S3 Protection pour la première fois grâce à une période d'essai gratuite de 30 jours. Pour ceux Compte AWS qui l' GuardDuty activent pour la première fois, S3 Protection est déjà activé et inclus dans cet essai gratuit de 30 jours. Pour de plus amples informations, veuillez consulter Estimation des GuardDuty coûts.

Nous vous recommandons d'activer S3 Protection dans GuardDuty. Si cette fonctionnalité n'est pas activée, GuardDuty vous ne serez pas en mesure de surveiller entièrement vos compartiments Amazon S3 ou de détecter un accès suspect aux données stockées dans vos compartiments S3.

Comment GuardDuty utilise les événements de données S3

Lorsque vous activez les événements de données S3 (protection S3), vous GuardDuty commencez à analyser les événements de données S3 provenant de tous vos compartiments S3 et à les surveiller pour détecter toute activité malveillante ou suspecte. Pour de plus amples informations, veuillez consulter AWS CloudTrail événements de données pour S3.

Lorsqu'un utilisateur non authentifié accède à un objet S3, cela signifie que celui-ci est accessible au public. Par conséquent, GuardDuty ne traite pas de telles demandes. GuardDuty traite les demandes adressées aux objets S3 en utilisant des informations d'identification valides IAM (AWS Identity and Access Management) ou AWS STS (AWS Security Token Service).

> **Remarque**
>
> Après avoir activé S3 Protection, Amazon GuardDuty surveille les événements liés aux données provenant des compartiments Amazon S3 situés dans la même région que celle où vous l'avez activée GuardDuty.

Lorsqu'une menace potentielle est GuardDuty détectée sur la base de la surveillance des événements liés aux données S3, elle génère une constatation de sécurité. Pour plus d'informations sur les types de résultats GuardDuty pouvant être générés pour les compartiments Amazon S3, consultezGuardDuty Types de recherche S3.

Si vous désactivez S3 Protection, GuardDuty arrête la surveillance des événements de données S3 concernant les données stockées dans vos compartiments S3.

Fonctionnalité dans la protection S3

AWS CloudTrail événements de données pour S3

Les événements de données, également appelés opérations de plan de données, fournissent des informations sur les opérations de ressource exécutées sur ou dans une ressource. Ils s'agit souvent d'activités dont le volume est élevé.

Voici des exemples d'événements de CloudTrail données GuardDuty pouvant être surveillés pour S3 :

- `GetObject`APIopérations
- `PutObject`APIopérations
- `ListObjects`APIopérations
- `DeleteObject`APIopérations

Lorsque vous l'activez GuardDuty pour la première fois, S3 Protection est activé par défaut et est également inclus dans la période d'essai gratuite de 30 jours. Toutefois, cette fonctionnalité

est facultative et vous pouvez choisir de l'activer ou de la désactiver pour n'importe quel compte ou n'importe quelle région à tout moment. Pour de plus amples informations sur la configuration d'Amazon S3 en tant que fonctionnalité, veuillez consulter Protection S3.

Configuration de la protection S3 pour un compte autonome

Pour les comptes associés par AWS Organizations, ce processus peut être automatisé via les paramètres de la console. Pour de plus amples informations, veuillez consulter Configuration de la protection S3 dans des environnements à comptes multiples.

Pour activer ou désactiver la protection S3

Choisissez votre méthode d'accès préférée pour configurer la protection S3 pour un compte autonome.

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Protection S3.
3. La page Protection S3 fournit l'état actuel de la protection S3 pour votre compte. Choisissez Activer ou Désactiver pour activer ou désactiver la protection S3 à tout moment.
4. Choisissez Confirmer pour confirmer votre sélection.

API/CLI

1. Exécutez updateDetector à l'aide de votre ID de détecteur valide pour la région actuelle et en transmettant l'objet `features name` en tant que `S3_DATA_EVENTS` défini sur `ENABLED` ou `DISABLED` pour activer ou désactiver la protection S3, respectivement.

   > **Note**
   >
   > Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

2. Vous pouvez également utiliser AWS Command Line Interface. Pour activer la protection S3, exécutez la commande suivante et assurez-vous d'utiliser votre propre ID de détecteur valide.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

Pour désactiver la protection S3, remplacez `ENABLED` par `DISABLED` dans l'exemple.

Configuration de la protection S3 dans des environnements à comptes multiples

Dans un environnement multi-comptes, seul le compte d' GuardDuty administrateur délégué a la possibilité de configurer (activer ou désactiver) S3 Protection pour les comptes des membres de son AWS organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration depuis leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Le compte d' GuardDuty administrateur délégué peut choisir d'activer automatiquement S3 Protection sur tous les comptes, uniquement sur les nouveaux comptes ou sur aucun compte de l'organisation. Pour de plus amples informations, veuillez consulter Gestion de comptes avec AWS Organizations.

Configuration de S3 Protection pour un compte GuardDuty d'administrateur délégué

Choisissez votre méthode d'accès préférée pour configurer S3 Protection pour le compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte de gestion.
2. Dans le panneau de navigation, choisissez Protection S3.
3. Sur la page Protection S3, choisissez Modifier.
4. Effectuez l’une des actions suivantes :

   Utilisation d'Activer pour tous les comptes

   - Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.

- Choisissez Save (Enregistrer).

Utilisation de Configurer les comptes manuellement

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Choisissez Save (Enregistrer).

API/CLI

updateDetectorExécuté en utilisant l'ID du détecteur du compte GuardDuty administrateur délégué pour la région en cours et en transmettant l'`features`objet `name` sous `S3_DATA_EVENTS` et en `status` tant que`ENABLED`.

Vous pouvez également configurer S3 Protection en utilisant AWS Command Line Interface. Exécutez la commande suivante et assurez-vous de remplacer *`12abc34d567e8fa901bc2d34e56789f0`* avec l'identifiant du détecteur du compte GuardDuty administrateur délégué pour la région actuelle.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

Activer automatiquement la protection S3 pour tous les comptes membres de l'organisation

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide de votre compte administrateur.

2. Effectuez l’une des actions suivantes :

Utilisation de la page Protection S3

1. Dans le panneau de navigation, choisissez Protection S3.
2. Choisissez Activer pour tous les comptes. Cette action active automatiquement la protection S3 pour les comptes existants et nouveaux de l'organisation.
3. Choisissez Save (Enregistrer).

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de la page Comptes

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez les préférences d'activation automatique avant Ajouter des comptes par invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes sous Protection S3.
4. Choisissez Save (Enregistrer).

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes, veuillez consulter Activer ou désactiver la protection S3 de manière sélective dans les comptes membres.

API/CLI

- Pour activer ou désactiver la protection S3 de manière sélective pour vos comptes membres, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Assurez-vous de remplacer *`12abc34d567e8fa901bc2d34e56789f0`* avec le compte `detector-id` de l' GuardDuty administrateur délégué, et *`111122223333`*. Pour désactiver S3 Protection, remplacez `ENABLED` par`DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer la protection S3 pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la protection S3 pour tous les comptes membres actifs existants de votre organisation.

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le panneau de navigation, choisissez Protection S3.
3. Sur la page Protection S3, vous pouvez afficher l'état actuel de la configuration. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Choisissez Confirmer.

API/CLI

- Pour activer ou désactiver la protection S3 de manière sélective pour vos comptes membres, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Assurez-vous de remplacer *`12abc34d567e8fa901bc2d34e56789f0`* avec le compte `detector-id` de l' GuardDuty administrateur délégué, et *`111122223333`*. Pour désactiver S3 Protection, remplacez `ENABLED` par`DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer automatiquement la protection S3 pour les nouveaux comptes membres

Choisissez votre méthode d'accès préférée pour activer la protection S3 pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte d' GuardDuty administrateur délégué peut activer de nouveaux comptes membres dans une organisation via la console, en utilisant la page S3 Protection ou Comptes.

Pour activer automatiquement la protection S3 pour les nouveaux comptes membres

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l’une des actions suivantes :

   - Utilisation de la page Protection S3 :

     1. Dans le panneau de navigation, choisissez Protection S3.
     2. Sur la page Protection S3, choisissez Modifier.
     3. Choisissez Configurer les comptes manuellement.
     4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la protection S3 sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
     5. Choisissez Save (Enregistrer).

   - Utilisation de la page Comptes :

     1. Dans le panneau de navigation, choisissez Accounts (Comptes).
     2. Sur la page Comptes, choisissez les préférences d'activation automatique.
     3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous Protection S3.
     4. Choisissez Save (Enregistrer).

API/CLI

- Pour activer ou désactiver la protection S3 de manière sélective pour vos comptes membres, lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Pour la désactiver, veuillez consulter Activer ou désactiver la protection S3 de manière sélective dans les comptes membres. Définissez les préférences pour activer ou désactiver automatiquement le plan de protection dans cette région pour les nouveaux comptes (`NEW`) qui rejoignent l'organisation, pour tous les comptes (`ALL`) ou pour aucun des comptes (`NONE`) de l'organisation. Pour plus d'informations, consultez la section autoEnableOrganizationMembres. Selon vos préférences, vous devrez peut-être remplacer `NEW` par `ALL` ou `NONE`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer ou désactiver la protection S3 de manière sélective dans les comptes membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver de manière sélective la protection S3 pour les comptes membres.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

   Sur la page Comptes, veuillez consulter la colonne Protection S3 pour connaître l'état de votre compte membre.

3. Pour activer ou désactiver de manière sélective la protection S3

   Sélectionnez le compte pour lequel vous souhaitez configurer la protection S3. Vous pouvez sélectionner plusieurs comptes à la fois. Dans le menu déroulant Modifier les plans de protection, choisissez S3Pro, puis choisissez l'option appropriée.

API/CLI

Pour activer ou désactiver la protection S3 de manière sélective pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération à l'aide de votre propre identifiant de détecteur.

L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. Pour la désactiver, remplacez `true` par `false`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

> **Note**
>
> Si vous utilisez des scripts pour intégrer de nouveaux comptes et que vous souhaitez désactiver S3 Protection dans vos nouveaux comptes, vous pouvez modifier l'createDetectorAPIopération avec l'`dataSources`objet facultatif comme décrit dans cette rubrique.

Désactivation automatique de S3 Protection pour les nouveaux comptes GuardDuty

> **Important**
>
> Par défaut, S3 Protection est automatiquement activé pour Comptes AWS cette jointure GuardDuty pour la première fois.

Si vous êtes un compte GuardDuty administrateur activé GuardDuty pour la première fois sur un nouveau compte et que vous ne souhaitez pas que S3 Protection soit activé par défaut, vous pouvez

le désactiver en modifiant l'createDetectorAPIopération avec l'`features`objet optionnel. L'exemple suivant utilise le AWS CLI pour activer un nouveau GuardDuty détecteur avec la protection S3 désactivée.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

GuardDuty EKSProtection

EKSLa surveillance des journaux d'audit vous aide à détecter les activités potentiellement suspectes dans les EKS clusters d'Amazon Elastic Kubernetes Service (Amazon). EKS EKSLa surveillance des journaux EKS d'audit utilise les journaux d'audit pour capturer les activités chronologiques des utilisateurs, des applications utilisant Kubernetes API et du plan de contrôle. Pour de plus amples informations, veuillez consulter EKSsurveillance du journal d'audit.

> **Note**
>
> EKSLa surveillance du temps d'exécution est gérée dans le cadre de la surveillance du temps d'exécution. Pour de plus amples informations, veuillez consulter GuardDuty Surveillance du temps d'exécution.

Fonctionnalités de EKS la protection

EKSsurveillance du journal d'audit

EKSles journaux d'audit capturent les actions séquentielles au sein de votre EKS cluster Amazon, notamment les activités des utilisateurs, des applications utilisant Kubernetes API et du plan de contrôle. La journalisation d'audit est un composant de tous les clusters Kubernetes.

Pour plus d'informations, consultez la section Audit dans la documentation Kubernetes.

Amazon EKS autorise l'ingestion des journaux d'EKSaudit en tant qu'Amazon CloudWatch Logs via la fonction de journalisation du plan de EKS contrôle. GuardDuty ne gère pas la journalisation de votre plan de EKS contrôle Amazon et ne rend pas les journaux EKS d'audit accessibles sur votre compte si vous ne les avez pas activés pour AmazonEKS. Pour gérer l'accès à vos journaux d'EKSaudit et leur conservation, vous devez configurer la fonctionnalité de journalisation du plan de EKS contrôle Amazon. Pour plus d'informations, consultez la section Activation et désactivation des journaux du plan de contrôle dans le guide de EKS l'utilisateur Amazon.

Pour plus d'informations sur la configuration de la surveillance des journaux d'EKSaudit, consultezEKSSurveillance du journal d'audit.

EKSSurveillance du journal d'audit

EKSLa surveillance des journaux d'audit vous aide à détecter les activités potentiellement suspectes dans vos EKS clusters au sein d'Amazon Elastic Kubernetes Service. Lorsque vous activez la surveillance des journaux EKS d'audit, vous GuardDuty commencez immédiatement à effectuer une surveillance à EKSsurveillance du journal d'audit partir de vos EKS clusters Amazon et à les analyser pour détecter toute activité potentiellement malveillante et suspecte. Il utilise les événements du journal d'audit Kubernetes directement depuis la fonction de journalisation du plan EKS de contrôle Amazon via un flux indépendant et duplicatif de journaux d'audit. Ce processus ne nécessite aucune configuration supplémentaire et n'affecte aucune des configurations de journalisation existantes du plan de EKS contrôle Amazon que vous pourriez avoir.

Lorsque vous désactivez la surveillance des journaux EKS d'audit, la surveillance et l'analyse des journaux EKS d'audit de vos EKS ressources Amazon sont GuardDuty immédiatement arrêtées.

EKSLa surveillance du journal d'audit n'est peut-être pas disponible partout Régions AWS où GuardDuty elle est disponible. Pour de plus amples informations, veuillez consulter Disponibilité des fonctionnalités propres à la région.

Comment la période d'essai gratuite de 30 jours affecte les comptes GuardDuty

- Lorsque vous l'activez GuardDuty pour la première fois, la surveillance des journaux EKS d'audit est déjà incluse dans la période d'essai gratuite de 30 jours.
- Les GuardDuty comptes existants, pour lesquels l'essai gratuit de 30 jours est déjà terminé, peuvent activer la surveillance du journal EKS d'audit pour la première fois avec une période d'essai gratuite de 30 jours.

Configuration de la surveillance du journal d'EKSaudit pour un compte autonome

Choisissez votre méthode d'accès préférée pour activer ou désactiver la surveillance du journal d'EKSaudit pour un compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez EKS Protection.

3. Dans l'onglet Configuration, vous pouvez consulter l'état de configuration actuel de EKS Audit Log Monitoring. Dans la section Surveillance du journal EKS d'audit, choisissez Activer pour activer ou Désactiver pour désactiver la fonctionnalité de surveillance du journal EKS d'audit.
4. Choisissez Save (Enregistrer).

API/CLI

- Exécutez l'updateDetectorAPIopération en utilisant l'ID de détecteur régional du compte GuardDuty administrateur délégué et en transmettant le nom `EKS_AUDIT_LOGS` et le statut de l'`features`objet sous la forme `ENABLED` ou`DISABLED`.

  Vous pouvez également activer ou désactiver la surveillance du journal EKS d'audit en exécutant la AWS CLI commande a. L'exemple de code suivant active la surveillance du journal GuardDuty EKS d'audit. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

Configuration de la surveillance EKS des journaux d'audit dans les environnements à comptes multiples

Dans un environnement à comptes multiples, seul le compte GuardDuty administrateur délégué a la possibilité d'activer ou de désactiver la fonctionnalité de surveillance du journal EKS d'audit pour les comptes des membres de son organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Ce compte d' GuardDuty administrateur délégué peut choisir d'activer automatiquement la surveillance du journal EKS d'audit pour tous les nouveaux comptes lorsqu'ils rejoignent l'organisation. Pour plus d'informations sur les environnements à comptes multiples, consultez Gérer plusieurs comptes sur Amazon. GuardDuty

Configuration de la surveillance du journal d'EKSaudit pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour configurer la surveillance du journal EKS d'audit pour le compte GuardDuty d'administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte de gestion.
2. Dans le volet de navigation, choisissez EKS Protection.
3. Dans l'onglet Configuration, vous pouvez consulter l'état de configuration actuel de EKS Audit Log Monitoring dans la section correspondante. Pour mettre à jour la configuration du compte GuardDuty administrateur délégué, choisissez Modifier dans le volet de surveillance du journal EKS d'audit.
4. Effectuez l’une des actions suivantes :

   Utilisation d'Activer pour tous les comptes

   - Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
   - Choisissez Save (Enregistrer).

   Utilisation de Configurer les comptes manuellement

   - Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
   - Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
   - Choisissez Save (Enregistrer).

API/CLI

Exécutez l'updateDetectorAPIopération en utilisant votre propre identifiant de détecteur régional et en passant l'`features`objet au `name` `status` fur `EKS_AUDIT_LOGS` `ENABLED` et à mesure`DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

Vous pouvez activer ou désactiver la surveillance du journal EKS d'audit en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser un compte GuardDuty d'administrateur délégué valide *`detector ID`*.

> **Note**
>
> L'exemple de code suivant active la surveillance du journal EKS d'audit. Assurez-vous de remplacer *`12abc34d567e8fa901bc2d34e56789f0`* avec le compte `detector-id` de l' GuardDuty administrateur délégué et *`555555555555`* avec le compte Compte AWS de l' GuardDuty administrateur délégué.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Pour désactiver la surveillance du journal EKS d'audit, remplacez `ENABLED` par`DISABLED`.

Activer automatiquement la surveillance du journal EKS d'audit pour tous les comptes des membres

Choisissez votre méthode d'accès préférée pour activer le suivi du journal EKS d'audit pour les comptes membres existants de votre organisation.

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.
2. Effectuez l’une des actions suivantes :

Utilisation de la page EKSProtection

1. Dans le volet de navigation, choisissez EKSProtection.
2. Dans l'onglet Configuration, vous pouvez consulter l'état actuel de la surveillance des journaux EKS d'audit pour les comptes membres actifs de votre organisation.

   Pour mettre à jour la configuration de surveillance du journal d'EKSaudit, choisissez Modifier.
3. Choisissez Activer pour tous les comptes. Cette action active automatiquement la surveillance du journal EKS d'audit pour les comptes existants et nouveaux de l'organisation.
4. Choisissez Save (Enregistrer).

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de la page Comptes

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez les préférences d'activation automatique avant Ajouter des comptes par invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes sous EKSAudit Log Monitoring.
4. Choisissez Save (Enregistrer).

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes et que vous souhaitez personnaliser la configuration de surveillance des journaux EKS d'audit pour des comptes spécifiques de votre organisation, consultezActiver ou désactiver de manière sélective la surveillance du journal EKS d'audit pour les comptes des membres.

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance des journaux EKS d'audit pour vos comptes de membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer la surveillance du journal EKS d'audit pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer la surveillance du journal EKS d'audit pour tous les comptes de membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la surveillance du journal EKS d'audit pour tous les comptes de membres actifs existants de l'organisation.

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le volet de navigation, choisissez EKSProtection.

3. Sur la page EKSProtection, vous pouvez consulter l'état actuel de la configuration de l'analyse des programmes malveillants GuardDuty initiée. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Choisissez Save (Enregistrer).

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance des journaux EKS d'audit pour vos comptes de membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer la surveillance du journal EKS d'audit pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer automatiquement la surveillance du journal EKS d'audit pour les nouveaux comptes de membres

Les comptes de membres nouvellement ajoutés doivent être activés GuardDuty avant de sélectionner la configuration de l'analyse des programmes malveillants GuardDuty initiée par le client. Les comptes des membres gérés par invitation peuvent configurer manuellement une analyse des

logiciels malveillants GuardDuty initiée pour leurs comptes. Pour de plus amples informations, veuillez consulter Step 3 - Accept an invitation.

Choisissez votre méthode d'accès préférée pour activer la surveillance des journaux EKS d'audit pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte GuardDuty administrateur délégué peut activer la surveillance du journal EKS d'audit pour les nouveaux comptes membres d'une organisation, à l'aide de la page Surveillance du journal EKS d'audit ou des comptes.

Pour activer automatiquement la surveillance du journal EKS d'audit pour les nouveaux comptes de membres

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.
2. Effectuez l'une des actions suivantes :
   - À l'aide de EKSla page Protection :

     1. Dans le volet de navigation, choisissez EKSProtection.
     2. Sur la page EKSProtection, choisissez Modifier dans le journal EKS d'audit de surveillance.
     3. Choisissez Configurer les comptes manuellement.
     4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la surveillance du journal EKS d'audit sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
     5. Choisissez Save (Enregistrer).
   - Utilisation de la page Comptes :

     1. Dans le panneau de navigation, choisissez Accounts (Comptes).
     2. Sur la page Comptes, choisissez les préférences d'activation automatique.
     3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous EKSAudit Log Monitoring.

4. Choisissez Save (Enregistrer).

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance des journaux EKS d'audit pour vos nouveaux comptes, exécutez l'UpdateOrganizationConfigurationAPIopération en utilisant le vôtre *detector ID*.
- L'exemple suivant montre comment activer la surveillance du journal EKS d'audit pour les nouveaux membres qui rejoignent votre organisation. Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Activer ou désactiver de manière sélective la surveillance du journal EKS d'audit pour les comptes des membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver la surveillance des journaux EKS d'audit pour certains comptes membres de votre organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).

   Sur la page Comptes, consultez la colonne Surveillance du journal EKS d'audit pour connaître l'état de votre compte de membre.

3. Pour activer ou désactiver la surveillance EKS du journal d'audit

   Sélectionnez le compte que vous souhaitez configurer pour la surveillance du journal EKS d'audit. Vous pouvez sélectionner plusieurs comptes à la fois. Dans le menu déroulant Modifier les plans de protection, choisissez EKSAudit Log Monitoring, puis choisissez l'option appropriée.

API/CLI

Pour activer ou désactiver de manière sélective la surveillance des journaux EKS d'audit pour vos comptes membres, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.

L'exemple suivant montre comment activer la surveillance du journal EKS d'audit pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`. Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

GuardDuty Surveillance du temps d'exécution

Runtime Monitoring observe et analyse les événements au niveau du système d'exploitation, du réseau et des fichiers pour vous aider à détecter les menaces potentielles dans des AWS charges de travail spécifiques de votre environnement.

AWS Ressources prises en charge dans Runtime Monitoring : GuardDuty avait initialement publié Runtime Monitoring pour prendre en charge uniquement les ressources Amazon Elastic Kubernetes Service (Amazon). EKS Désormais, vous pouvez également utiliser la fonctionnalité de surveillance du temps d'exécution pour détecter les menaces pour vos ressources AWS Fargate Amazon Elastic Container Service (AmazonECS) et Amazon Elastic Compute Cloud (AmazonEC2).

GuardDuty ne prend pas en charge les EKS clusters Amazon exécutés sur AWS Fargate.

Dans ce document et dans d'autres sections relatives à la surveillance du temps d'exécution, GuardDuty utilise la terminologie du type de ressource pour faire référence aux ressources AmazonEKS, Fargate ECS Amazon et EC2 Amazon.

La surveillance du temps d'exécution utilise un agent de GuardDuty sécurité qui ajoute de la visibilité sur le comportement d'exécution, comme l'accès aux fichiers, l'exécution des processus, les arguments de ligne de commande et les connexions réseau. Pour chaque type de ressource que vous souhaitez surveiller pour détecter les menaces potentielles, vous pouvez gérer l'agent de sécurité pour ce type de ressource spécifique automatiquement ou manuellement (à l'exception de Fargate (ECSAmazon uniquement)). La gestion automatique de l'agent de sécurité signifie que vous autorisez GuardDuty l'installation et la mise à jour de l'agent de sécurité en votre nom. D'autre part, lorsque vous gérez manuellement l'agent de sécurité pour vos ressources, vous êtes responsable de l'installer et de le mettre à jour, selon les besoins.

Cette fonctionnalité étendue GuardDuty peut vous aider à identifier et à répondre aux menaces potentielles susceptibles de cibler les applications et les données exécutées dans vos charges de travail et instances individuelles. Par exemple, une menace peut potentiellement commencer par compromettre un conteneur unique qui exécute une application Web vulnérable. Cette application Web peut disposer d'autorisations d'accès aux conteneurs et aux charges de travail sous-jacents. Dans ce scénario, des informations d'identification mal configurées peuvent potentiellement élargir l'accès au compte et aux données qui y sont stockées.

En analysant les événements d'exécution des conteneurs et des charges de travail individuels, GuardDuty vous pouvez identifier la compromission d'un conteneur et des AWS informations

d'identification associées dans une phase initiale, et détecter les tentatives d'augmentation des privilèges, les API demandes suspectes et les accès malveillants aux données de votre environnement.

Table des matières

Comment ça marche

Pour utiliser le Runtime Monitoring, vous devez activer le Runtime Monitoring, puis gérer l'agent GuardDuty de sécurité. La liste suivante explique ce processus en deux étapes :

1. Activez la surveillance du temps d'exécution pour votre compte afin qu'il GuardDuty puisse accepter les événements d'exécution qu'il reçoit de vos EC2 instances Amazon, de vos ECS clusters Amazon et de vos EKS charges de travail Amazon.
2. Gérez l' GuardDuty agent pour les ressources individuelles dont vous souhaitez surveiller le comportement d'exécution. Selon le type de ressource, vous pouvez choisir de déployer l'agent de GuardDuty sécurité manuellement ou en autorisant GuardDuty sa gestion en votre nom, ce que l'on appelle la configuration automatique de l'agent.

   GuardDuty utilise des rôles d'identité d'instance qui authentifient l'agent de sécurité pour chaque type de ressource afin d'envoyer les événements d'exécution associés au point de VPC terminaison.

> **Note**
>
> GuardDuty ne vous permet pas d'accéder aux événements d'exécution.

Lorsque vous gérez l'agent de sécurité (manuellement ou via GuardDuty) dans EKS Runtime Monitoring ou Runtime Monitoring pour les EC2 instances, et qu'GuardDuty il est actuellement déployé sur une EC2 instance Amazon et que vous le recevez Types d'événement d'exécution collectés de cette instance, l'analyse Compte AWS des journaux de VPC flux provenant de cette EC2 instance Amazon ne vous GuardDuty sera pas facturée. Cela permet GuardDuty d'éviter le double coût d'utilisation sur le compte.

Les rubriques suivantes expliquent comment l'activation de la surveillance du temps d'exécution et la gestion GuardDuty de l'agent de sécurité fonctionnent différemment pour chaque type de ressource.

Table des matières

Comment fonctionne Runtime Monitoring avec les EC2 instances Amazon

Vos EC2 instances Amazon peuvent exécuter plusieurs types d'applications et de charges de travail dans votre AWS environnement. Lorsque vous activez la surveillance du temps d'exécution et que vous gérez l'agent de GuardDuty sécurité, GuardDuty cela vous aide à détecter les menaces dans vos EC2 instances Amazon existantes et dans les nouvelles instances potentielles. Cette fonctionnalité prend également en charge les EC2 instances Amazon ECS gérées par Amazon.

L'activation de la surveillance du temps d'exécution permet de GuardDuty préparer les événements d'exécution provenant des processus en cours d'exécution et des nouveaux processus au sein EC2 des instances Amazon. GuardDuty nécessite qu'un agent de sécurité envoie les événements d'exécution de votre EC2 instance à GuardDuty.

Pour les EC2 instances Amazon, l'agent GuardDuty de sécurité fonctionne au niveau de l'instance. Vous pouvez décider si vous souhaitez surveiller toutes les EC2 instances Amazon de votre compte

ou certaines d'entre elles. Si vous souhaitez gérer des instances sélectives, l'agent de sécurité n'est requis que pour ces instances.

GuardDuty peut également consommer des événements d'exécution provenant de nouvelles tâches et de tâches existantes exécutées dans des EC2 instances Amazon au sein de ECS clusters Amazon.

Pour installer l'agent GuardDuty de sécurité, Runtime Monitoring propose les deux options suivantes :

- Utiliser la configuration automatique des agents (recommandé), ou
- Gestion manuelle de l'agent de sécurité

Utiliser la configuration automatique des agents via GuardDuty (recommandé)

Utilisez la configuration automatique de l'agent qui GuardDuty permet d'installer l'agent de sécurité sur vos EC2 instances Amazon en votre nom. GuardDuty gère également les mises à jour de l'agent de sécurité.

Par défaut, GuardDuty installe l'agent de sécurité sur toutes les instances de votre compte. Si vous souhaitez GuardDuty installer et gérer l'agent de sécurité pour certaines EC2 instances uniquement, ajoutez des balises d'inclusion ou d'exclusion à vos EC2 instances, selon vos besoins.

Parfois, il se peut que vous ne souhaitiez pas surveiller les événements d'exécution pour toutes les EC2 instances Amazon associées à votre compte. Dans les cas où vous souhaitez surveiller les événements d'exécution pour un nombre limité d'instances, ajoutez une balise d'inclusion sous la forme `GuardDutyManaged` : `true` à ces instances sélectionnées. À compter de la disponibilité de la configuration automatique des agents pour AmazonEC2, si votre EC2 instance possède une balise d'inclusion (`GuardDutyManaged:true`), cette balise GuardDuty sera honorée et l'agent de sécurité sera géré pour les instances sélectionnées, même si vous n'activez pas explicitement la configuration automatique des agents.

En revanche, s'il existe un nombre limité d'EC2instances pour lesquelles vous ne souhaitez pas surveiller les événements d'exécution, ajoutez une balise d'exclusion (`GuardDutyManaged:false`) à ces instances sélectionnées. GuardDuty respectera la balise d'exclusion en n'installant ni en ne gérant l'agent de sécurité pour ces EC2 ressources.

Impact

Lorsque vous utilisez la configuration automatique des agents dans une organisation Compte AWS ou une organisation, vous autorisez GuardDuty à effectuer les étapes suivantes en votre nom :

- GuardDuty crée une SSM association pour toutes vos EC2 instances Amazon qui sont SSM gérées et apparaissent sous Fleet Manager dans la https://console.aws.amazon.com/systems-manager/console.
- Utilisation de balises d'inclusion avec désactivation de la configuration automatique des agents : après avoir activé la surveillance du temps d'exécution, lorsque vous n'activez pas la configuration automatique des agents mais que vous ajoutez une balise d'inclusion à votre EC2 instance Amazon, cela signifie que vous êtes autorisé GuardDuty à gérer l'agent de sécurité en votre nom. SSMl'association installera ensuite l'agent de sécurité dans chaque instance dotée de la balise d'inclusion (`GuardDutyManaged:true`).
- Si vous activez la configuration automatique de l'agent, SSM l'association installera ensuite l'agent de sécurité dans toutes les EC2 instances appartenant à votre compte.
- Utilisation de balises d'exclusion avec configuration automatique des agents : avant d'activer la configuration automatique des agents, lorsque vous ajoutez des balises d'exclusion à votre EC2 instance Amazon, cela signifie que vous autorisez GuardDuty à empêcher l'installation et la gestion de l'agent de sécurité pour cette instance sélectionnée.

  Désormais, lorsque vous activez la configuration automatique de l'agent, l'SSMassociation installe et gère l'agent de sécurité dans toutes les EC2 instances, à l'exception de celles qui sont étiquetées avec la balise d'exclusion.
- GuardDuty crée des VPC points de terminaison dans tous les environnements VPCsVPCs, y compris partagés, à condition qu'au moins une EC2 instance Linux ne soit VPC pas dans l'état d'instance terminée ou en état d'arrêt. Cela inclut les systèmes centralisés VPC et parlésVPCs. GuardDuty ne prend pas en charge la création d'un VPC point de terminaison uniquement pour le système centraliséVPC. Pour plus d'informations sur le VPC fonctionnement de la centralisation, consultez la section VPCPoints de terminaison de l'interface dans le AWS livre blanc intitulé « Création d'une infrastructure multiréseau évolutive et sécurisée ». VPC AWS

  Pour plus d'informations sur les différents états des instances, consultez la section Cycle de vie des instances dans le guide de EC2 l'utilisateur Amazon.

  GuardDuty prend également en chargeUtilisation partagée VPC avec des agents de sécurité automatisés. Lorsque tous les prérequis sont pris en compte pour votre organisation et Compte AWS que GuardDuty vous utiliserez le partage VPC pour recevoir les événements d'exécution.

> **Note**
>
> Il n'y a aucun coût supplémentaire pour l'utilisation du VPC terminal.

Gestion manuelle de l'agent de sécurité

Il existe deux méthodes pour gérer EC2 manuellement l'agent de sécurité pour Amazon :

- Utilisez des documents GuardDuty gérés AWS Systems Manager pour installer l'agent de sécurité sur vos EC2 instances Amazon déjà SSM gérées.

  Chaque fois que vous lancez une nouvelle EC2 instance Amazon, assurez-vous qu'elle est SSM activée.
- Utilisez des scripts RPM package manager (RPM) pour installer l'agent de sécurité sur vos EC2 instances Amazon, qu'elles soient SSM gérées ou non.

Étape suivante

Pour démarrer avec la configuration de Runtime Monitoring afin de surveiller vos EC2 instances Amazon, consultezConditions requises pour le support des EC2 instances Amazon.

Comment fonctionne la surveillance du temps d'exécution avec Fargate (Amazon uniquement) ECS

Lorsque vous activez la surveillance du temps d' GuardDuty exécution, il est prêt à consommer les événements d'exécution d'une tâche. Ces tâches s'exécutent au sein des ECS clusters Amazon, qui à leur tour s'exécutent sur les AWS Fargate (Fargate) instances. GuardDuty Pour recevoir ces événements d'exécution, vous devez utiliser l'agent de sécurité dédié entièrement géré.

Runtime Monitoring prend en charge la gestion de l'agent de sécurité pour vos ECS clusters Amazon (AWS Fargate) uniquement via GuardDuty. La gestion manuelle de l'agent de sécurité sur les ECS clusters Amazon n'est pas prise en charge.

Vous pouvez GuardDuty autoriser la gestion de l'agent GuardDuty de sécurité en votre nom, en utilisant la configuration automatique de l'agent pour un AWS compte ou une organisation. GuardDuty commencera à déployer l'agent de sécurité sur les nouvelles tâches Fargate lancées

dans vos clusters Amazon. ECS La liste suivante indique ce à quoi vous devez vous attendre lorsque vous activez l'agent GuardDuty de sécurité.

Impact de l'activation de l'agent GuardDuty de sécurité

GuardDuty crée un point de terminaison de cloud privé virtuel (VPC)

Lorsque vous déployez l'agent GuardDuty de sécurité, GuardDuty vous créez un VPC point de terminaison via lequel l'agent de sécurité transmet les événements d'exécution GuardDuty.

Remarques

- Utilisation d'un agent centralisé VPC avec un agent automatisé — Lorsque vous utilisez la configuration d'agent GuardDuty automatisée pour un type de ressource, GuardDuty vous créez un VPC point de terminaison en votre nom pour tous lesVPCs. Cela inclut les systèmes centralisés VPC et parlésVPCs. GuardDuty ne prend pas en charge la création d'un VPC point de terminaison uniquement pour le système centraliséVPC. Pour plus d'informations sur le VPC fonctionnement de la centralisation, consultez la section VPCPoints de terminaison de l'interface dans le AWS livre blanc intitulé « Création d'une infrastructure multiréseau évolutive et sécurisée ». VPC AWS
- Il n'y a aucun coût supplémentaire pour l'utilisation du VPC terminal.

GuardDuty ajoute un conteneur de sidecar

Pour une nouvelle tâche ou un nouveau service Fargate qui commence à s'exécuter, GuardDuty un conteneur (sidecar) s'attache à chaque conteneur au sein de la tâche Amazon Fargate. ECS L'agent GuardDuty de sécurité fonctionne dans le GuardDuty conteneur joint. Cela permet GuardDuty de collecter les événements d'exécution de chaque conteneur exécuté dans le cadre de ces tâches.

Lorsque vous démarrez une tâche Fargate, si GuardDuty le conteneur (sidecar) ne peut pas être lancé correctement, la surveillance du temps d'exécution est conçue pour ne pas empêcher l'exécution des tâches.

Par défaut, une tâche Fargate est immuable. GuardDuty ne déploiera pas le sidecar lorsqu'une tâche est déjà en cours d'exécution. Si vous souhaitez surveiller un conteneur dans une tâche déjà en cours d'exécution, vous pouvez arrêter la tâche et la redémarrer.

Comment fonctionne le Runtime Monitoring avec les EKS clusters Amazon

Runtime Monitoring utilise un EKSmodule complémentaire `aws-guardduty-agent`, également appelé agent GuardDuty de sécurité. Une fois l'agent de GuardDuty sécurité déployé sur vos EKS clusters, GuardDuty il est en mesure de recevoir des événements d'exécution pour ces EKS clusters.

GuardDuty prend en charge EKS les clusters Amazon exécutés uniquement sur EC2 des instances Amazon. GuardDuty ne prend pas en charge les EKS clusters Amazon exécutés sur AWS Fargate.

Vous pouvez surveiller les événements d'exécution de vos EKS clusters Amazon au niveau du compte ou du cluster. Vous ne pouvez gérer l'agent de GuardDuty sécurité que pour les EKS clusters Amazon que vous souhaitez surveiller pour détecter les menaces. Vous pouvez gérer l'agent GuardDuty de sécurité manuellement ou en l'autorisant GuardDuty à le gérer en votre nom, à l'aide de la configuration automatisée de l'agent.

Lorsque vous utilisez l'approche de configuration automatique de l'agent GuardDuty pour permettre de gérer le déploiement de l'agent de sécurité en votre nom, celui-ci crée automatiquement un point de terminaison Amazon Virtual Private Cloud (AmazonVPC). L'agent de sécurité transmet les événements d'exécution à l'aide GuardDuty de ce point de VPC terminaison Amazon.

> **Remarques**
>
> - Il n'y a aucun coût supplémentaire pour l'utilisation du VPC terminal.
> - Utilisation d'un agent centralisé VPC avec un agent automatisé — Lorsque vous utilisez la configuration d'agent GuardDuty automatisée pour un type de ressource, GuardDuty vous créez un VPC point de terminaison en votre nom pour tous lesVPCs. Cela inclut les systèmes centralisés VPC et parlésVPCs. GuardDuty ne prend pas en charge la création d'un VPC point de terminaison uniquement pour le système centraliséVPC. Pour plus d'informations sur le VPC fonctionnement de la centralisation, consultez la section VPCPoints de terminaison de l'interface dans le AWS livre blanc intitulé « Création d'une infrastructure multiréseau évolutive et sécurisée ». VPC AWS

Après la configuration de la surveillance de l'exécution

Évaluez la couverture du temps d'

Après avoir activé la surveillance du temps d'exécution et déployé l'agent de GuardDuty sécurité, nous vous recommandons d'évaluer en permanence l'état de couverture de la ressource sur laquelle vous avez déployé l'agent de sécurité. L'état de couverture peut être sain ou malsain. Un état de couverture sain indique que la ressource correspondante GuardDuty reçoit les événements d'exécution en cas d'activité au niveau du système d'exploitation.

Lorsque l'état de couverture devient sain pour la ressource, elle GuardDuty est en mesure de recevoir les événements d'exécution et de les analyser pour détecter les menaces. Lorsque vous GuardDuty détectez une menace de sécurité potentielle dans les tâches ou les applications exécutées dans vos charges de travail et instances de conteneur, GuardDuty génère un ou plusieurs types de résultats de surveillance du temps d'exécution.

Vous pouvez également configurer un Amazon EventBridge (EventBridge) pour recevoir une notification lorsque le statut de couverture passe de Malsain à Santé ou autre. Pour de plus amples informations, veuillez consulter Évaluation de la couverture d'exécution de vos ressources.

Configuration CPU et surveillance de la mémoire pour l'agent GuardDuty de sécurité

Après avoir vérifié que l'état de couverture est « sain », vous pouvez évaluer les performances de l'agent de sécurité pour votre type de ressource. Pour les EKS clusters Amazon dotés de la version 1.5 ou supérieure de l'agent de sécurité, GuardDuty prend en charge la configuration des paramètres de l'agent de sécurité (module complémentaire). Pour de plus amples informations, veuillez consulter Configuration CPU et surveillance de la mémoire.

GuardDuty détecte les menaces potentielles

Dès qu'il GuardDuty commence à recevoir les événements d'exécution de votre ressource, il commence à analyser ces événements. Lorsqu'une menace de sécurité potentielle est GuardDuty détectée dans l'une de vos EC2 instances Amazon, ECS clusters Amazon ou EKS clusters Amazon, elle en génère une ou pluriellesTypes de recherche liés à la surveillance du temps. Vous pouvez accéder aux détails de la recherche pour consulter les détails des ressources concernées.

Comment fonctionne l'essai gratuit de 30 jours dans Runtime Monitoring

La période d'essai gratuite de 30 jours fonctionne différemment pour les nouveaux GuardDuty comptes et pour les comptes existants qui ont déjà activé la surveillance du temps EKS d'exécution avant que la fonctionnalité de surveillance du temps d'exécution ne soit étendue aux EC2 instances Amazon et AWS Fargate (Amazon ECS uniquement).

J'utilise la période GuardDuty d'essai ou je n'ai jamais activé la surveillance du temps EKS d'exécution

La liste suivante explique le fonctionnement de la période d'essai gratuite de 30 jours si vous utilisez la période d'essai de GuardDuty 30 jours ou si vous n'avez jamais activé la surveillance du temps EKS d'exécution :

- Lorsque vous l'activez GuardDuty pour la première fois, la surveillance du temps d'EKSexécution et la surveillance du temps d'exécution ne sont pas activées par défaut.

  Lorsque vous activez la surveillance du temps d'exécution pour votre compte ou votre organisation, assurez-vous de configurer également l'agent de GuardDuty sécurité pour la ressource que vous souhaitez surveiller pour détecter les menaces. Par exemple, si vous souhaitez utiliser le Runtime Monitoring pour vos EC2 instances Amazon, après avoir activé le Runtime Monitoring, vous devez également configurer l'agent de sécurité pour AmazonEC2. Vous pouvez choisir de le faire manuellement ou automatiquement GuardDuty.
- Le plan de protection Runtime Monitoring est activé au niveau du compte. La période d'essai gratuite de 30 jours fonctionne au niveau des ressources. Une fois que l'agent de GuardDuty sécurité est déployé sur un type de ressource spécifique, l'essai gratuit de 30 jours commence lorsque le premier événement d'exécution associé à ce type de ressource est GuardDuty reçu. Par exemple, vous avez déployé l' GuardDuty agent au niveau des ressources (pour une EC2 instance Amazon, un ECS cluster Amazon et un EKS cluster Amazon). Dès GuardDuty réception du premier événement d'exécution pour une EC2 instance Amazon, l'essai gratuit de 30 jours commence EC2 uniquement pour Amazon.
- Lorsque vous souhaitez activer uniquement la surveillance de l'EKSexécution : lorsque vous l'activez GuardDuty pour la première fois, la surveillance du temps EKS d'exécution n'est pas activée par défaut (après la sortie de la surveillance du temps d'exécution). Vous devez activer la surveillance du EKS temps d'exécution. Pour l'utiliser de manière optimale, assurez-vous de

gérer l'agent de GuardDuty sécurité manuellement ou d'activer la configuration automatique de l'agent afin qu'il GuardDuty gère l'agent en votre nom. Votre période d'essai gratuite de 30 jours pour EKS Runtime Monitoring commence lorsque GuardDuty vous recevez son premier événement d'exécution pour la EKS ressource Amazon.

J'ai activé EKS Runtime Monitoring avant le lancement de Runtime Monitoring

- Pour un GuardDuty compte existant sur lequel le plan de protection EKS Runtime Monitoring est activé et qui utilise l'expérience de la GuardDuty console pour utiliser ce plan de protection : avec l'annonce de Runtime Monitoring, l'expérience de la console EKS Runtime Monitoring est désormais consolidée dans Runtime Monitoring. Votre configuration actuelle pour EKS Runtime Monitoring reste la même. Vous pouvez continuer à utiliser le CLI supportAPI/pour effectuer des opérations associées à la surveillance du EKS temps d'exécution.
- Pour utiliser le EKS Runtime Monitoring dans le cadre du Runtime Monitoring, vous devez configurer le Runtime Monitoring pour votre compte ou votre organisation. Pour conserver la même configuration pour la surveillance du temps d'exécution, voirMigration de la surveillance du temps EKS d'exécution vers la surveillance du temps d'exécution. Toutefois, cela n'aura aucune incidence sur votre essai gratuit de 30 jours pour Amazon EKS Resource.
- Le plan de protection Runtime Monitoring est activé au niveau du compte par région. Une fois l'agent de GuardDuty sécurité déployé sur l'un des types de ressources spécifiés (EC2instance Amazon et ECS cluster Amazon), l'essai gratuit de 30 jours commence lorsque le premier événement d'exécution associé à la ressource est GuardDuty reçu. Un essai gratuit de 30 jours est associé à chaque type de ressource.

  Par exemple, après avoir activé la surveillance du temps d'exécution, vous choisissez de déployer l' GuardDuty agent uniquement sur une EC2 instance Amazon. L'essai gratuit de 30 jours pour cette ressource ne débutera que lors de la GuardDuty réception de son premier événement d'exécution pour une EC2 instance Amazon. Plus tard, lorsque vous déploierez l' GuardDuty agent pour Fargate (ECSAmazon uniquement), l'essai gratuit de 30 jours pour cette ressource GuardDuty ne débutera que lors de la réception de son premier événement d'exécution pour le cluster Amazon. ECS Si vous avez déjà activé la surveillance du temps EKS d'exécution pour votre compte, GuardDuty cela ne réinitialise pas l'essai gratuit de 30 jours pour une EKS ressource Amazon.

Concepts clés - Approches de gestion des agents GuardDuty de sécurité

Examinez les concepts clés qui vous aideront à gérer l'agent de sécurité sur vos EKS clusters Amazon et vos ECS clusters Amazon.

Table des matières

Ressource Fargate (ECSAmazon uniquement) - Approches GuardDuty pour gérer les agents de sécurité

La surveillance du temps d'exécution vous permet de détecter les menaces de sécurité potentielles sur tous les ECS clusters Amazon (au niveau du compte) ou sur des clusters sélectifs (au niveau du cluster) de votre compte. Lorsque vous activez la configuration automatisée des agents pour chaque tâche Amazon ECS Fargate qui sera exécutée GuardDuty , un conteneur annexe sera ajouté pour chaque charge de travail de conteneur au sein de cette tâche. L'agent GuardDuty de sécurité est déployé dans ce conteneur de side-car. C'est ainsi que l' GuardDuty on obtient une visibilité sur le comportement d'exécution des conteneurs dans les ECS tâches Amazon.

Runtime Monitoring prend en charge la gestion de l'agent de sécurité pour vos ECS clusters Amazon (AWS Fargate) uniquement via GuardDuty. La gestion manuelle de l'agent de sécurité sur les ECS clusters Amazon n'est pas prise en charge.

Avant de configurer vos comptes, déterminez comment vous souhaitez gérer l'agent de GuardDuty sécurité et éventuellement surveiller le comportement d'exécution des conteneurs appartenant aux ECS tâches Amazon. Envisagez les approches suivantes.

Rubriques

Gérez l'agent GuardDuty de sécurité pour tous les ECS clusters Amazon

Cette approche vous aidera à détecter les menaces de sécurité potentielles au niveau du compte. Utilisez cette approche lorsque vous GuardDuty souhaitez détecter des menaces de sécurité potentielles pour tous les ECS clusters Amazon appartenant à votre compte.

Gérez l'agent de GuardDuty sécurité pour la plupart des ECS clusters Amazon, mais excluez certains ECS clusters Amazon

Utilisez cette approche lorsque vous GuardDuty souhaitez détecter des menaces de sécurité potentielles pour la plupart des ECS clusters Amazon de votre AWS environnement, mais en exclure certains. Cette approche vous permet de surveiller le comportement d'exécution des conteneurs au sein de vos ECS tâches Amazon au niveau du cluster. Par exemple, le nombre de ECS clusters Amazon appartenant à votre compte est de 1 000. Toutefois, vous ne souhaitez surveiller que 930 ECS clusters Amazon.

Cette approche vous oblige à ajouter une GuardDuty balise prédéfinie aux ECS clusters Amazon que vous ne souhaitez pas surveiller. Pour de plus amples informations, veuillez consulter Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS.

Gérer l'agent GuardDuty de sécurité pour certains ECS clusters Amazon

Utilisez cette approche lorsque vous GuardDuty souhaitez détecter des menaces de sécurité potentielles pour certains ECS clusters Amazon. Cette approche vous permet de surveiller le comportement d'exécution des conteneurs au sein de vos ECS tâches Amazon au niveau du cluster. Par exemple, le nombre de ECS clusters Amazon appartenant à votre compte est de 1 000. Toutefois, vous ne souhaitez surveiller que 230 clusters.

Cette approche nécessite que vous ajoutiez une GuardDuty balise prédéfinie aux ECS clusters Amazon que vous souhaitez surveiller. Pour de plus amples informations, veuillez consulter Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS.

Amazon EKS clusters - Approches pour gérer les agents GuardDuty de sécurité

GuardDuty Pour utiliser les événements d'exécution de vos EKS clusters au niveau du compte ou du cluster, il est nécessaire de gérer l'agent GuardDuty de sécurité pour les clusters correspondants.

Approches de gestion des agents GuardDuty de sécurité

Avant le 13 septembre 2023, vous pouviez configurer GuardDuty pour gérer l'agent de sécurité au niveau du compte. Ce comportement indique que, par défaut, GuardDuty il gérera l'agent de sécurité sur tous les EKS clusters appartenant à un Compte AWS. Désormais, GuardDuty fournit une fonctionnalité granulaire pour vous aider à choisir les EKS clusters dans lesquels vous GuardDuty souhaitez gérer l'agent de sécurité.

Lorsque vous le souhaitezGestion manuelle GuardDuty de l'agent de sécurité, vous pouvez toujours sélectionner les EKS clusters que vous souhaitez surveiller. Toutefois, pour gérer l'agent manuellement, la création d'un point de VPC terminaison Amazon pour vous Compte AWS est une condition préalable.

> **Note**
>
> Quelle que soit l'approche que vous utilisez pour gérer l'agent GuardDuty de sécurité, la surveillance du temps EKS d'exécution est toujours activée au niveau du compte.

Rubriques

- Gérez l'agent de sécurité via GuardDuty
- Gestion manuelle GuardDuty de l'agent de sécurité

Gérez l'agent de sécurité via GuardDuty

GuardDuty déploie et gère l'agent de sécurité en votre nom. À tout moment, vous pouvez surveiller les EKS clusters de votre compte en utilisant l'une des approches suivantes.

Rubriques

- Surveillez tous les EKS clusters
- Surveillez tous les EKS clusters et excluez les EKS clusters sélectifs
- Surveiller des EKS clusters sélectifs

Surveillez tous les EKS clusters

- Quand utiliser cette approche : utilisez cette approche lorsque vous GuardDuty souhaitez déployer et gérer l'agent de sécurité pour tous les EKS clusters de votre compte. Par défaut, l'agent de

sécurité GuardDuty sera également déployé sur un nouveau EKS cluster potentiellement créé dans votre compte.

- Impact de l'utilisation de cette approche :
  - GuardDuty crée un point de terminaison Amazon Virtual Private Cloud (AmazonVPC) via lequel l'agent de GuardDuty sécurité transmet les événements d'exécution GuardDuty. La création du point de VPC terminaison Amazon n'entraîne aucun coût supplémentaire lorsque vous gérez l'agent de sécurité via GuardDuty.
  - Il est nécessaire que votre nœud de travail dispose d'un chemin réseau valide vers un point de `guardduty-data` VPC terminaison actif. GuardDuty déploie l'agent de sécurité sur vos EKS clusters. Amazon Elastic Kubernetes Service (EKSAmazon) coordonnera le déploiement de l'agent de sécurité sur les nœuds des clusters. EKS
  - Sur la base de la disponibilité des adresses IP, GuardDuty sélectionne le sous-réseau pour créer un VPC point de terminaison. Si vous utilisez des topologies réseau avancées, vous devez vérifier que la connectivité est possible.
- Remarque — Actuellement, lorsque vous utilisez cette option, EKS Runtime Monitoring ne crée pas de partageVPC.

Surveillez tous les EKS clusters et excluez les EKS clusters sélectifs

- Quand utiliser cette approche : utilisez cette approche lorsque vous GuardDuty souhaitez gérer l'agent de sécurité pour tous les EKS clusters de votre compte, mais exclure certains EKS clusters.

  Cette méthode utilise une approche basée sur les balises [1] dans laquelle vous pouvez étiqueter les EKS clusters pour lesquels vous ne souhaitez pas recevoir les événements d'exécution. La balise prédéfinie doit avoir `GuardDutyManaged-false` comme paire clé-valeur.
- Impact de l'utilisation de cette approche :
  - Cette approche nécessite que vous n'activiez la gestion automatique des GuardDuty agents qu'après avoir ajouté des balises aux EKS clusters que vous souhaitez exclure de la surveillance.

    Par conséquent, l'impact lorsque vous Gérez l'agent de sécurité via GuardDuty s'applique également à cette approche. Lorsque vous ajoutez des balises avant d'activer la gestion automatique des agents, l' GuardDuty agent de sécurité ne GuardDuty sera ni déployé ni géré pour les EKS clusters exclus de la surveillance.
- Considérations :

- Vous devez ajouter la paire clé-valeur du tag sous la forme suivante `GuardDutyManaged` : `false` pour les EKS clusters sélectifs avant d'activer la configuration automatisée de l'agent, sinon l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters jusqu'à ce que vous utilisiez le tag.
- Vous devez empêcher la modification des balises, sauf par des identités approuvées.

  > **Important**
  >
  > Gérez les autorisations permettant de modifier la valeur de la `GuardDutyManaged` balise pour votre EKS cluster à l'aide de politiques ou de politiques de contrôle IAM des services. Pour plus d'informations, voir Politiques de contrôle des services (SCPs) dans le guide de AWS Organizations l'utilisateur ou Contrôler l'accès aux AWS ressources dans le guide de IAM l'utilisateur.

- Pour un EKS cluster potentiellement nouveau que vous ne souhaitez pas surveiller, assurez-vous d'ajouter la paire `GuardDutyManaged` `false` clé-valeur au moment de créer ce EKS cluster.
- Cette approche tiendra également compte des mêmes considérations que celles spécifiées pour Surveillez tous les EKS clusters.

Surveiller des EKS clusters sélectifs

- Quand utiliser cette approche : utilisez cette approche lorsque vous souhaitez GuardDuty déployer et gérer les mises à jour de l'agent de sécurité uniquement pour certains EKS clusters de votre compte. Cette méthode utilise une approche basée sur les balises [1] dans laquelle vous pouvez étiqueter le EKS cluster pour lequel vous souhaitez recevoir les événements d'exécution.
- Impact de l'utilisation de cette approche :
  - En utilisant des balises d'inclusion, l'agent de sécurité GuardDuty sera automatiquement déployé et géré uniquement pour les EKS clusters sélectionnés marqués « `GuardDutyManaged` - » `true` en tant que paire clé-valeur.
  - L'utilisation de cette approche aura également le même impact que celui spécifié pour Surveillez tous les EKS clusters.
- Considérations :

- Si la valeur de la `GuardDutyManaged` balise n'est pas définie sur`true`, la balise d'inclusion ne fonctionnera pas comme prévu, ce qui peut avoir un impact sur la surveillance de votre EKS cluster.
- Pour vous assurer que vos EKS clusters sélectifs sont surveillés, vous devez empêcher la modification des balises, sauf par des identités fiables.

  > **Important**
  >
  > Gérez les autorisations permettant de modifier la valeur de la `GuardDutyManaged` balise pour votre EKS cluster à l'aide de politiques ou de politiques de contrôle IAM des services. Pour plus d'informations, voir Politiques de contrôle des services (SCPs) dans le guide de AWS Organizations l'utilisateur ou Contrôler l'accès aux AWS ressources dans le guide de IAM l'utilisateur.

- Pour un EKS cluster potentiellement nouveau que vous ne souhaitez pas surveiller, assurez-vous d'ajouter la paire `GuardDutyManaged` `false` clé-valeur au moment de créer ce EKS cluster.
- Cette approche tiendra également compte des mêmes considérations que celles spécifiées pour Surveillez tous les EKS clusters.

[1] Pour plus d'informations sur le balisage de EKS clusters sélectifs, consultez la section Marquage de vos EKS ressources Amazon dans le guide de EKSl'utilisateur Amazon.

Gestion manuelle GuardDuty de l'agent de sécurité

- Quand utiliser cette approche : utilisez cette approche lorsque vous souhaitez déployer et gérer manuellement l'agent de GuardDuty sécurité sur tous vos EKS clusters. Assurez-vous que la surveillance du temps EKS d'exécution est activée pour vos comptes. L'agent GuardDuty de sécurité risque de ne pas fonctionner comme prévu si vous n'activez pas la surveillance du EKS temps d'exécution.
- Impact de l'utilisation de cette approche — Vous devrez coordonner le déploiement du logiciel de l'agent de GuardDuty sécurité au sein de vos EKS clusters sur tous les comptes et sur les Régions AWS sites où cette fonctionnalité est disponible.
- Considérations : vous devez garantir un flux de données sécurisé tout en surveillant et en comblant les lacunes de couverture à mesure que de nouveaux clusters et de nouvelles charges de travail sont déployés en permanence.

Activer la surveillance du GuardDuty temps d'exécution

Avant d'activer la surveillance du temps d'exécution dans votre compte, assurez-vous que le type de ressource pour lequel vous souhaitez surveiller les événements d'exécution répond aux exigences de la plate-forme. Pour de plus amples informations, veuillez consulter Prérequis.

Si vous utilisiez EKS Runtime Monitoring avant le lancement de Runtime Monitoring, vous pouvez utiliser le APIs pour vérifier et mettre à jour la configuration existante pour EKS Runtime Monitoring. Vous pouvez également migrer votre configuration existante de EKS Runtime Monitoring vers Runtime Monitoring. Pour de plus amples informations, veuillez consulter Migration de la surveillance du temps EKS d'exécution vers la surveillance du temps d'exécution.

> **Note**
>
> À l'heure actuelle, cette documentation fournit les étapes permettant d'activer la surveillance du temps d'exécution pour vos comptes et votre organisation par console uniquement. Vous pouvez également activer la surveillance du temps d'exécution à l'aide d'APIActions ou AWS CLI pour GuardDuty.

Vous pouvez configurer la surveillance du temps d'exécution en suivant les étapes décrites dans les rubriques suivantes.

Table des matières

Conditions préalables à l'activation de la surveillance du temps d'exécution

Pour activer la surveillance du temps d'exécution et gérer l'agent de GuardDuty sécurité, vous devez remplir les conditions requises pour chaque type de ressource que vous souhaitez surveiller pour détecter les menaces.

Table des matières

- Conditions requises pour le support des EC2 instances Amazon
- Conditions préalables à l' AWS Fargate assistance (Amazon ECS uniquement)
- Conditions préalables à la prise en charge des EKS clusters Amazon
- Utilisation de l'infrastructure en tant que code (IaC) avec des agents de sécurité GuardDuty automatisés

Conditions requises pour le support des EC2 instances Amazon

Gérer EC2 les SSM instances

Les EC2 instances Amazon pour lesquelles vous GuardDuty souhaitez surveiller les événements d'exécution doivent être AWS Systems Manager (SSM) gérées. Cela vaut indépendamment du fait que vous l'utilisiez GuardDuty pour gérer l'agent de sécurité automatiquement ou manuellement (sauf Méthode 2 - En utilisant les gestionnaires de packages Linux).

Pour gérer vos EC2 instances Amazon avec AWS Systems Manager, consultez la section Configuration de Systems Manager pour les EC2 instances Amazon dans le Guide de AWS Systems Manager l'utilisateur.

Validation des exigences architecturales

L'architecture de la distribution de votre système d'exploitation peut avoir un impact sur le comportement GuardDuty de l'agent de sécurité. Vous devez répondre aux exigences suivantes avant d'utiliser Runtime Monitoring pour les EC2 instances Amazon :

- Le tableau suivant indique la distribution du système d'exploitation qui a été vérifiée pour prendre en charge l'agent GuardDuty de sécurité pour les EC2 instances Amazon.

Distribution du système d'exploitation	Version de noyau	Support du noyau	CPUarchitecture	
			64 bits (AMD64)	Gravitone (1) ARM64
• AL2et AL2 023 • Ubuntu 20.04 et Ubuntu 22.04	5,4, 5,10, 5,15, 6,1, 6,5, 6,8	eBPF, Tracepoints, Kprobe	Pris en charge	Pris en charge

  - Debian 11 et
    Debian 12

- Exigences supplémentaires - Uniquement si vous avez Amazon ECS /Amazon EC2

  Pour Amazon ECS /AmazonEC2, nous vous recommandons d'utiliser la dernière version ECS optimisée pour Amazon AMIs (datée du 29 septembre 2023 ou ultérieure) ou d'utiliser la version v1.77.0 de ECS l'agent Amazon.

Validation de la politique de contrôle des services de votre organisation

Si vous avez défini une politique de contrôle des services (SCP) pour gérer les autorisations dans votre organisation, vérifiez que la limite des autorisations n'est pas restrictive`guardduty:SendSecurityTelemetry`. Il est nécessaire pour GuardDuty prendre en charge la surveillance du temps d'exécution sur différents types de ressources.

Si vous êtes un compte membre, connectez-vous à l'administrateur délégué associé. Pour plus d'informations sur la gestion SCPs de votre organisation, voir Politiques de contrôle des services (SCPs).

Lors de l'utilisation de la configuration automatique des agents

Pour Utiliser la configuration automatique des agents (recommandé) cela, vous Compte AWS devez remplir les prérequis suivants :

- Lorsque vous utilisez des balises d'inclusion avec une configuration d'agent automatisée, GuardDuty pour créer une SSM association pour une nouvelle instance, assurez-vous que la nouvelle instance est SSM gérée et qu'elle apparaît sous Fleet Manager dans la https://console.aws.amazon.com/systems-manager/console.
- Lorsque vous utilisez des balises d'exclusion avec une configuration automatique de l'agent :
  - Ajoutez le `false` tag `GuardDutyManaged` : avant de configurer l'agent GuardDuty automatique pour votre compte.

    Assurez-vous d'ajouter la balise d'exclusion à vos EC2 instances Amazon avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour AmazonEC2, toute EC2 instance lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.
  - Pour que les balises d'exclusion fonctionnent, mettez à jour la configuration de l'instance afin que le document d'identité de l'instance soit disponible dans le service de métadonnées d'instance

(IMDS). La procédure pour effectuer cette étape fait déjà partie Activer la surveillance du temps d'exécution de votre compte.

CPUet limite de mémoire pour GuardDuty l'agent

CPUlimite

La CPU limite maximale pour l'agent GuardDuty de sécurité associé aux EC2 instances Amazon est de 10 % du total des v CPU cores. Par exemple, si votre EC2 instance possède 4 CPU cœurs, l'agent de sécurité peut utiliser au maximum 40 % des 400 % disponibles.

Limite de mémoire

En ce qui concerne la mémoire associée à votre EC2 instance Amazon, l'agent de GuardDuty sécurité peut utiliser une quantité limitée de mémoire.

Le tableau suivant indique la limite de mémoire.

Mémoire de l'EC2instance Amazon	Mémoire maximale pour l' GuardDuty agent
Moins de 8 Go	128 Mo
Moins de 32 Go	256 Mo
Plus ou égal à 32 Go	1 Go

Étape suivante

L'étape suivante consiste à configurer la surveillance du temps d'exécution et à gérer l'agent de sécurité (automatiquement ou manuellement).

Conditions préalables à l' AWS Fargate assistance (Amazon ECS uniquement)

Validation des exigences architecturales

La plate-forme que vous utilisez peut avoir un impact sur GuardDuty la manière dont l'agent de sécurité prend GuardDuty en charge la réception des événements d'exécution de vos ECS clusters Amazon. Vous devez confirmer que vous utilisez l'une des plateformes vérifiées.

Considérations initiales :

La AWS Fargate (Fargate) plate-forme de vos ECS clusters Amazon doit être Linux. La version de plateforme correspondante doit être au moins`1.4.0`, ou`LATEST`. Pour plus d'informations sur les versions de la plateforme, consultez la section Versions de la plateforme Linux dans le manuel Amazon Elastic Container Service Developer Guide.

Les versions de la plateforme Windows ne sont pas encore prises en charge.

Plateformes vérifiées

La distribution et l'CPUarchitecture du système d'exploitation ont un impact sur le support fourni par l'agent GuardDuty de sécurité. Le tableau suivant présente la configuration vérifiée pour le déploiement de l'agent de GuardDuty sécurité et la configuration de la surveillance du temps d'exécution.

Distribution du système d'exploitation	Support du noyau	CPUarchitecture	
		64 bits (AMD64)	Gravitone (1) ARM64
Linux	eBPF, Tracepoints, Kprobe	Pris en charge	Pris en charge

Fournir ECR les autorisations et les détails du sous-réseau

Avant d'activer la surveillance du temps d'exécution, vous devez fournir les informations suivantes :

Fournir un rôle d'exécution de tâches avec des autorisations

Le rôle d'exécution des tâches nécessite que vous disposiez de certaines autorisations Amazon Elastic Container Registry (AmazonECR). Vous pouvez soit utiliser la politique mazonECSTask ExecutionRolePolicy gérée A, soit ajouter les autorisations suivantes à votre `TaskExecutionRole` politique :

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
```

```
...
```

Pour restreindre davantage les ECR autorisations Amazon, vous pouvez ajouter le ECR référentiel Amazon URI qui héberge l'agent GuardDuty de sécurité pour AWS Fargate (Amazon ECS uniquement). Pour de plus amples informations, veuillez consulter Référentiel pour GuardDuty agent sur AWS Fargate (Amazon ECS uniquement).

Fournir les détails du sous-réseau dans la définition des tâches

Vous pouvez soit fournir les sous-réseaux publics en tant qu'entrée dans la définition de votre tâche, soit créer un point de ECR VPC terminaison Amazon.

- Utilisation de l'option de définition des tâches : pour exécuter le CreateServiceet UpdateServiceAPIsdans le Amazon Elastic Container Service API Reference, vous devez transmettre les informations du sous-réseau. Pour plus d'informations, consultez les définitions des ECS tâches Amazon dans le manuel Amazon Elastic Container Service Developer Guide.
- En utilisant l'option Amazon ECR VPC Endpoint — Fournissez le chemin réseau vers Amazon ECR — Assurez-vous que le ECR référentiel URI Amazon hébergeant l'agent GuardDuty de sécurité est accessible au réseau. Si vos tâches Fargate doivent être exécutées dans un sous-réseau privé, Fargate aura besoin du chemin réseau pour télécharger le conteneur. GuardDuty

  Pour plus d'informations sur l'activation de Fargate pour télécharger GuardDuty le conteneur, consultez la section Utilisation des ECR images Amazon avec Amazon ECS dans le guide de l'utilisateur d'Amazon Elastic Container Registry.

Validation de la politique de contrôle des services de votre organisation

Cette étape est nécessaire pour GuardDuty prendre en charge la surveillance du temps d'exécution et évaluer la couverture des différents types de ressources.

Si vous avez défini une politique de contrôle des services (SCP) pour gérer les autorisations dans votre organisation, vérifiez que la limite des autorisations n'est pas restrictive `guardduty:SendSecurityTelemetry` dans votre politique `TaskExecutionRole` et dans la vôtre.

La politique suivante est un exemple d'autorisation de la `guardduty:SendSecurityTelemetry` stratégie :

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
    "Effect": "Allow",
            "Action": [
                ...,
                ...,
                "guardduty:SendSecurityTelemetry"
            ],
            "Resource": "*"
        }
    ]
}
```

1. Suivez les étapes suivantes pour vérifier que la limite des autorisations n'est pas restrictive `guardduty:SendSecurityTelemetry` :
    1. Connectez-vous à la IAM console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
    2. Dans le volet de navigation, sous Gestion des accès, sélectionnez Rôles.
    3. Choisissez le nom du rôle pour la page de détails.
    4. Développez la section Limite des autorisations. Assurez-vous que le n'`guardduty:SendSecurityTelemetry`est pas refusé ou restreint.
2. Suivez les étapes suivantes pour vérifier que les limites d'autorisations de votre `TaskExecutionRole` politique ne sont pas restrictives `guardduty:SendSecurityTelemetry` :
    1. Connectez-vous à la IAM console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
    2. Dans le volet de navigation, sous Gestion des accès, sélectionnez Politiques.
    3. Choisissez le nom de la politique pour la page de détails.
    4. Sous l'onglet Entités jointes, consultez la section Les entités jointes en tant que limite d'autorisations. Assurez-vous que le n'`guardduty:SendSecurityTelemetry`est pas refusé ou restreint.

Pour plus d'informations sur les politiques et les autorisations, consultez la section Limites des autorisations dans le guide de IAM l'utilisateur.

Si vous êtes un compte membre, connectez-vous à l'administrateur délégué associé. Pour plus d'informations sur la gestion SCPs de votre organisation, voir Politiques de contrôle des services (SCPs).

CPUet limites de mémoire

Dans la définition de la tâche Fargate, vous devez spécifier la valeur et CPU la valeur de mémoire au niveau de la tâche. Le tableau suivant indique les combinaisons valides de valeurs de niveau de tâche CPU et de mémoire, ainsi que la limite de mémoire maximale de l'agent de GuardDuty sécurité correspondant pour le GuardDuty conteneur.

CPUvaleur	Valeur de mémoire	GuardDuty limite de mémoire maximale de l'agent
256 (0,25 V) CPU	512 MiB, 1 Go, 2 Go	128 Mo
512 (0,5 VCPU)	1 Go, 2 Go, 3 Go, 4 Go	
1024 (1 vCPU)	2 GO, 3 GO, 4 GO	
	5 GO, 6 GO, 7 GO, 8 GO	
2048 (2 vCPU)	Entre 4 Go et 16 Go par incréments de 1 Go	
4096 (4 vCPU)	Entre 8 Go et 20 Go par incréments de 1 Go	
8192 (8 vCPU)	Entre 16 Go et 28 Go par incréments de 4 Go	256 Mo
	Entre 32 Go et 60 Go par incréments de 4 Go	512 Mo
16384 (16 vCPU)	Entre 32 Go et 120 Go par incréments de 8 Go	1 Go

Après avoir activé la surveillance du temps d'exécution et vérifié que l'état de couverture de votre cluster est sain, vous pouvez configurer et consulter les métriques Container Insight. Pour plus d'informations, consultez Configuration de la surveillance sur le ECS cluster Amazon.

L'étape suivante consiste à configurer la surveillance du temps d'exécution ainsi que l'agent de sécurité.

Conditions préalables à la prise en charge des EKS clusters Amazon

Validation des exigences architecturales

La plate-forme que vous utilisez peut avoir un impact sur GuardDuty la manière dont l'agent de sécurité prend GuardDuty en charge la réception des événements d'exécution de vos EKS clusters. Vous devez confirmer que vous utilisez l'une des plateformes vérifiées. Si vous gérez l' GuardDuty agent manuellement, assurez-vous que la version de Kubernetes prend en charge la version de l' GuardDuty agent actuellement utilisée.

Plateformes vérifiées

La distribution du système d'exploitation, la version du noyau et CPU l'architecture ont une incidence sur le support fourni par l'agent GuardDuty de sécurité. Le tableau suivant présente la configuration vérifiée pour le déploiement de l'agent de GuardDuty sécurité et la configuration de la surveillance du EKS temps d'exécution.

Distribution du système d'exploitation	Version de noyau	Support du noyau	CPUarchitecture		Version de Kubernetes prise en charge
			64 bits (AMD64)	Gravitone (1) ARM64 (Graviton2 et versions ultérieures) [1]	
Ubuntu AL2 AL2023 [3]	5,4, 5,10, 5,15, 6,1 [2]	Par BPF Tracepoints, K-probe	Pris en charge	Pris en charge	V1.21 - V1.30
Bottlerocket					V1.23 - V1.30

1. La surveillance du temps d'exécution pour les EKS clusters Amazon ne prend pas en charge les instances Graviton de première génération telles que les types d'instances A1.
2. Actuellement, avec la version Kernel`6.1`, je ne GuardDuty peux pas générer Types de recherche liés à la surveillance du temps ceux qui sont liés àDNSévénements.
3. Runtime Monitoring prend en charge la version AL2 0.23 avec la sortie de l'agent de GuardDuty sécurité v1.6.0 et versions ultérieures. Pour de plus amples informations, veuillez consulter GuardDuty agent de sécurité pour les EKS clusters Amazon.

Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty

Le tableau suivant indique les versions de Kubernetes pour vos EKS clusters prises en charge par GuardDuty l'agent de sécurité.

Version de Kubernetes	Version de l'agent GuardDuty de sécurité EKS complémentaire Amazon
1,28 - 1,30	v1.4.1 et versions ultérieures
1,27	v1.3.0, v1.3.1
1,26	v1.2.0
1,21 - 1,25	Toutes les versions

Certaines versions de l'agent GuardDuty de sécurité atteindront la fin du support standard. Pour plus d'informations sur les versions publiées de l'agent, consultezGuardDuty agent de sécurité pour les EKS clusters Amazon.

CPUet limites de mémoire

Le tableau suivant indique les limites CPU et les limites de mémoire du EKS module complémentaire Amazon pour GuardDuty (`aws-guardduty-agent`).

Paramètre	Limite minimum	Limite maximum
CPU	200 m	1 000 m
Mémoire	256 milles	1 024 milles

Lorsque vous utilisez le EKS module complémentaire Amazon version 1.5.0 ou supérieure, il GuardDuty permet de configurer le schéma du module complémentaire pour vos valeurs CPU et celles de la mémoire. Pour plus d'informations sur la plage configurable, consultezParamètres et valeurs configurables.

Une fois que vous avez activé la surveillance du temps EKS d'exécution et évalué l'état de couverture de vos EKS clusters, vous pouvez configurer et consulter les indicateurs d'analyse des conteneurs. Pour de plus amples informations, veuillez consulter Configuration CPU et surveillance de la mémoire.

Étape suivante

L'étape suivante consiste à configurer la surveillance du temps d'exécution et à gérer l'agent de sécurité manuellement ou automatiquement par le biais de cette méthode GuardDuty.

Utilisation de l'infrastructure en tant que code (IaC) avec des agents de sécurité GuardDuty automatisés

Utilisez cette section uniquement si la liste suivante s'applique à votre cas d'utilisation :

- Vous utilisez des outils d'infrastructure en tant que code (IaC), tels que Terraform, pour gérer vos AWS ressources, AWS Cloud Development Kit (AWS CDK) et
- Vous devez activer la configuration GuardDuty automatique des agents pour un ou plusieurs types de ressources : Amazon EKSEC2, Amazon ou Amazon ECS -Fargate.

Présentation du graphe de dépendance des ressources IaC

Lorsque vous activez la configuration GuardDuty automatique de l'agent pour un type de ressource, vous GuardDuty créez automatiquement un VPC point de terminaison et un groupe de sécurité associés à ce VPC point de terminaison, puis installez l'agent de sécurité pour ce type de ressource. Par défaut, le point de VPC terminaison et le groupe de sécurité associé ne GuardDuty seront

supprimés qu'une fois que vous aurez désactivé la surveillance du temps d'exécution. Pour de plus amples informations, veuillez consulter Impact de la désactivation et du nettoyage des ressources.

Lorsque vous utilisez un outil IaC, celui-ci gère un graphe de dépendance des ressources. Au moment de la suppression de ressources à l'aide de l'outil IaC, celui-ci supprime uniquement les ressources qui peuvent être suivies dans le cadre du graphe de dépendance des ressources. Les outils IaC peuvent ne pas connaître les ressources créées en dehors de leur configuration spécifiée. Par exemple, vous créez un VPC avec un outil IaC, puis vous y ajoutez un groupe de sécurité à l'aide VPC d'une AWS console ou d'une API opération. Dans le graphe de dépendance des ressources, la VPC ressource que vous créez dépend du groupe de sécurité associé. Si vous supprimez cette VPC ressource à l'aide de l'outil IaC, vous obtiendrez une erreur. Le moyen de contourner cette erreur consiste à supprimer manuellement le groupe de sécurité associé ou à mettre à jour la configuration IaC pour inclure cette ressource ajoutée.

Problème courant : suppression de ressources dans IaC

Lorsque vous utilisez la configuration GuardDuty automatique des agents, vous souhaiterez peut-être supprimer une ressource (AmazonEKS, Amazon ou Amazon EC2 ECS -Fargate) que vous avez créée à l'aide d'un outil IaC. Toutefois, cette ressource dépend d'un VPC point de terminaison GuardDuty créé. Cela empêche l'outil IaC de supprimer la ressource par lui-même et vous oblige à désactiver la surveillance du temps d'exécution, qui supprime automatiquement le VPC point de terminaison.

Par exemple, lorsque vous tentez de supprimer le VPC point de terminaison GuardDuty créé en votre nom, une erreur similaire aux exemples suivants s'affiche.

Example

Exemple d'erreur lors de l'utilisation CDK

```
The following resource(s) failed to delete:
 [mycdkvpcapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpcapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
 dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
 ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
 HandlerErrorCode: InvalidRequest)
```

Example

Exemple d'erreur lors de l'utilisation de Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
 subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
       status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

Solution - Empêcher le problème de suppression de ressources

Cette section vous aide à gérer le VPC point de terminaison et le groupe de sécurité indépendamment de GuardDuty.

Pour vous approprier totalement les ressources configurées à l'aide de l'outil iAC, effectuez les étapes suivantes dans l'ordre indiqué :

1. Créez unVPC. Pour autoriser l'entrée, associez un GuardDuty VPC point de terminaison au groupe de sécurité, à celaVPC.
2. Activez la configuration GuardDuty automatique des agents pour votre type de ressource

Une fois les étapes précédentes terminées, il ne GuardDuty créera pas son propre VPC point de terminaison et réutilisera celui que vous avez créé à l'aide de l'outil IaC.

Pour plus d'informations sur la création du vôtreVPC, consultez Create a VPC only in the Amazon VPC Transit Gateway. Pour plus d'informations sur la création d'un VPC point de terminaison, consultez la section suivante correspondant à votre type de ressource :

- Pour AmazonEC2, voirCréation manuelle d'un point de VPC terminaison Amazon.
- Pour AmazonEKS, voirConditions préalables au déploiement de l'agent GuardDuty de sécurité.

Activation de la surveillance du temps d'exécution pour un compte autonome

Suivez les étapes ci-dessous pour activer la surveillance du temps d'exécution dans votre compte.

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Dans l'onglet Configuration, choisissez Activer pour activer la surveillance du temps d'exécution pour votre compte.
4. GuardDuty Pour recevoir les événements d'exécution d'un ou de plusieurs types de ressources (une EC2 instance Amazon, un ECS cluster Amazon ou un EKS cluster Amazon), utilisez les options suivantes pour gérer l'agent de sécurité pour ces ressources :

   Pour activer l'agent GuardDuty de sécurité

   - Gestion de l'agent de sécurité automatisé pour l'EC2instance Amazon
   - Gestion manuelle de l'agent de sécurité pour une EC2 instance Amazon
   - Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS
   - Gestion automatique de l'agent de sécurité pour les EKS clusters Amazon
   - Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon

Activation de la surveillance du temps d'exécution pour les environnements à comptes multiples

Dans les environnements à comptes multiples, seul le compte d' GuardDuty administrateur délégué peut activer ou désactiver la surveillance du temps d'exécution pour les comptes des membres et gérer la configuration automatique des agents pour les types de ressources appartenant aux comptes membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter Managing multiple accounts.

Pour le compte GuardDuty d'administrateur délégué

Pour activer la surveillance du temps d'exécution pour le compte GuardDuty administrateur délégué

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sous l'onglet Configuration, choisissez Modifier dans la section Configuration de la surveillance du temps d'exécution.
4. Utilisation d'Activer pour tous les comptes

   Si vous souhaitez activer la surveillance du temps d'exécution pour tous les comptes appartenant à l'organisation, y compris le compte d' GuardDuty administrateur délégué, choisissez Activer pour tous les comptes.
5. Utilisation de Configurer les comptes manuellement

   Si vous souhaitez activer la surveillance du temps d'exécution pour chaque compte membre individuellement, choisissez Configurer les comptes manuellement.

   - Choisissez Activer sous la section Administrateur délégué (ce compte).
6. GuardDuty Pour recevoir les événements d'exécution d'un ou de plusieurs types de ressources (une EC2 instance Amazon, un ECS cluster Amazon ou un EKS cluster Amazon), utilisez les options suivantes pour gérer l'agent de sécurité pour ces ressources :

   Pour activer l'agent GuardDuty de sécurité

   - Gestion de l'agent de sécurité automatisé pour l'EC2instance Amazon
   - Gestion manuelle de l'agent de sécurité pour une EC2 instance Amazon
   - Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS
   - Gestion automatique de l'agent de sécurité pour les EKS clusters Amazon
   - Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon

Pour tous les comptes de membres

Pour activer la surveillance du temps d'exécution pour tous les comptes membres de l'organisation

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide du compte GuardDuty d'administrateur délégué.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sur la page Runtime Monitoring, sous l'onglet Configuration, choisissez Modifier dans la section Configuration de Runtime Monitoring.

4. Choisissez Activer pour tous les comptes.
5. GuardDuty Pour recevoir les événements d'exécution d'un ou de plusieurs types de ressources (une EC2 instance Amazon, un ECS cluster Amazon ou un EKS cluster Amazon), utilisez les options suivantes pour gérer l'agent de sécurité pour ces ressources :

   Pour activer l'agent GuardDuty de sécurité

   - Gestion de l'agent de sécurité automatisé pour l'EC2instance Amazon
   - Gestion manuelle de l'agent de sécurité pour une EC2 instance Amazon
   - Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS
   - Gestion automatique de l'agent de sécurité pour les EKS clusters Amazon
   - Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon

Pour tous les comptes de membres actifs existants

Pour activer la surveillance du temps d'exécution pour les comptes membres existants de l'organisation

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide du compte GuardDuty d'administrateur délégué de l'organisation.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sur la page Runtime Monitoring, sous l'onglet Configuration, vous pouvez consulter l'état actuel de la configuration Runtime Monitoring.
4. Dans le volet Runtime Monitoring, dans la section Comptes membres actifs, sélectionnez Actions.
5. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
6. Choisissez Confirmer.
7. GuardDuty Pour recevoir les événements d'exécution d'un ou de plusieurs types de ressources (une EC2 instance Amazon, un ECS cluster Amazon ou un EKS cluster Amazon), utilisez les options suivantes pour gérer l'agent de sécurité pour ces ressources :

Pour activer l'agent GuardDuty de sécurité

- Gestion de l'agent de sécurité automatisé pour l'EC2instance Amazon
- Gestion manuelle de l'agent de sécurité pour une EC2 instance Amazon
- Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS
- Gestion automatique de l'agent de sécurité pour les EKS clusters Amazon
- Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Activer automatiquement la surveillance du temps d'exécution pour les nouveaux comptes de membres uniquement

Pour activer la surveillance du temps d'exécution pour les nouveaux comptes membres de votre organisation

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide du compte d' GuardDuty administrateur délégué désigné par l'organisation.
2. Dans le volet de navigation, choisissez Runtime Monitoring
3. Sous l'onglet Configuration, choisissez Modifier dans la section Configuration de la surveillance du temps d'exécution.
4. Choisissez Configurer les comptes manuellement.
5. Sélectionnez Activer automatiquement pour les nouveaux comptes membres.
6. GuardDuty Pour recevoir les événements d'exécution d'un ou de plusieurs types de ressources (une EC2 instance Amazon, un ECS cluster Amazon ou un EKS cluster Amazon), utilisez les options suivantes pour gérer l'agent de sécurité pour ces ressources :

   Pour activer l'agent GuardDuty de sécurité

   - Gestion de l'agent de sécurité automatisé pour l'EC2instance Amazon

- Gestion manuelle de l'agent de sécurité pour une EC2 instance Amazon
- Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS
- Gestion automatique de l'agent de sécurité pour les EKS clusters Amazon
- Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon

Pour les comptes de membres actifs sélectionnés uniquement

Pour activer la surveillance du temps d'exécution pour les comptes de membres actifs individuels

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sur la page Comptes, passez en revue les valeurs des colonnes Runtime Monitoring et Manage automatique de l'agent. Ces valeurs indiquent si la surveillance du temps d'exécution et la gestion des GuardDuty agents sont activées ou non pour le compte correspondant.
4. Dans le tableau Comptes, sélectionnez le compte pour lequel vous souhaitez activer la surveillance du temps d'exécution. Vous pouvez choisir plusieurs comptes à la fois.
5. Choisissez Confirmer.
6. Choisissez Modifier les plans de protection. Choisissez l'action appropriée.
7. Choisissez Confirmer.
8. GuardDuty Pour recevoir les événements d'exécution d'un ou de plusieurs types de ressources (une EC2 instance Amazon, un ECS cluster Amazon ou un EKS cluster Amazon), utilisez les options suivantes pour gérer l'agent de sécurité pour ces ressources :

   Pour activer l'agent GuardDuty de sécurité

   - Gestion de l'agent de sécurité automatisé pour l'EC2instance Amazon
   - Gestion manuelle de l'agent de sécurité pour une EC2 instance Amazon
   - Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS
   - Gestion automatique de l'agent de sécurité pour les EKS clusters Amazon
   - Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon

Gestion des agents GuardDuty de sécurité

Vous pouvez gérer l'agent GuardDuty de sécurité pour la ressource que vous souhaitez surveiller. Si vous souhaitez surveiller plusieurs types de ressources, assurez-vous de gérer l' GuardDuty agent correspondant à cette ressource.

> **Important**
>
> Lorsque vous utilisez l'agent GuardDuty de sécurité pour une EC2 instance Amazon, vous pouvez installer et utiliser l'agent sur l'hôte sous-jacent au sein d'un EKS cluster Amazon. Si vous avez déjà déployé un agent de sécurité sur ce EKS cluster, deux agents de sécurité peuvent être exécutés simultanément sur le même hôte. Pour plus d'informations sur le GuardDuty fonctionnement de ce scénario, consultezGestion des agents de sécurité doubles.

Les rubriques suivantes vous aideront à suivre les prochaines étapes de gestion de l'agent de sécurité.

Table des matières

Utilisation partagée VPC avec des agents de sécurité automatisés

Lorsque vous choisissez GuardDuty de gérer automatiquement l'agent de sécurité, Runtime Monitoring prend en charge l'utilisation d'un Comptes AWS identifiant partagé VPC appartenant à la même organisation dans AWS Organizations. En votre nom, GuardDuty vous pouvez définir la politique relative aux VPC terminaux Amazon en fonction des détails associés au partage VPC pour votre organisation.

Avant cette version, l'utilisation du partage VPCs n'était GuardDuty prise en charge que lorsque vous choisissiez de gérer l'agent GuardDuty de sécurité manuellement.

Table des matières

Comment ça marche

Lorsque le compte propriétaire du partage VPC active la surveillance du temps d'exécution et la configuration automatisée des agents pour l'une des ressources (Amazon EKS ou AWS Fargate (Amazon ECS uniquement)), toutes les ressources partagées VPCs sont éligibles à l'installation automatique du point de VPC terminaison Amazon partagé et du groupe de sécurité associé dans le compte VPC propriétaire partagé. GuardDuty récupère l'identifiant de l'organisation associé à l'Amazon VPC partagé.

Désormais, ceux Comptes AWS qui appartiennent à la même organisation que le compte VPC propriétaire Amazon partagé peuvent également partager le même point de VPC terminaison Amazon. GuardDuty crée le compte partagé VPC lorsque le compte VPC propriétaire partagé ou le compte participant a besoin d'un point de VPC terminaison Amazon. Parmi les exemples de besoin d'un point de VPC terminaison Amazon, citons l'activation GuardDuty, la surveillance du temps EKS d'exécution, la surveillance du temps d'exécution ou le lancement d'une nouvelle tâche Amazon ECS -Fargate. Lorsque ces comptes activent la surveillance du temps d'exécution et la configuration automatique des agents pour n'importe quel type de ressource, ils GuardDuty créent un point de VPC terminaison Amazon et définissent la politique du point de terminaison avec le même identifiant d'organisation que celui du compte VPC propriétaire partagé. GuardDuty ajoute une `GuardDutyManaged` balise et lui attribue la valeur `true` pour le point de VPC terminaison Amazon qui le GuardDuty crée. Si le compte VPC propriétaire Amazon partagé n'a pas activé la surveillance du temps d'exécution ou la configuration automatique des agents pour aucune des ressources, GuardDuty la politique relative aux VPC terminaux Amazon n'est pas définie. Pour plus d'informations sur la configuration de la surveillance du temps d'exécution et la gestion automatique de l'agent de sécurité dans le compte VPC propriétaire partagé, consultezActiver la surveillance du GuardDuty temps d'exécution.

Chacun des comptes utilisant la même politique de point de VPC terminaison Amazon est appelé AWS compte participant de l'Amazon partagé associéVPC.

L'exemple suivant montre la politique de point de VPC terminaison par défaut VPC du compte propriétaire partagé et du compte participant. Le `aws:PrincipalOrgID` affichera l'identifiant de

l'organisation associé à la VPC ressource partagée. L'utilisation de cette politique est limitée aux comptes de participants présents dans l'organisation du compte propriétaire.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Conditions préalables à l'utilisation du partage VPC

Conditions préalables à la configuration initiale

Effectuez les étapes suivantes dans Compte AWS le cas où vous souhaitez devenir propriétaire du partage VPC :

1. Création d'une organisation : créez une organisation en suivant les étapes décrites dans la section Création et gestion d'une organisation du Guide de AWS Organizations l'utilisateur.

   Pour plus d'informations sur l'ajout ou la suppression de comptes de membres, consultez la section Gestion Comptes AWS au sein de votre organisation.
2. Création d'une VPC ressource partagée — Vous pouvez créer une VPC ressource partagée à partir du compte du propriétaire. Pour plus d'informations, consultez la section Partager votre compte VPC avec d'autres comptes dans le guide de VPC l'utilisateur Amazon.

Prérequis spécifiques à la surveillance du temps d' GuardDutyexécution

La liste suivante fournit les prérequis spécifiques à GuardDuty :

- Le compte propriétaire du compte partagé VPC et du compte participant peuvent provenir de différentes organisations de GuardDuty. Cependant, ils doivent appartenir à la même organisation que AWS Organizations. Cela est nécessaire pour GuardDuty créer un point de VPC terminaison Amazon et un groupe de sécurité pour le partageVPC. Pour plus d'informations sur le fonctionnement du partageVPCs, consultez Partager le vôtre VPC avec d'autres comptes dans le guide de VPC l'utilisateur Amazon.
- Activez la surveillance du temps EKS d'exécution ou la surveillance du temps d'exécution, ainsi que la configuration GuardDuty automatique des agents pour toutes les ressources VPC du compte propriétaire partagé et du compte participant. Pour de plus amples informations, veuillez consulter Activer la surveillance du temps d'exécution.

  Si vous avez déjà effectué ces configurations, passez à l'étape suivante.
- Lorsque vous travaillez avec une tâche Amazon EKS ou Amazon ECS (AWS Fargate uniquement), assurez-vous de choisir la VPC ressource partagée associée au compte propriétaire et de sélectionner ses sous-réseaux.

Questions fréquemment posées (FAQs)

La liste suivante fournit les étapes de résolution des problèmes relatifs aux questions fréquemment posées lors de l'utilisation d'une VPC ressource partagée avec la configuration GuardDuty automatique des agents activée dans Runtime Monitoring :

J'utilise déjà le Runtime Monitoring (ou EKS Runtime Monitoring). Comment activer le partage VPC ?

Pour plus d'informations sur les conditions requises pour créer un partageVPC, consultezPrérequis.

Lorsque le compte VPC propriétaire partagé et le compte participant répondent aux conditions requises, il GuardDuty essaiera de définir automatiquement la politique des points de VPC terminaison Amazon.

Si, avant cette version, vous avez Compte AWS rencontré un problème de couverture lié au fait que le partage VPC n'était pas pris en charge, respectez les conditions préalables. Lorsque votre type de ressource (Amazon EKS ou tâche Amazon ECS (AWS Fargate uniquement)) invoque l'exigence d'un point de VPC terminaison partagé, il GuardDuty tente de définir la nouvelle politique de point de VPC terminaison.

En tant que compte VPC propriétaire partagé, je souhaite que la politique de point de VPC terminaison partagé soit limitée à un sous-ensemble de comptes de participants de mon organisation. Comment puis-je le faire ?

Si une `true` balise `GuardDutyManaged` : est associée au point de terminaison, supprimez-la. Cela empêche toute GuardDuty tentative de modification ou de remplacement de la politique de point de VPC terminaison du partageVPC.

Pour plus d'informations, consultez Contrôler l'accès aux points de VPC terminaison à l'aide de politiques relatives aux points de terminaison.

Pourquoi le point de VPC terminaison partagé passe-t-il de **`aws:PrincipalAccount`** à **`aws:PrincipalOrgId`** ? Comment puis-je éviter cela ?

Lorsqu'il GuardDuty détecte que le VPC est partagé par plusieurs comptes de la même organisation dans AWS Organizations, GuardDuty tente de modifier la politique pour spécifier l'ID de l'organisation.

Pour éviter cela, supprimez la `true` balise `GuardDutyManaged` : du point de VPC terminaison partagé. Cela empêche toute GuardDuty tentative de modification ou de remplacement de la politique de point de VPC terminaison du partageVPC.

Que se passe-t-il lorsque le compte VPC propriétaire partagé ou l'un des comptes participants désactive le Runtime Monitoring (GuardDuty ou EKS Runtime Monitoring) ?

Lorsque le compte VPC propriétaire partagé désactive GuardDuty la surveillance du temps d'exécution (ou la surveillance du temps EKS d'exécution), GuardDuty vérifie si un type de ressource appartenant au compte du participant a utilisé le point de VPC terminaison partagé ou si un compte participant a déjà activé la gestion des GuardDuty agents pour un type de ressource quelconque. Dans l'affirmative, le point de VPC terminaison et le groupe de sécurité GuardDuty ne seront pas supprimés.

Si le compte VPC participant partagé désactive GuardDuty la surveillance du temps d'exécution (ou la surveillance du temps EKS d'exécution), cela n'a aucun impact sur le compte VPC du propriétaire partagé et le compte propriétaire ne supprimera ni la VPC ressource partagée ni le groupe de sécurité.

Comment puis-je supprimer la VPC ressource partagée ? Quel en sera l'impact ?

En tant que compte VPC propriétaire partagé, vous pouvez supprimer la VPC ressource partagée même si elle est utilisée par votre compte ou par l'un des comptes participants à Runtime Monitoring.

Pour plus d'informations sur la suppression du partage VPC et sur la compréhension de son impact, consultezTo delete a VPC endpoint.

Gestion des agents de sécurité doubles installés sur un hôte

EC2Les instances Amazon peuvent prendre en charge plusieurs types de charges de travail. Lorsque vous configurez un agent de sécurité automatique sur une EC2 instance Amazon, la même EC2 instance peut être associée à un autre agent de sécuritéEKS.

Présentation

Imaginons un scénario dans lequel vous avez activé la surveillance du temps d'exécution. À présent, vous activez l'agent automatique pour Amazon EKS via GuardDuty. Vous avez également activé l'agent automatique pour AmazonEC2. Il peut arriver que le même hôte sous-jacent soit installé avec deux agents de sécurité, l'un pour Amazon EKS et l'autre pour AmazonEC2. Cela peut entraîner l'exécution de deux agents de sécurité sur le même hôte, collectant des événements d'exécution et les envoyant à GuardDuty, et générant potentiellement des résultats dupliqués.

Impact

- Lorsque plusieurs agents de sécurité sont exécutés sur le même hôte, votre compte peut être confronté à des besoins de traitement CPU de mémoire doublés. Pour plus d'informations sur les limites de mémoire CPU et de mémoire pour chaque type de ressource, consultez la section Prérequis relative à cette ressource.
- GuardDuty a conçu la fonctionnalité de surveillance du temps d'exécution de telle sorte que même si deux agents de sécurité collectent des événements d'exécution auprès du même hôte sous-jacent se chevauchent, votre compte ne sera débité que pour un seul flux d'événements d'exécution.

Comment GuardDuty gère plusieurs agents

GuardDuty détecte lorsque deux agents de sécurité sont exécutés sur le même hôte et désigne un seul d'entre eux comme étant l'agent de sécurité qui collecte activement les événements d'exécution. Le second agent consommera un minimum de ressources système afin d'éviter tout impact sur les performances de vos applications.

GuardDuty prend en compte les scénarios suivants :

- Lorsqu'une EC2 instance entre dans le champ de compétence d'Amazon EKS et des agents EC2 de sécurité Amazon, l'agent EKS de sécurité est prioritaire. Cela ne s'applique que lorsque vous

utilisez l'agent de sécurité v1.1.0 ou supérieur pour AmazonEC2. Les anciennes versions de l'agent continueront à s'exécuter et à collecter les événements d'exécution, car les anciennes versions de l'agent ne sont pas affectées par la hiérarchisation.

- Lorsque Amazon EKS et Amazon EC2 ont tous deux GuardDuty géré des agents de sécurité et que votre EC2 instance Amazon est également SSM gérée, les deux agents de sécurité sont installés au niveau de l'hôte. Une fois les agents installés, GuardDuty décide quel agent de sécurité continuera de fonctionner. Lorsque les deux agents de sécurité sont en cours d'exécution, un seul d'entre eux finira par collecter les événements d'exécution.
- Lorsque les agents de sécurité associés aux deux EC2 et EKS exécutés simultanément GuardDuty peuvent générer des résultats dupliqués uniquement pendant la période de chevauchement.

  Cela peut se produire lorsque :

  - des agents de sécurité pour les deux EC2 et EKS configurés via GuardDuty (automatiquement), ou
  - Votre EKS ressource Amazon dispose d'un agent de sécurité automatisé.
- Lorsque l'agent EKS de sécurité est déjà en cours d'exécution, si vous le déployez manuellement sur le EC2 même hôte sous-jacent et que vous répondez à toutes les conditions requises, il est GuardDuty possible que vous n'installiez pas un deuxième agent de sécurité.

Gestion de l'agent de sécurité automatisé pour l'EC2instance Amazon

> **Note**
>
> Avant de continuer, assurez-vous de suivre toutes lesConditions requises pour le support des EC2 instances Amazon.

Migration d'un agent EC2 manuel Amazon vers un agent automatisé

Cette section s'applique à vous Compte AWS si vous gériez auparavant l'agent de sécurité manuellement et que vous souhaitez maintenant utiliser la configuration GuardDuty automatique de l'agent. Si cela ne vous concerne pas, poursuivez la configuration de l'agent de sécurité pour votre compte.

Lorsque vous activez l'agent GuardDuty automatique, GuardDuty gère l'agent de sécurité en votre nom. Pour plus d'informations sur les étapes GuardDuty à suivre, consultezUtiliser la configuration automatique des agents (recommandé).

Nettoyage des ressources

Supprimer SSM l'association

- Supprimez toute SSM association que vous avez peut-être créée lorsque vous gériez EC2 manuellement l'agent de sécurité pour Amazon. Pour plus d'informations, consultez la section Suppression d'associations.
- Cela GuardDuty permet de prendre en charge la gestion des SSM actions, que vous utilisiez des agents automatisés au niveau du compte ou au niveau de l'instance (en utilisant des balises d'inclusion ou d'exclusion). Pour plus d'informations sur SSM les actions qui peuvent être entreprises, GuardDuty consultezAutorisations de rôle liées à un service pour GuardDuty.
- Lorsque vous supprimez une SSM association précédemment créée pour gérer manuellement l'agent de sécurité, il peut y avoir une brève période de chevauchement lors de la GuardDuty création d'une SSM association pour gérer automatiquement l'agent de sécurité. Au cours de cette période, vous pourriez rencontrer des conflits liés à la SSM planification. Pour plus d'informations, consultez Amazon EC2 SSM Scheduling.

Gérez les balises d'inclusion et d'exclusion pour vos EC2 instances Amazon

- Balises d'inclusion — Lorsque vous n'activez pas la configuration GuardDuty automatique des agents mais que vous balisez l'une de vos EC2 instances Amazon avec une balise d'inclusion (`GuardDutyManaged:true`), vous GuardDuty créez une SSM association qui installera et gérera l'agent de sécurité sur les EC2 instances sélectionnées. Il s'agit d'un comportement attendu qui vous permet de gérer l'agent de sécurité uniquement sur certaines EC2 instances. Pour de plus amples informations, veuillez consulter Comment fonctionne Runtime Monitoring avec les EC2 instances Amazon.

  Pour GuardDuty empêcher l'installation et la gestion de l'agent de sécurité, supprimez la balise d'inclusion de ces EC2 instances. Pour plus d'informations, consultez la section Ajouter et supprimer des balises dans le guide de EC2 l'utilisateur Amazon.
- Balises d'exclusion : lorsque vous souhaitez activer la configuration GuardDuty automatique des agents pour toutes les EC2 instances de votre compte, assurez-vous qu'aucune EC2 instance n'est associée à une balise d'exclusion (`GuardDutyManaged:false`).

Configuration de GuardDuty l'agent pour un compte autonome

Configure for all instances

Pour configurer la surveillance du temps d'exécution pour toutes les instances de votre compte autonome

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Dans l'onglet Configuration, choisissez Modifier.
4. Dans la EC2section, choisissez Activer.
5. Choisissez Save (Enregistrer).
6. Vous pouvez vérifier que l'SSMassociation GuardDuty créée installera et gérera l'agent de sécurité sur toutes les EC2 ressources appartenant à votre compte.

   a. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

   b. Ouvrez l'onglet Cibles de l'SSMassociation (`GuardDutyRuntimeMonitoring-do-not-delete`). Notez que la touche Tag apparaît sous la forme InstanceIds.

Using inclusion tag in selected instances

Pour configurer l'agent GuardDuty de sécurité pour certaines EC2 instances Amazon

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `true` balise `GuardDutyManaged` : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.
3. Vous pouvez vérifier que l'SSMassociation GuardDuty créée installera et gérera l'agent de sécurité uniquement sur les EC2 ressources étiquetées avec les balises d'inclusion.

   Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

- Ouvrez l'onglet Cibles pour l'SSMassociation créée (`GuardDutyRuntimeMonitoring-do-not-delete`). La touche Tag apparaît sous la forme de tag : GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assurez-vous d'ajouter la balise d'exclusion à vos EC2 instances Amazon avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour AmazonEC2, toute EC2 instance lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour certaines EC2 instances Amazon

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `false` balise `GuardDutyManaged` : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.
3. Pour que les balises d'exclusion soient disponibles dans les métadonnées de l'instance, effectuez les opérations suivantes :

   a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

      S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.

   b. Sélectionnez l'instance pour laquelle vous souhaitez autoriser les balises.

   c. Dans le menu Actions, sélectionnez Paramètres de l'instance.

   d. Choisissez Autoriser les balises dans les métadonnées de l'instance.

   e. Sous Accès aux balises dans les métadonnées de l'instance, sélectionnez Autoriser.

   f. Choisissez Save (Enregistrer).
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécutionCouverture pour l'EC2instance Amazon.

Configuration de GuardDuty l'agent dans un environnement à comptes multiples

Pour le compte GuardDuty d'administrateur délégué

Configure for all instances

Si vous avez choisi Activer pour tous les comptes pour la surveillance du temps d'exécution, choisissez l'une des options suivantes pour le compte d' GuardDuty administrateur délégué :

- Option 1

  Sous Configuration automatique de l'agent, dans la EC2section, sélectionnez Activer pour tous les comptes.
- Option 2
  - Sous Configuration automatique de l'agent, dans la EC2section, sélectionnez Configurer les comptes manuellement.
  - Sous Administrateur délégué (ce compte), choisissez Activer.
- Choisissez Save (Enregistrer).

Si vous avez choisi Configurer les comptes manuellement pour la surveillance du temps d'exécution, effectuez les étapes suivantes :

- Sous Configuration automatique de l'agent, dans la EC2section, sélectionnez Configurer les comptes manuellement.
- Sous Administrateur délégué (ce compte), choisissez Activer.
- Choisissez Save (Enregistrer).

Quelle que soit l'option que vous choisissez pour activer la configuration automatique de l'agent pour le compte d' GuardDuty administrateur délégué, vous pouvez vérifier que l'SSMassociation GuardDuty créée installera et gérera l'agent de sécurité sur toutes les EC2 ressources appartenant à ce compte.

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

2. Ouvrez l'onglet Cibles de l'SSMassociation (`GuardDutyRuntimeMonitoring-do-not-delete`). Notez que la touche Tag apparaît sous la forme InstanceIds.

Using inclusion tag in selected instances

Pour configurer GuardDuty l'agent pour certaines EC2 instances Amazon

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `true` balise `GuardDutyManaged` : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.

   L'ajout de cette balise permettra GuardDuty d'installer et de gérer l'agent de sécurité pour ces EC2 instances sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.
3. Vous pouvez vérifier que l'SSMassociation GuardDuty créée installera et gérera l'agent de sécurité uniquement sur les EC2 ressources étiquetées avec les balises d'inclusion.

   Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

   - Ouvrez l'onglet Cibles pour l'SSMassociation créée (`GuardDutyRuntimeMonitoring-do-not-delete`). La touche Tag apparaît sous la forme de tag : GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assurez-vous d'ajouter la balise d'exclusion à vos EC2 instances Amazon avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour AmazonEC2, toute EC2 instance lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer GuardDuty l'agent pour certaines EC2 instances Amazon

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `false` balise `GuardDutyManaged` : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.
3. Pour que les balises d'exclusion soient disponibles dans les métadonnées de l'instance, effectuez les opérations suivantes :

   a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

      S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.

   b. Dans le menu Actions, sélectionnez Paramètres de l'instance.

   c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécutionCouverture pour l'EC2instance Amazon.

Activation automatique pour tous les comptes membres

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Configure for all instances

Les étapes suivantes supposent que vous avez choisi Activer pour tous les comptes dans la section Runtime Monitoring :

1. Choisissez Activer pour tous les comptes dans la section Configuration automatique des agents pour Amazon EC2.

2. Vous pouvez vérifier que l'SSMassociation qui GuardDuty crée (`GuardDutyRuntimeMonitoring-do-not-delete`) installera et gérera l'agent de sécurité sur toutes les EC2 ressources appartenant à ce compte.

   a. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

   b. Ouvrez l'onglet Cibles de l'SSMassociation. Notez que la touche Tag apparaît sous la forme InstanceIds.

Using inclusion tag in selected instances

Pour configurer GuardDuty l'agent pour certaines EC2 instances Amazon

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `true` balise `GuardDutyManaged` : aux EC2 instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.

   L'ajout de cette balise permettra GuardDuty d'installer et de gérer l'agent de sécurité pour ces EC2 instances sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.
3. Vous pouvez vérifier que l'SSMassociation GuardDuty créée installera et gérera l'agent de sécurité sur toutes les EC2 ressources appartenant à votre compte.

   a. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

   b. Ouvrez l'onglet Cibles de l'SSMassociation (`GuardDutyRuntimeMonitoring-do-not-delete`). Notez que la touche Tag apparaît sous la forme InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Assurez-vous d'ajouter la balise d'exclusion à vos EC2 instances Amazon avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour

AmazonEC2, toute EC2 instance lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour certaines EC2 instances Amazon

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `false` balise `GuardDutyManaged` : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.
3. Pour que les balises d'exclusion soient disponibles dans les métadonnées de l'instance, effectuez les opérations suivantes :

   a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

      S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.

   b. Dans le menu Actions, sélectionnez Paramètres de l'instance.

   c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécutionCouverture pour l'EC2instance Amazon.

Activation automatique pour les nouveaux comptes de membres uniquement

Le compte d' GuardDuty administrateur délégué peut définir la configuration automatique de l'agent pour la EC2 ressource Amazon afin qu'elle soit automatiquement activée pour les nouveaux comptes membres lorsqu'ils rejoignent l'organisation.

Configure for all instances

Les étapes suivantes supposent que vous avez sélectionné Activer automatiquement les nouveaux comptes membres dans la section Runtime Monitoring :

1. Dans le volet de navigation, choisissez Runtime Monitoring.

2. Sur la page Runtime Monitoring, choisissez Modifier.
3. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la configuration automatique des agents pour Amazon EC2 sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette sélection.
4. Choisissez Save (Enregistrer).

Lorsqu'un nouveau compte membre rejoint l'organisation, cette configuration est automatiquement activée pour lui. GuardDuty Pour gérer l'agent de sécurité pour les EC2 instances Amazon appartenant à ce nouveau compte membre, assurez-vous que toutes les conditions préalables Par EC2 exemple sont remplies.

Lorsqu'une SSM association est créée (`GuardDutyRuntimeMonitoring-do-not-delete`), vous pouvez vérifier qu'elle installera et gérera l'agent de sécurité sur toutes les EC2 instances appartenant au nouveau compte membre. SSM

- Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
- Ouvrez l'onglet Cibles de l'SSMassociation. Notez que la touche Tag apparaît sous la forme InstanceIds.

Using inclusion tag in selected instances

Pour configurer l'agent GuardDuty de sécurité pour les instances sélectionnées de votre compte

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `true` balise `GuardDutyManaged` : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.

   L'ajout de cette balise permettra GuardDuty d'installer et de gérer l'agent de sécurité pour ces instances sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.
3. Vous pouvez vérifier que l'SSMassociation GuardDuty créée installera et gérera l'agent de sécurité uniquement sur les EC2 ressources étiquetées avec les balises d'inclusion.

a. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.

b. Ouvrez l'onglet Cibles pour l'SSMassociation créée. La touche Tag apparaît sous la forme de tag : GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assurez-vous d'ajouter la balise d'exclusion à vos EC2 instances Amazon avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour AmazonEC2, toute EC2 instance lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour des instances spécifiques de votre compte autonome

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `false` balise `GuardDutyManaged` : aux instances que vous ne souhaitez pas GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.
3. Pour que les balises d'exclusion soient disponibles dans les métadonnées de l'instance, effectuez les opérations suivantes :

   a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

      S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.

   b. Dans le menu Actions, sélectionnez Paramètres de l'instance.

   c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez désormais évaluer le temps d'exécutionCouverture pour l'EC2instance Amazon.

Comptes de membres sélectifs uniquement

Configure for all instances

1. Sur la page Comptes, sélectionnez un ou plusieurs comptes pour lesquels vous souhaitez activer la configuration automatisée de l'agent Runtime Monitoring (Amazon). EC2 Assurez-vous que la surveillance du temps d'exécution est déjà activée sur les comptes que vous sélectionnez au cours de cette étape.
2. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration automatisée de l'agent Runtime Monitoring-Automated (Amazon). EC2
3. Choisissez Confirmer.

Using inclusion tag in selected instances

Pour configurer l'agent GuardDuty de sécurité pour les instances sélectionnées

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `true` balise `GuardDutyManaged` : aux instances que vous souhaitez GuardDuty surveiller et détecter les menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.

   L'ajout de cette balise permettra GuardDuty de gérer l'agent de sécurité pour vos EC2 instances Amazon étiquetées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents (Runtime Monitoring - Automated agent configuration (EC2).

Using exclusion tag in selected instances

> **Note**
>
> Assurez-vous d'ajouter la balise d'exclusion à vos EC2 instances Amazon avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour AmazonEC2, toute EC2 instance lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer l'agent GuardDuty de sécurité pour les instances sélectionnées

1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `false` balise `GuardDutyManaged` : aux EC2 instances que vous ne souhaitez pas GuardDuty surveiller ou détecter de menaces potentielles. Pour plus d'informations sur l'ajout de cette balise, voir Pour ajouter une balise à une ressource individuelle.
3. Pour que les balises d'exclusion soient disponibles dans les métadonnées de l'instance, effectuez les opérations suivantes :

   a. Dans l'onglet Détails de votre instance, consultez l'état de l'option Autoriser les balises dans les métadonnées de l'instance.

      S'il est actuellement désactivé, suivez les étapes ci-dessous pour changer le statut en Activé. Sinon, Ignorez cette étape.

   b. Dans le menu Actions, sélectionnez Paramètres de l'instance.

   c. Choisissez Autoriser les balises dans les métadonnées de l'instance.
4. Après avoir ajouté la balise d'exclusion, effectuez les mêmes étapes que celles spécifiées dans l'onglet Configurer pour toutes les instances.

Vous pouvez maintenant évaluerCouverture pour l'EC2instance Amazon.

Gestion manuelle de l'agent de sécurité pour une EC2 instance Amazon

Après avoir activé la surveillance du temps d'exécution, vous devez installer l'agent GuardDuty de sécurité manuellement. En installant l'agent, GuardDuty il recevra les événements d'exécution des EC2 instances Amazon.

Pour gérer l'agent GuardDuty de sécurité, vous devez créer un point de VPC terminaison Amazon, puis suivre les étapes pour installer l'agent de sécurité manuellement.

Création manuelle d'un point de VPC terminaison Amazon

Avant de pouvoir installer l'agent GuardDuty de sécurité, vous devez créer un point de terminaison Amazon Virtual Private Cloud (AmazonVPC). Cela vous aidera à GuardDuty recevoir les événements d'exécution de vos EC2 instances Amazon.

> **Note**
>
> Il n'y a aucun coût supplémentaire pour l'utilisation du VPC terminal.

Pour créer un point de VPC terminaison Amazon

1. Connectez-vous à la VPC console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous cloud VPC privé, sélectionnez Endpoints.
3. Choisissez Créer un point de terminaison.
4. Sur la page Créer un point de terminaison, pour Catégorie de services, choisissez Autres services de points de terminaison.
5. Pour Nom du service, entrez **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Assurez-vous de remplacer *`us-east-1`* avec votre Région AWS. Il doit s'agir de la même région que l'EC2instance Amazon associée à votre identifiant de AWS compte.
6. Choisissez Vérifier le service.
7. Une fois le nom du service vérifié avec succès, choisissez l'VPCemplacement de votre instance. Ajoutez la politique suivante pour limiter l'utilisation des VPC terminaux Amazon au compte spécifié uniquement. Avec l'organisation `Condition` indiquée sous cette stratégie, vous pouvez mettre à jour la stratégie suivante pour restreindre l'accès à votre point de terminaison. Pour fournir le support Amazon VPC Endpoint à un compte IDs spécifique de votre organisation, consultezOrganization condition to restrict access to your endpoint.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
```

```
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

L'identifiant du `aws:PrincipalAccount` compte doit correspondre au compte contenant le point de VPC terminaison VPC et. La liste suivante indique comment partager le VPC point de terminaison avec un autre AWS compte IDs :

- Pour spécifier plusieurs comptes pour accéder au VPC point de terminaison, `"aws:PrincipalAccount: "`*`111122223333`*`"` remplacez-le par le bloc suivant :

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
        ]
  ```

  Assurez-vous de remplacer le AWS compte par le compte IDs IDs des comptes qui ont besoin d'accéder au VPC point de terminaison.
- Pour autoriser tous les membres d'une organisation à accéder au VPC point de terminaison, remplacez-le `"aws:PrincipalAccount: "`*`111122223333`*`"` par la ligne suivante :

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

  Assurez-vous de remplacer l'organisation *`o-abcdef0123`* avec l'identifiant de votre organisation.
- Pour restreindre l'accès à une ressource par un identifiant d'organisation, ajoutez votre `ResourceOrgID` nom à la politique. Pour plus d'informations, consultez `aws:ResourceOrgID`le guide de IAM l'utilisateur.

  ```
  "aws:ResourceOrgID": "o-abcdef0123"
  ```

8. Sous Paramètres supplémentaires, choisissez Activer DNS le nom.
9. Sous Sous-réseaux, choisissez les sous-réseaux dans lesquels réside votre instance.

10. Sous Groupes de sécurité, choisissez un groupe de sécurité dont le port entrant 443 est activé depuis votre VPC (ou votre EC2 instance Amazon). Si vous ne possédez pas encore de groupe de sécurité dont le port entrant 443 est activé, consultez la section Créer un groupe de sécurité dans le guide de l'EC2utilisateur Amazon.

    En cas de problème lors de la restriction des autorisations entrantes à votre VPC (ou instance), fournissez le support au port 443 entrant depuis n'importe quelle adresse IP. `(0.0.0.0/0)`

Installation manuelle de l'agent de sécurité

GuardDuty propose les deux méthodes suivantes pour installer l'agent GuardDuty de sécurité sur vos EC2 instances Amazon :

- Méthode 1 - En utilisant AWS Systems Manager — Cette méthode nécessite que votre EC2 instance Amazon soit AWS Systems Manager gérée.
- Méthode 2 - En utilisant les gestionnaires de packages Linux — Vous pouvez utiliser cette méthode, que vos EC2 instances Amazon soient AWS Systems Manager gérées ou non.

Méthode 1 - En utilisant AWS Systems Manager

Pour utiliser cette méthode, assurez-vous que vos EC2 instances Amazon sont AWS Systems Manager gérées, puis installez l'agent.

AWS Systems Manager EC2instance Amazon gérée

Suivez les étapes ci-dessous pour AWS Systems Manager gérer vos EC2 instances Amazon.

- AWS Systems Managervous aide à gérer vos AWS applications et vos ressources end-to-end et à garantir des opérations sécurisées à grande échelle.

  Pour gérer vos EC2 instances Amazon avec AWS Systems Manager, consultez la section Configuration de Systems Manager pour les EC2 instances Amazon dans le Guide de AWS Systems Manager l'utilisateur.
- Le tableau suivant présente les nouveaux AWS Systems Manager documents GuardDuty gérés :

Nom du document	Type de document	Objectif
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Pour empaqueter l'agent GuardDuty de sécurité.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Command	Pour exécuter un script d'installation/désinstallation afin d'installer l' GuardDuty agent de sécurité.

Pour plus d'informations AWS Systems Manager, consultez les documents Amazon EC2 Systems Manager dans le guide de AWS Systems Manager l'utilisateur.

> **Pour les serveurs Debian**
>
> Les Amazon Machine Images (AMIs) pour le serveur Debian fournies par AWS nécessitent que vous installiez l' AWS Systems Manager agent (SSMagent). Vous devrez effectuer une étape supplémentaire pour installer l'SSMagent afin de SSM gérer vos instances du serveur Amazon EC2 Debian. Pour plus d'informations sur les étapes à suivre, consultez la section Installation manuelle de l'SSMagent sur les instances du serveur Debian dans le guide de AWS Systems Manager l'utilisateur.

Pour installer l' GuardDuty agent pour l'EC2instance Amazon en utilisant AWS Systems Manager

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le volet de navigation, sélectionnez Documents
3. Dans Owned by Amazon, sélectionnez`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Choisissez Run Command (Exécuter une commande).
5. Entrez les paramètres Run Command suivants

   - Action : Choisissez Installer.

- Type d'installation : Choisissez Installer ou Désinstaller.
- Nom : `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
- Version : si ce champ reste vide, vous obtiendrez la dernière version de l'agent de GuardDuty sécurité. Pour plus d'informations sur les versions publiées,GuardDuty agent de sécurité pour les EC2 instances Amazon.

6. Sélectionnez l'EC2instance Amazon ciblée. Vous pouvez sélectionner une ou plusieurs EC2 instances Amazon. Pour plus d'informations, voir AWS Systems Manager Exécution de commandes depuis la console dans le Guide de AWS Systems Manager l'utilisateur
7. Vérifiez si l'installation de l' GuardDuty agent est saine. Pour de plus amples informations, veuillez consulter Validation de l'état d'installation GuardDuty de l'agent de sécurité.

Méthode 2 - En utilisant les gestionnaires de packages Linux

Avec cette méthode, vous pouvez installer l'agent GuardDuty de sécurité en exécutant RPM des scripts ou des scripts Debian. En fonction des systèmes d'exploitation, vous pouvez choisir une méthode préférée :

- Utilisez RPM des scripts pour installer l'agent de sécurité sur les distributions du système d'exploitation AL2 ou sur les distributions AL2 023.
- Utilisez des scripts Debian pour installer l'agent de sécurité sur les distributions du système d'exploitation Ubuntu ou Debian. Pour plus d'informations sur les distributions de systèmes d'exploitation Ubuntu et Debian prises en charge, consultezValidation des exigences architecturales.

RPM installation

> **Important**
>
> Nous vous recommandons de vérifier la RPM signature GuardDuty de l'agent de sécurité avant de l'installer sur votre machine.

1. Vérifiez la RPM signature de l'agent de GuardDuty sécurité

a. Préparez le modèle

Préparez les commandes avec la clé publique appropriée, la signature de x86_64RPM, la signature d'arm64 RPM et le lien d'accès correspondant aux RPM scripts hébergés dans les compartiments Amazon S3. Remplacez la valeur du Région AWS, l'ID de AWS compte et la version de l' GuardDuty agent pour accéder aux RPM scripts.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
publickey.pem
```

- GuardDuty RPMsignature de l'agent de sécurité :

  Signature de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/
amazon-guardduty-agent-1.3.0.x86_64.sig
```

  Signature d'arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.sig
```

- Liens d'accès aux RPM scripts du compartiment Amazon S3 :

  Lien d'accès pour x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/
amazon-guardduty-agent-1.3.0.x86_64.rpm
```

  Lien d'accès pour arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.rpm
```

Région AWS	Nom de la région	AWS ID de compte
eu-west-1	Europe (Irlande)	694911143906

us-east-1	USA Est (Virginie du Nord)	593207742271
us-west-2	USA Ouest (Oregon)	733349766148
eu-west-3	Europe (Paris)	665651866788
us-east-2	USA Est (Ohio)	307168627858
eu-central-1	Europe (Francfort)	323658145986
ap-northeast-2	Asie-Pacifique (Séoul)	914738172881
eu-north-1	Europe (Stockholm)	591436053604
ap-east-1	Asie-Pacifique (Hong Kong)	258348409381
me-south-1	Moyen-Orient (Bahreïn)	536382113932
eu-west-2	Europe (Londres)	892757235363
ap-northeast-1	Asie-Pacifique (Tokyo)	533107202818
ap-southeast-1	Asie-Pacifique (Singapour)	174946120834
ap-south-1	Asie-Pacifique (Mumbai)	251508486986
ap-southeast-3	Asie-Pacifique (Jakarta)	510637619217
sa-east-1	Amérique du Sud (São Paulo)	758426053663
ap-northeast-3	Asie-Pacifique (Osaka)	273192626886
eu-south-1	Europe (Milan)	266869475730
af-south-1	Afrique (Le Cap)	197869348890
ap-southeast-2	Asie-Pacifique (Sydney)	005257825471

me-central-1	Moyen-Orient (UAE)	000014521398
us-west-1	USA Ouest (Californie du Nord)	684579721401
ca-central-1	Canada (Centre)	354763396469
ca-west-1	Canada Ouest (Calgary)	339712888787
ap-south-2	Asie-Pacifique (Hyderabad)	950823858135
eu-south-2	Europe (Espagne)	919611009337
eu-central-2	Europe (Zurich)	529164026651
ap-southeast-4	Asie-Pacifique (Melbourne)	251357961535
il-central-1	Israël (Tel Aviv)	870907303882

b. Téléchargez le modèle

Dans la commande suivante, pour télécharger la clé publique appropriée, la signature de x86_64RPM, la signature d'arm64 RPM et le lien d'accès correspondant aux RPM scripts hébergés dans les compartiments Amazon S3, assurez-vous de remplacer l'ID de compte par l' Compte AWS ID approprié et la région par votre région actuelle.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm ./amazon-guardduty-
agent-1.3.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig ./amazon-guardduty-
agent-1.3.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
publickey.pem ./publickey.pem
```

c. Importer la clé publique

Utilisez la commande suivante pour importer la clé publique dans la base de données :

```
gpg --import publickey.pem
```

gpg affiche l'importation avec succès

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Vérifiez la signature

Utilisez la commande suivante pour vérifier la signature

```
gpg --verify amazon-guardduty-agent-1.3.0.x86_64.sig amazon-guardduty-
agent-1.3.0.x86_64.rpm
```

Si la vérification est réussie, vous verrez un message similaire au résultat ci-dessous. Vous pouvez maintenant procéder à l'installation de l'agent de GuardDuty sécurité à l'aide deRPM.

Exemple de sortie :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Si la vérification échoue, cela signifie que la signature RPM a été potentiellement falsifiée. Vous devez supprimer la clé publique de la base de données et recommencer le processus de vérification.

Exemple :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Utilisez la commande suivante pour supprimer la clé publique de la base de données :

```
gpg --delete-keys AwsGuardDuty
```

Maintenant, réessayez le processus de vérification.

2. Connectez-vous SSH depuis Linux ou macOS.
3. Installez l'agent GuardDuty de sécurité à l'aide de la commande suivante :

```
sudo rpm -ivh amazon-guardduty-agent-1.3.0.x86_64.rpm
```

4. Vérifiez si l'installation de l' GuardDuty agent est saine. Pour plus d'informations sur les étapes, consultezValidation de l'état d'installation GuardDuty de l'agent de sécurité.

Debian installation

> **Important**
>
> Nous recommandons de vérifier la signature GuardDuty de l'agent de sécurité Debian avant de l'installer sur votre machine.

1. Vérifier la signature GuardDuty de l'agent de sécurité Debian

   a. Préparez des modèles pour la clé publique appropriée, la signature du paquet Debian amd64, la signature du paquet Debian arm64 et le lien d'accès correspondant aux scripts Debian hébergés dans les compartiments Amazon S3

   Dans les modèles suivants, remplacez la valeur du Région AWS, de l'ID de AWS compte et de la version de l' GuardDuty agent pour accéder aux scripts des paquets Debian.

   - Clé publique :

   ```
   s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
   publickey.pem
   ```

   - GuardDuty Signature de l'agent de sécurité Debian :

Signature d'amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/
amazon-guardduty-agent-1.3.0.amd64.sig
```

Signature d'arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.sig
```

- Liens d'accès aux scripts Debian dans le compartiment Amazon S3 :

  Lien d'accès pour amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/
amazon-guardduty-agent-1.3.0.amd64.deb
```

  Lien d'accès pour arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.deb
```

Région AWS	Nom de la région	AWS ID de compte
eu-west-1	Europe (Irlande)	694911143906
us-east-1	USA Est (Virginie du Nord)	593207742271
us-west-2	USA Ouest (Oregon)	733349766148
eu-west-3	Europe (Paris)	665651866788
us-east-2	USA Est (Ohio)	307168627858
eu-central-1	Europe (Francfort)	323658145986
ap-northeast-2	Asie-Pacifique (Séoul)	914738172881

eu-north-1	Europe (Stockholm)	591436053604
ap-east-1	Asie-Pacifique (Hong Kong)	258348409381
me-south-1	Moyen-Orient (Bahreïn)	536382113932
eu-west-2	Europe (Londres)	892757235363
ap-northeast-1	Asie-Pacifique (Tokyo)	533107202818
ap-southeast-1	Asie-Pacifique (Singapour)	174946120834
ap-south-1	Asie-Pacifique (Mumbai)	251508486986
ap-southeast-3	Asie-Pacifique (Jakarta)	510637619217
sa-east-1	Amérique du Sud (São Paulo)	758426053663
ap-northeast-3	Asie-Pacifique (Osaka)	273192626886
eu-south-1	Europe (Milan)	266869475730
af-south-1	Afrique (Le Cap)	197869348890
ap-southeast-2	Asie-Pacifique (Sydney)	005257825471
me-central-1	Moyen-Orient (UAE)	000014521398
us-west-1	USA Ouest (Californie du Nord)	684579721401
ca-central-1	Canada (Centre)	354763396469
ca-west-1	Canada Ouest (Calgary)	339712888787
ap-south-2	Asie-Pacifique (Hyderabad)	950823858135

eu-south-2	Europe (Espagne)	919611009337
eu-central-2	Europe (Zurich)	529164026651
ap-southeast-4	Asie-Pacifique (Melbourne)	251357961535
il-central-1	Israël (Tel Aviv)	870907303882

b. Téléchargez la clé publique appropriée pour télécharger, la signature d'amd64, la signature d'arm64 et le lien d'accès correspondant aux scripts Debian hébergés dans des compartiments Amazon S3

Dans les commandes suivantes, remplacez l'identifiant du compte par l' Compte AWS identifiant approprié, et la région par votre région actuelle.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.deb ./amazon-guardduty-
agent-1.3.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.sig ./amazon-guardduty-
agent-1.3.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
publickey.pem ./publickey.pem
```

c. Importer la clé publique dans la base de données

```
gpg --import publickey.pem
```

gpg affiche l'importation avec succès

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Vérifiez la signature

```
gpg --verify amazon-guardduty-agent-1.3.0.amd64.sig amazon-guardduty-
agent-1.3.0.amd64.deb
```

Après une vérification réussie, vous verrez un message similaire au résultat suivant :

Exemple de sortie :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Vous pouvez maintenant procéder à l'installation de l'agent GuardDuty de sécurité à l'aide de Debian.

Cependant, si la vérification échoue, cela signifie que la signature du paquet Debian a été potentiellement falsifiée.

Exemple :

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Utilisez la commande suivante pour supprimer la clé publique de la base de données :

```
gpg --delete-keys AwsGuardDuty
```

Maintenant, réessayez le processus de vérification.

2. Connectez-vous SSH depuis Linux ou macOS.
3. Installez l'agent GuardDuty de sécurité à l'aide de la commande suivante :

   ```
   sudo dpkg -i amazon-guardduty-agent-1.3.0.amd64.deb
   ```

4. Vérifiez si l'installation de l' GuardDuty agent est saine. Pour plus d'informations sur les étapes, consultezValidation de l'état d'installation GuardDuty de l'agent de sécurité.

Erreur de mémoire insuffisante

Si vous rencontrez une `out-of-memory` erreur lors de l'installation ou de la mise à jour EC2 manuelle GuardDuty de l'agent de sécurité pour Amazon, consultezRésolution d'une erreur de mémoire insuffisante.

Validation de l'état d'installation GuardDuty de l'agent de sécurité

Pour vérifier si l'agent GuardDuty de sécurité est sain

1. Connectez-vous SSH depuis Linux ou macOS.
2. Exécutez la commande suivante pour vérifier l'état de l'agent GuardDuty de sécurité :

```
sudo systemctl status amazon-guardduty-agent
```

Si vous souhaitez consulter les journaux d'installation de l'agent de sécurité, ils sont disponibles sous`/var/log/amzn-guardduty-agent/`.

Pour consulter les journaux, faites`sudo journalctl -u amazon-guardduty-agent`.

Mise à jour manuelle GuardDuty de l'agent de sécurité

Vous pouvez mettre à jour l'agent GuardDuty de sécurité à l'aide de la commande Exécuter. Vous pouvez suivre les mêmes étapes que celles que vous avez utilisées pour installer l'agent GuardDuty de sécurité.

Désinstallation manuelle de l'agent de sécurité

Cette section fournit des méthodes pour désinstaller l'agent de GuardDuty sécurité de vos EC2 ressources Amazon. Si vous envisagez également de désactiver la surveillance du temps d'exécution, consultezImpact de la désactivation.

Méthode 1 - À l'aide de la commande Exécuter

Pour désinstaller l'agent de GuardDuty sécurité à l'aide de la commande Exécuter

1. Vous pouvez désinstaller l'agent GuardDuty de sécurité en suivant les étapes indiquées dans la section AWS Systems Manager Exécuter la commande du Guide de l'AWS Systems Manager utilisateur. Utilisez l'action Désinstaller dans les paramètres pour désinstaller l'agent GuardDuty de sécurité.

   Dans la section Cibles, assurez-vous que l'impact ne concerne que les EC2 instances Amazon dont vous souhaitez désinstaller l'agent de sécurité.

   Utilisez le GuardDuty document et le distributeur suivants :

   - Nom du document : `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`

- Distributeur : `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. Après avoir fourni tous les détails, lorsque vous choisissez Exécuter, l'agent de sécurité déployé sur les EC2 instances Amazon ciblées est supprimé.

   Pour supprimer la configuration du point de VPC terminaison Amazon, vous devez désactiver à la fois le Runtime Monitoring et Amazon EKS Runtime Monitoring.

Méthode 2 - En utilisant les gestionnaires de packages Linux

1. Connectez-vous SSH depuis Linux ou macOS.
2. Commande de désinstallation

   La commande suivante permet de désinstaller l'agent de GuardDuty sécurité de l'EC2instance Amazon à laquelle vous vous connectez :

   - Pour RPM :

     ```
     sudo rpm -e amazon-guardduty-agent
     ```

   - Pour Debian :

     ```
     sudo dpkg --purge amazon-guardduty-agent
     ```

   Après avoir exécuté la commande, vous pouvez également consulter les journaux associés à la commande.

Supprimer le point de VPC terminaison Amazon

Lorsque vous souhaitez désactiver la surveillance du temps d'exécution ou désinstaller l'agent de GuardDuty sécurité de votre compte, vous pouvez également choisir de supprimer le point de VPC terminaison Amazon créé manuellement (Création manuelle d'un point de VPC terminaison Amazon).

Pour supprimer le point de VPC terminaison Amazon à l'aide de la console

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Points de terminaison.

3. Sélectionnez le point de terminaison créé manuellement au moment de l'activation de Runtime Monitoring.
4. Choisissez Actions, Supprimer les VPC points de terminaison.
5. À l'invite de confirmation, saisissez **`delete`**.
6. Sélectionnez Delete (Supprimer).

Pour supprimer le point de VPC terminaison Amazon en utilisant AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- Remove-EC2VpcEndpointCmdlet (Outils pour Windows) PowerShell

Gestion de l'agent de sécurité automatisé pour Fargate (Amazon uniquement) ECS

Runtime Monitoring prend en charge la gestion de l'agent de sécurité pour vos ECS clusters Amazon (AWS Fargate) uniquement via GuardDuty. La gestion manuelle de l'agent de sécurité sur les ECS clusters Amazon n'est pas prise en charge.

GuardDutyPour activer la gestion de l'agent de sécurité pour vos ressources ECS -Fargate, suivez les étapes décrites dans les sections suivantes.

Table des matières

Configuration de GuardDuty l'agent pour un compte autonome

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Sous l'onglet Configuration :

a. Pour gérer la configuration automatisée des agents pour tous les ECS clusters Amazon (au niveau du compte)

   Choisissez Activer dans la section Configuration automatique de l'agent pour AWS Fargate (ECSuniquement). Lorsqu'une nouvelle tâche Fargate est GuardDuty lancée, ECS Amazon gère le déploiement de l'agent de sécurité.

   - Choisissez Save (Enregistrer).

b. Pour gérer la configuration automatisée des agents en excluant certains ECS clusters Amazon (au niveau du cluster)

   i. Ajoutez une balise au ECS cluster Amazon dont vous souhaitez exclure toutes les tâches. La paire clé-valeur doit être `GuardDutyManaged` -. `false`

   ii. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
```

```
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
```

```
                }
            }
        }
    ]
}
```

iii. Sous l'onglet Configuration, choisissez Activer dans la section Configuration automatique de l'agent.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à votre ECS cluster Amazon avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon, l'agent de sécurité sera déployé dans toutes les tâches lancées au sein du ECS cluster Amazon correspondant.

Pour les ECS clusters Amazon qui n'ont pas été exclus, GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

iv. Choisissez Save (Enregistrer).

c. Pour gérer la configuration automatisée des agents en incluant certains ECS clusters Amazon (au niveau du cluster)

i. Ajoutez une balise à un ECS cluster Amazon pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être `GuardDutyManaged` -. `true`

ii. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
```

```
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

GuardDuty Agent de configuration pour un environnement multi-comptes

Dans un environnement à comptes multiples, seul le compte d' GuardDuty administrateur délégué peut activer ou désactiver la configuration automatique des agents pour les comptes des membres, et gérer la configuration automatique des agents pour les ECS clusters Amazon appartenant aux comptes membres de leur organisation. Un compte GuardDuty membre ne peut pas modifier cette configuration. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres

à l'aide de AWS Organizations. Pour plus d'informations sur les environnements multicomptes, consultez la section Gestion de plusieurs comptes dans GuardDuty.

Activation de la configuration automatique des agents pour le compte GuardDuty d'administrateur délégué

Manage for all Amazon ECS clusters (account level)

Si vous avez choisi Activer pour tous les comptes pour la surveillance du temps d'exécution, les options suivantes s'offrent à vous :

- Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gérera l'agent de sécurité pour toutes les ECS tâches Amazon lancées.
- Choisissez Configurer les comptes manuellement.

Si vous avez choisi Configurer les comptes manuellement dans la section Surveillance du temps d'exécution, procédez comme suit :

1. Choisissez Configurer les comptes manuellement dans la section Configuration automatique de l'agent.
2. Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).

Choisissez Save (Enregistrer).

Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
- UpdateServicedans le Amazon Elastic Container Service API Reference.
- update-service dans la référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce ECS cluster Amazon avec la paire clé-valeur sous `GuardDutyManaged` la forme -. `false`
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
4. Dans le volet de navigation, choisissez Runtime Monitoring.

5.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à vos ECS clusters Amazon avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des ECS tâches Amazon lancées.

   Dans l'onglet Configuration, choisissez Activer dans la configuration de l'agent automatisé.

   Pour les ECS clusters Amazon qui n'ont pas été exclus, GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

6. Choisissez Save (Enregistrer).
7. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un ECS cluster Amazon pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être `GuardDutyManaged` -. `true`
2. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
```

```
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Lorsque vous utilisez des balises d'inclusion pour vos ECS clusters Amazon, vous n'avez pas besoin d'activer explicitement GuardDuty l'agent via la configuration automatique des agents.

3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.

- UpdateServicedans le Amazon Elastic Container Service API Reference.
- update-service dans la référence des AWS CLI commandes.

Activation automatique pour tous les comptes membres

Manage for all Amazon ECS clusters (account level)

Les étapes suivantes supposent que vous avez choisi Activer pour tous les comptes dans la section Runtime Monitoring.

1. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gérera l'agent de sécurité pour toutes les ECS tâches Amazon lancées.
2. Choisissez Save (Enregistrer).
3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce ECS cluster Amazon avec la paire clé-valeur sous `GuardDutyManaged` la forme -. `false`
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
```

```
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
4. Dans le volet de navigation, choisissez Runtime Monitoring.
5.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à vos ECS clusters Amazon avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des ECS tâches Amazon lancées.

   Dans l'onglet Configuration, choisissez Modifier.
6. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent

Pour les ECS clusters Amazon qui n'ont pas été exclus, GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

7. Choisissez Save (Enregistrer).
8. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Quelle que soit la manière dont vous choisissez d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller certaines tâches Amazon ECS Fargate pour tous les comptes membres de votre organisation.

1. N'activez aucune configuration dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle que vous avez sélectionnée à l'étape précédente.
2. Choisissez Save (Enregistrer).
3. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Lorsque vous utilisez des balises d'inclusion pour vos ECS clusters Amazon, vous n'avez pas besoin d'activer explicitement la gestion automatique des GuardDuty agents.

4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Activation de la configuration automatique des agents pour les comptes de membres actifs existants

Manage for all Amazon ECS clusters (account level)

1. Sur la page Runtime Monitoring, sous l'onglet Configuration, vous pouvez consulter l'état actuel de la configuration automatique des agents.
2. Dans le volet de configuration de l'agent automatisé, dans la section Comptes membres actifs, sélectionnez Actions.
3. Dans Actions, choisissez Activer pour tous les comptes membres actifs existants.
4. Choisissez Confirmer.
5. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce ECS cluster Amazon avec la paire clé-valeur sous `GuardDutyManaged` la forme -. `false`
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
4. Dans le volet de navigation, choisissez Runtime Monitoring.
5.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à vos ECS clusters Amazon avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des ECS tâches Amazon lancées.

   Sous l'onglet Configuration, dans la section Configuration automatique de l'agent, sous Comptes membres actifs, sélectionnez Actions.
6. Dans Actions, choisissez Activer pour tous les comptes membres actifs.

   Pour les ECS clusters Amazon qui n'ont pas été exclus, GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.
7. Choisissez Confirmer.

8. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un ECS cluster Amazon pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être `GuardDutyManaged` -. `true`
2. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
```

```
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Lorsque vous utilisez des balises d'inclusion pour vos ECS clusters Amazon, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Activation automatique Configuration automatique des agents pour les nouveaux membres

Manage for all Amazon ECS clusters (account level)

1. Sur la page Runtime Monitoring, choisissez Modifier pour mettre à jour la configuration existante.
2. Dans la section Configuration automatique de l'agent, sélectionnez Activer automatiquement pour les nouveaux comptes membres.
3. Choisissez Save (Enregistrer).
4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps

d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

- Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
- UpdateServicedans le Amazon Elastic Container Service API Reference.
- update-service dans la référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce ECS cluster Amazon avec la paire clé-valeur sous `GuardDutyManaged` la forme -. `false`
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
4. Dans le volet de navigation, choisissez Runtime Monitoring.
5.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à vos ECS clusters Amazon avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des ECS tâches Amazon lancées.

   Dans l'onglet Configuration, sélectionnez Activer automatiquement pour les nouveaux comptes membres dans la section Configuration automatique de l'agent.

   Pour les ECS clusters Amazon qui n'ont pas été exclus, GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.
6. Choisissez Save (Enregistrer).
7. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un ECS cluster Amazon pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être `GuardDutyManaged` -. `true`
2. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Lorsque vous utilisez des balises d'inclusion pour vos ECS clusters Amazon, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

3. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Activation sélective de la configuration automatique des agents pour les comptes de membres actifs

Manage for all Amazon ECS (account level)

1. Sur la page Comptes, sélectionnez les comptes pour lesquels vous souhaitez activer la configuration automatique de l'agent Runtime Monitoring (-Fargate)ECS. Vous pouvez sélectionner plusieurs comptes. Assurez-vous que les comptes que vous sélectionnez à cette étape sont déjà activés avec Runtime Monitoring.
2. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration automatisée de l'agent Runtime Monitoring-Automated (ECS-Fargate).
3. Choisissez Confirmer.
4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce ECS cluster Amazon avec la paire clé-valeur sous `GuardDutyManaged` la forme -. `false`
2. Empêchez la modification des balises, sauf par les entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
4. Dans le volet de navigation, choisissez Runtime Monitoring.

5.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à vos ECS clusters Amazon avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon GuardDuty, le conteneur annexe sera attaché à tous les conteneurs des ECS tâches Amazon lancées.

   Sur la page Comptes, sélectionnez les comptes pour lesquels vous souhaitez activer la configuration automatique de l'agent Runtime Monitoring (-Fargate)ECS. Vous pouvez sélectionner plusieurs comptes. Assurez-vous que les comptes que vous sélectionnez à cette étape sont déjà activés avec Runtime Monitoring.

   Pour les ECS clusters Amazon qui n'ont pas été exclus, GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

6. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration automatisée de l'agent Runtime Monitoring-Automated (ECS-Fargate).
7. Choisissez Save (Enregistrer).
8. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Assurez-vous de ne pas activer la configuration d'agent automatisée (ou la configuration d'agent automatisée de surveillance du temps d'exécution (ECS-Fargate)) pour les comptes sélectionnés dotés des ECS clusters Amazon que vous souhaitez surveiller.

2. Ajoutez une balise à un ECS cluster Amazon pour lequel vous souhaitez inclure toutes les tâches. La paire clé-valeur doit être `GuardDutyManaged` -. `true`
3. Empêchez la modification de ces balises, sauf par des entités de confiance. La politique décrite dans Empêcher la modification des balises, sauf selon les principes autorisés dans le Guide de AWS Organizations l'utilisateur, a été modifiée pour être applicable ici.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
```

```
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Lorsque vous utilisez des balises d'inclusion pour vos ECS clusters Amazon, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

4. Lorsque vous GuardDuty souhaitez surveiller des tâches faisant partie d'un service, un nouveau service doit être déployé une fois que vous avez activé la surveillance du temps d'exécution. Si le dernier déploiement d'un ECS service spécifique a été lancé avant que vous n'activiez la surveillance du temps d'exécution, vous pouvez soit redémarrer le service, soit le mettre à jour en utilisant`forceNewDeployment`.

   Pour savoir comment mettre à jour le service, consultez les ressources suivantes :

   - Mettre à jour un ECS service Amazon à l'aide de la console décrite dans le manuel Amazon Elastic Container Service Developer Guide.
   - UpdateServicedans le Amazon Elastic Container Service API Reference.
   - update-service dans la référence des AWS CLI commandes.

Gestion automatique de l'agent de sécurité pour les EKS clusters Amazon

Configuration de l'agent automatisé pour un compte autonome

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Runtime Monitoring.
3. Dans l'onglet Configuration, choisissez Activer pour activer la configuration automatique des agents pour votre compte.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveillez tous les EKS clusters)	1. Choisissez Activer dans la section Configura tion automatique de l'agent. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters existants et potentiellement nouveaux de votre compte. 2. Choisissez Save (Enregistrer).
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:UntagResource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	iam::123456789012:role/org-admins/iam-admin"]
	3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
	4. Dans le volet de navigation, choisissez Runtime Monitoring.
	Note Ajoutez toujours la balise d'exclusion à vos EKS clusters avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte.
	5. Dans l'onglet Configuration, choisissez Activer dans la section de gestion des GuardDuty agents. Pour les EKS clusters qui n'ont pas été exclus de la surveillance, GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.
	6. Choisissez Save (Enregistrer).
	Pour exclure un EKS cluster de la surveillance une fois que l'agent de GuardDuty sécurité a déjà été déployé sur ce cluster
	1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. Après cette étape, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce EKS cluster. Cela peut avoir un impact sur vos statistiques d'utilisation. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	iam::123456789012:role/org-admins/iam-admin"] 3. Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce EKS cluster. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Impact de la désactivation et du nettoyage des ressources.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
Surveillez des EKS clusters sélectifs à l'aide de balises d'inclusion	1. Assurez-vous de choisir Désactiver dans la section Configuration automatique de l'agent. Maintenez la surveillance du temps d'exécution activée. 2. Choisissez Enregistrer. 3. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`true`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les EKS clusters sélectifs que vous souhaitez surveiller. 4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:UntagResource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	Lorsque vous avez plusieurs entités approuvée s, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gestion manuelle de l'agent	1. Assurez-vous de choisir Désactiver dans la section Configuration automatique de l'agent. Maintenez la surveillance du temps d'exécution activée. 2. Choisissez Save (Enregistrer). 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Configuration de l'agent automatisé pour les environnements multi-comptes

Dans les environnements à comptes multiples, seul le compte d' GuardDuty administrateur délégué peut activer ou désactiver la configuration automatique des agents pour les comptes des membres, et gérer l'agent automatique pour les EKS clusters appartenant aux comptes membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter Managing multiple accounts.

Configuration de la configuration automatique de l'agent pour le compte GuardDuty administrateur délégué

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveillez tous les EKS clusters)	Si vous avez choisi Activer pour tous les comptes dans la section Surveillance du temps d'exécution, les options suivantes s'offrent à vous : • Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gérera l'agent de sécurité pour tous les EKS clusters appartenant au compte de compte d' GuardDuty administrateur délégué ainsi que pour tous les EKS clusters appartenant à tous les comptes membres existants et potentiellement nouveaux de l'organisation. • Choisissez Configurer les comptes manuellement. Si vous avez choisi Configurer les comptes manuellement dans la section Surveillance du temps d'exécution, procédez comme suit : 1. Choisissez Configurer les comptes manuellement dans la section Configuration automatique de l'agent. 2. Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte). Choisissez Save (Enregistrer).
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide de balises d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDuty Managed` et sa valeur comme`false`.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:Untag Resource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/. 4. Dans le volet de navigation, choisissez Runtime Monitoring. **Note** Ajoutez toujours la balise d'exclusion à vos EKS clusters avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon, l'agent de GuardDuty

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	sécurité sera déployé sur tous les EKS clusters de votre compte. 5. Dans l'onglet Configuration, choisissez Activer dans la section de gestion des GuardDuty agents. Pour les EKS clusters qui n'ont pas été exclus de la surveillance, GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité. 6. Choisissez Save (Enregistrer). Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDuty Managed` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:Untag Resource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Si vous avez activé l'agent automatique pour ce EKS cluster, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce EKS cluster. Cela peut avoir un impact sur vos statistiques d'utilisation. Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce EKS cluster. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Impact de la désactivation et du nettoyage des ressources. 4. Si vous gériez manuellement l'agent de GuardDuty sécurité pour ce EKS cluster, consultezImpact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez des EKS clusters sélectifs à l'aide de balises d'inclusion	Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller EKS certains clusters de votre compte : 1. Assurez-vous de choisir Désactiver pour le compte GuardDuty administrateur délégué (ce compte) dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Choisissez Save (Enregistrer). 3. Ajoutez une balise à votre EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`true`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les EKS clusters sélectifs que vous souhaitez surveiller. 4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:Untag Resource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gestion manuelle de l'agent de GuardDuty sécurité	Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, vous pouvez gérer l'agent de sécurité manuellement pour vos EKS clusters. 1. Assurez-vous de choisir Désactiver pour le compte GuardDuty administrateur délégué (ce compte) dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Choisissez Save (Enregistrer). 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Activation automatique Agent automatique pour tous les comptes de membres

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveillez tous les EKS clusters)	Cette rubrique vise à activer la surveillance du temps d'exécuti on pour tous les comptes membres. Par conséquent, les étapes suivantes supposent que vous devez avoir choisi Activer pour tous les comptes dans la section Surveillance du temps d'exécution. 1. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. GuardDuty déploiera et gérera l'agent de sécurité pour tous les EKS clusters appartena nt au compte de compte d' GuardDuty administrateur délégué ainsi que pour tous les EKS clusters appartenant à tous les comptes membres existants et potentiellement nouveaux de l'organisation. 2. Choisissez Save (Enregistrer).
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide de balises d'exclusi on)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDuty Managed` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes

- Remplacez *ec2:DeleteTags* avec `eks:Untag Resource` .
- Remplacez *access-project* avec `GuardDutyManaged`
- Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance.

  Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` :

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
4. Dans le volet de navigation, choisissez Runtime Monitoring.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à vos EKS clusters avant d'activer l'agent automatisé pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte.

5. Sous l'onglet Configuration, choisissez Modifier dans la section Configuration de la surveillance du temps d'exécution.
6. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent. Pour les EKS clusters qui n'ont pas été exclus de la surveillance, GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.
7. Choisissez Save (Enregistrer).

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDuty Managed` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Si la configuration automatique de l'agent est activée pour ce EKS cluster, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce EKS cluster. Cela peut avoir un impact sur vos statistiques d'utilisation. Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce EKS cluster. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Impact de la désactivation et du nettoyage des ressources. 3. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:Untag Resource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 4. Si vous gériez manuellement l'agent de GuardDuty sécurité pour ce EKS cluster, consultezImpact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez des EKS clusters sélectifs à l'aide de balises d'inclusion	Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller des EKS clusters sélectifs pour tous les comptes membres de votre organisation : 1. N'activez aucune configuration dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Choisissez Save (Enregistrer). 3. Ajoutez une balise à votre EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`true`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les EKS clusters sélectifs que vous souhaitez surveiller. 4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:Untag Resource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gestion manuelle de l'agent de GuardDuty sécurité	Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, vous pouvez gérer l'agent de sécurité manuellement pour vos EKS clusters. 1. N'activez aucune configuration dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Choisissez Save (Enregistrer). 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Activation de l'agent automatique pour tous les comptes de membres actifs existants

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Pour gérer l'agent GuardDuty de sécurité pour les comptes de membres actifs existants de votre organisation

- GuardDuty Pour recevoir les événements d'exécution des EKS clusters appartenant aux comptes de membres actifs existants de l'organisation, vous devez choisir une approche préférée pour gérer l'agent GuardDuty de sécurité pour ces EKS clusters. Pour plus

d'informations sur ces approches, veuillez consulter Approches de gestion des agents GuardDuty de sécurité.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveillez tous les EKS clusters)	Pour surveiller tous les EKS clusters pour tous les comptes de membres actifs existants 1. Sur la page Runtime Monitoring, sous l'onglet Configuration, vous pouvez consulter l'état actuel de la configuration automatique des agents. 2. Dans le volet Configuration automatique de l'agent, dans la section Comptes membres actifs, sélection nez Actions. 3. Dans Actions, choisissez Activer pour tous les comptes membres actifs existants. 4. Choisissez Confirmer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:UntagResource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` :

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/. 4. Dans le volet de navigation, choisissez Runtime Monitoring. **Note** Ajoutez toujours la balise d'exclusion à vos EKS clusters avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte. 5. Sous l'onglet Configuration, dans le volet Configuration automatique de l'agent, sous Comptes membres actifs, sélectionnez Actions. 6. Dans Actions, choisissez Activer pour tous les comptes membres actifs. 7. Choisissez Confirmer. Pour exclure un EKS cluster de la surveillance une fois que l'agent de GuardDuty sécurité a déjà été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`false`.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. Après cette étape, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce EKS cluster. Cela peut avoir un impact sur vos statistiques d'utilisation. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"] 3. Quelle que soit la façon dont vous gérez l'agent de sécurité (par le biais GuardDuty ou manuellement), pour ne plus recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce EKS cluster. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Impact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez des EKS clusters sélectifs à l'aide de balises d'inclusion	1. Sur la page Comptes, une fois que vous avez activé la surveillance du temps d'exécution, n'activez pas la surveillance du temps d'exécution - Configuration automatique de l'agent. 2. Ajoutez une balise au EKS cluster qui appartient au compte sélectionné que vous souhaitez surveiller. La paire clé-valeur de la balise doit être `GuardDuty Managed -true`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les EKS clusters sélectifs que vous souhaitez surveiller. 3. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:UntagResource` . • Remplacez *`access-project`* avec `GuardDuty Managed` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque vous avez plusieurs entités approuvée s, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gestion manuelle de l'agent de GuardDuty sécurité	1. Assurez-vous de ne pas sélectionner Activer dans la section Configuration automatique de l'agent. Maintenez la surveillance du temps d'exécution activée. 2. Choisissez Save (Enregistrer). 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Activer automatiquement la configuration automatique des agents pour les nouveaux membres

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveillez tous les EKS clusters)	1. Sur la page Runtime Monitoring, choisissez Modifier pour mettre à jour la configuration existante. 2. Dans la section Configuration automatique de l'agent, sélectionnez Activer automatiquement pour les nouveaux comptes membres. 3. Choisissez Save (Enregistrer).

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide de balises d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:UntagResource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` :

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/. 4. Dans le volet de navigation, choisissez Runtime Monitoring. **Note** Ajoutez toujours la balise d'exclusion à vos EKS clusters avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte. 5. Dans l'onglet Configuration, sélectionnez Activer automatiquement les nouveaux comptes membres dans la section Gestion des GuardDuty agents. Pour les EKS clusters qui n'ont pas été exclus de la surveillance, GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité. 6. Choisissez Save (Enregistrer). Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster 1. Que vous gériez l'agent GuardDuty de sécurité par le biais GuardDuty ou manuellement, ajoutez une balise à

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	ce EKS cluster avec la clé as `GuardDutyManaged` et sa valeur as`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutil isateur Amazon. Si l'agent automatisé est activé pour ce EKS cluster, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce EKS cluster. Cela peut avoir un impact sur vos statistiques d'utilisa tion. Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce EKS cluster. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Impact de la désactivation et du nettoyage des ressources. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagRe source` . • Remplacez *`ec2:DeleteTags`* avec `eks:Untag Resource` .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	• Remplacez *access-project* avec `GuardDuty Managed` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvée s, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Si vous gériez manuellement l'agent de GuardDuty sécurité pour ce EKS cluster, consultezImpact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez des EKS clusters sélectifs à l'aide de balises d'inclusion	Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller EKS des clusters sélectifs pour les nouveaux comptes membres de votre organisation. 1. Assurez-vous de désactiver l'option Activer automatiquement pour les nouveaux comptes membres dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Choisissez Save (Enregistrer). 3. Ajoutez une balise à votre EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme `true`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les EKS clusters sélectifs que vous souhaitez surveiller. 4. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	• Remplacez *access-project* avec `GuardDuty Managed` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvée s, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gestion manuelle de l'agent de GuardDuty sécurité	Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, vous pouvez gérer l'agent de sécurité manuellement pour vos EKS clusters. 1. Assurez-vous de décocher la case Activer automatiq uement pour les nouveaux comptes membres dans la section Configuration automatique de l'agent. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Choisissez Save (Enregistrer). 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Configuration sélective de l'agent automatisé pour les comptes de membres actifs

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (Surveillez tous les EKS clusters)	1. Sur la page Comptes, sélectionnez les comptes pour lesquels vous souhaitez activer la configuration automatique des agents. Vous pouvez sélectionner plusieurs comptes à la fois. Assurez-vous que la surveillance du temps d'EKSexécution est déjà activée sur les comptes que vous sélectionnez à cette étape. 2. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer Runtime Monitoring - Configuration automatisée des agents. 3. Choisissez Confirmer.
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide de balises d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDuty Managed` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:Untag Resource` .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes

- Remplacez *access-project* avec `GuardDutyManaged`
- Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance.

  Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` :

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Ajoutez toujours la balise d'exclusion à vos EKS clusters avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte.

4. Sur la page Comptes, sélectionnez le compte pour lequel vous souhaitez activer Gérer automatiquement l'agent. Vous pouvez sélectionner plusieurs comptes à la fois.
5. Dans Modifier les plans de protection, choisissez l'option appropriée pour activer la configuration automatique de l'agent Runtime Monitoring pour le compte sélectionné.

   Pour les EKS clusters qui n'ont pas été exclus de la surveillance, GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.
6. Choisissez Save (Enregistrer).

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour exclure un EKS cluster de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster 1. Ajoutez une balise à ce EKS cluster avec la clé as `GuardDuty Managed` et sa valeur comme`false`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. Si vous avez déjà activé la configuration automatique de l'agent pour ce EKS cluster, l'agent de sécurité pour ce cluster ne GuardDuty sera pas mis à jour après cette étape. Cependant, l'agent de sécurité restera déployé et GuardDuty continuera à recevoir les événements d'exécution de ce EKS cluster. Cela peut avoir un impact sur vos statistiques d'utilisation. Pour arrêter de recevoir les événements d'exécution de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce EKS cluster. Pour plus d'informations sur la suppression de l'agent de sécurité déployé, veuillez consulter Impact de la désactivation et du nettoyage des ressources. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:Untag Resource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Si vous gériez l'agent GuardDuty de sécurité pour ce EKS cluster manuellement, vous devez le supprimer. Pour de plus amples informations, veuillez consulter Impact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez des EKS clusters sélectifs à l'aide de balises d'inclusion	Quelle que soit la manière dont vous avez choisi d'activer la surveillance du temps d'exécution, les étapes suivantes vous aideront à surveiller certains EKS clusters appartenant aux comptes sélectionnés : 1. Assurez-vous de ne pas activer la configuration automatique de l'agent Runtime Monitoring pour les comptes sélectionnés qui possèdent les EKS clusters que vous souhaitez surveiller. 2. Ajoutez une balise à votre EKS cluster avec la clé as `GuardDutyManaged` et sa valeur comme`true`. Pour plus d'informations sur le balisage de votre EKS cluster Amazon, consultez la section Utilisation des balises à l'aide de la console dans le guide de l'EKSutilisateur Amazon. Après avoir ajouté la balise, GuardDuty il gérera le déploiement et les mises à jour de l'agent de sécurité pour les EKS clusters sélectifs que vous souhaitez surveiller. 3. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie , remplacez les informations suivantes : • Remplacez *`ec2:CreateTags`* avec `eks:TagResource` . • Remplacez *`ec2:DeleteTags`* avec `eks:Untag Resource` . • Remplacez *`access-project`* avec `GuardDutyManaged` • Remplacez *`123456789012`* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` :

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gestion manuelle de l'agent de GuardDuty sécurité	1. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. Assurez-vous de ne pas activer Runtime Monitoring - Configuration automatique de l'agent pour aucun des comptes sélectionnés. 2. Choisissez Confirmer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon

Cette section décrit comment vous pouvez gérer votre agent EKS complémentaire Amazon (GuardDuty agent) après avoir activé Runtime Monitoring. Pour utiliser Runtime Monitoring, vous devez activer Runtime Monitoring et configurer le EKS module complémentaire Amazon,`aws-guardduty-agent`. L'exécution d'une seule de ces deux étapes ne permettra pas de GuardDuty détecter les menaces potentielles ni de générer des résultats.

Conditions préalables au déploiement de l'agent GuardDuty de sécurité

Cette section décrit les conditions préalables au déploiement manuel de l'agent GuardDuty de sécurité pour vos EKS clusters. Avant de continuer, assurez-vous d'avoir déjà configuré la surveillance du temps d'exécution pour vos comptes. L'agent GuardDuty de sécurité (EKSmodule complémentaire) ne fonctionnera pas si vous ne configurez pas la surveillance du temps d'exécution. Pour de plus amples informations, veuillez consulter Activer la surveillance du GuardDuty temps d'exécution. Une fois que vous avez terminé les étapes suivantes, veuillez consulter Déployer un agent GuardDuty de sécurité.

Choisissez votre méthode d'accès préférée pour créer un point de VPC terminaison Amazon.

Console

Création d'un VPC endpoint

1. Ouvrez la VPC console Amazon à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sous Cloud privé virtuel, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Sur la page Créer un point de terminaison, pour Catégorie de services, choisissez Autres services de points de terminaison.
5. Pour Nom du service, entrez **com.amazonaws.*us-east-1*.guardduty-data**.

   Assurez-vous de remplacer *us-east-1* avec la bonne région. Il doit s'agir de la même région que le EKS cluster qui appartient à votre Compte AWS identifiant.
6. Choisissez Vérifier le service.
7. Une fois le nom du service vérifié avec succès, choisissez l'VPCemplacement de votre cluster. Ajoutez la politique suivante pour limiter l'utilisation des VPC terminaux au compte spécifié uniquement. Avec l'organisation `Condition` indiquée sous cette stratégie, vous pouvez mettre à jour la stratégie suivante pour restreindre l'accès à votre point de terminaison. Pour fournir une assistance aux VPC terminaux à un compte IDs spécifique de votre organisation, consultezOrganization condition to restrict access to your endpoint.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
```

```
    "Principal": "*"
   }
  ]
}
```

L'identifiant du `aws:PrincipalAccount` compte doit correspondre au compte contenant le point de VPC terminaison VPC et. La liste suivante indique comment partager le VPC point de terminaison avec d'autres utilisateurs Compte AWS IDs :

Condition d'organisation pour restreindre l'accès à votre point de terminaison

- Pour spécifier plusieurs comptes pour accéder au VPC point de terminaison, remplacez-le `"aws:PrincipalAccount": "111122223333"` par ce qui suit :

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- Pour autoriser tous les membres d'une organisation à accéder au VPC point de terminaison, remplacez-le `"aws:PrincipalAccount": "111122223333"` par ce qui suit :

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Pour restreindre l'accès à une ressource à un ID d'organisation, ajoutez votre `ResourceOrgID` à la stratégie.

  Pour plus d'informations, consultez la section ResourceOrgID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Sous Paramètres supplémentaires, choisissez Activer DNS le nom.
9. Sous Sous-réseaux, choisissez les sous-réseaux dans lesquels réside votre cluster.
10. Sous Groupes de sécurité, choisissez un groupe de sécurité dont le port entrant 443 est activé depuis votre VPC (ou votre EKS cluster). Si vous ne possédez pas encore de groupe de sécurité dont le port entrant 443 est activé, créez un groupe de sécurité.

En cas de problème lors de la restriction des autorisations entrantes à votre VPC (ou à votre cluster), fournissez le support au port 443 entrant depuis n'importe quelle adresse IP ()`0.0.0.0/0`.

API/CLI

- Invoquer CreateVpcEndpoint.
- Utilisez les valeurs suivantes pour les paramètres :
  - Pour Nom du service, entrez **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

    Assurez-vous de remplacer *`us-east-1`* avec la bonne région. Il doit s'agir de la même région que le EKS cluster qui appartient à votre Compte AWS identifiant.
  - Pour DNSOptionsactiver l'DNSoption privée en la définissant sur`true`.
- Pour AWS Command Line Interface, voir create-vpc-endpoint.

Configurer les paramètres GuardDuty de l'agent de sécurité (module complémentaire) pour Amazon EKS

Vous pouvez configurer des paramètres spécifiques de votre agent GuardDuty de sécurité pour AmazonEKS. Ce support est disponible pour les versions 1.5.0 et supérieures de l'agent de GuardDuty sécurité. Pour plus d'informations sur les dernières versions des modules complémentaires, consultezGuardDuty agent de sécurité pour les EKS clusters Amazon.

Pourquoi dois-je mettre à jour le schéma de configuration de l'agent de sécurité ?

Le schéma de configuration de l'agent de GuardDuty sécurité est le même pour tous les conteneurs de vos EKS clusters Amazon. Lorsque les valeurs par défaut ne correspondent pas aux charges de travail et à la taille de l'instance associées, envisagez de configurer les CPU paramètres`PriorityClass`, les paramètres de mémoire et `dnsPolicy` les paramètres. Quelle que soit la façon dont vous gérez l' GuardDuty agent pour vos EKS clusters Amazon, vous pouvez configurer ou mettre à jour la configuration existante de ces paramètres.

Comportement de configuration automatique des agents avec paramètres configurés

Lorsqu'il GuardDuty gère l'agent de sécurité (EKSmodule complémentaire) en votre nom, il met à jour le module complémentaire, selon les besoins. GuardDuty définira la valeur des

paramètres configurables sur une valeur par défaut. Cependant, vous pouvez toujours mettre à jour les paramètres à la valeur souhaitée. Si cela entraîne un conflit, l'option par défaut resolveConflictsestNone.

Paramètres et valeurs configurables

Pour plus d'informations sur les étapes de configuration des paramètres du module complémentaire, voir :

- Déployer un agent GuardDuty de sécurité ou
- Mise à jour manuelle de l'agent de sécurité

Les tableaux suivants indiquent les plages et les valeurs que vous pouvez utiliser pour déployer le EKS module complémentaire Amazon manuellement ou pour mettre à jour les paramètres du module complémentaire existant.

CPUparamètres

Paramètres	Valeur par défaut	Gamme configurable
Requêtes	200 m	Entre 200 m et 10 000 m, les deux inclus
Limites	1 000 m	

Réglages de mémoire

Paramètres	Valeur par défaut	Gamme configurable
Requêtes	256 Mi	Entre 256 mi et 20 000 mi, les deux inclus
Limites	1024 milles	

Paramètres **`PriorityClass`**

Lorsque vous GuardDuty créez un EKS module complémentaire Amazon pour vous, le module attribué `PriorityClass` estaws-guardduty-agent.priorityclass. Cela signifie qu'aucune action ne sera entreprise en fonction de la priorité de l'agent pod. Vous pouvez

configurer ce paramètre complémentaire en choisissant l'une des `PriorityClass` options suivantes :

Configurable **`PriorityClass`**	Valeur **`preemptionPolicy`**	**`preemptionPolicy`** description	Valeur du pod
`aws-guardduty-agent.priorityclass`	`Never`	Aucune action	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	L'attribution de cette valeur préemptera un pod exécuté avec une valeur de priorité inférieure à la valeur du pod de l'agent.	100 000 000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2 000 000 000
`system-node-critical` [1]	`PreemptLowerPriority`		200 000 1000

[1] Kubernetes propose ces deux `PriorityClass` options — et. `system-cluster-critical` `system-node-critical` Pour plus d'informations, consultez la PriorityClassdocumentation de Kubernetes.

Paramètres **`dnsPolicy`**

Choisissez l'une des options de DNS stratégie suivantes prises en charge par Kubernetes. Lorsqu'aucune configuration n'est spécifiée, elle `ClusterFirst` est utilisée comme valeur par défaut.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Pour plus d'informations sur ces politiques, consultez la DNSpolitique de Pod dans la documentation de Kubernetes.

Déployer un agent GuardDuty de sécurité

Cette section décrit comment déployer l'agent de GuardDuty sécurité pour la première fois pour des EKS clusters spécifiques. Avant de passer à cette section, assurez-vous d'avoir déjà configuré les prérequis et activé la surveillance du temps d'exécution pour vos comptes. L'agent GuardDuty de sécurité (EKSmodule complémentaire) ne fonctionnera pas si vous n'activez pas la surveillance du temps d'exécution.

Choisissez votre méthode d'accès préférée pour déployer l'agent GuardDuty de sécurité pour la première fois.

Console

1. Ouvrez la EKS console Amazon à l'adresse https://console.aws.amazon.com/eks/home#/clusters.
2. Choisissez le nom de votre cluster.
3. Choisissez l'onglet Modules complémentaires.
4. Choisissez Obtenez plus de modules complémentaires.
5. Sur la page Sélectionner les modules complémentaires, choisissez Amazon GuardDuty Runtime Monitoring.
6. Sur la page Configurer les paramètres du module complémentaire sélectionné, utilisez les paramètres par défaut. Si le statut de votre EKS module complémentaire est Nécessite une activation, choisissez Activer GuardDuty. Cette action ouvre la GuardDuty console permettant de configurer la surveillance du temps d'exécution pour vos comptes.
7. Après avoir configuré la surveillance du temps d'exécution pour vos comptes, revenez à la EKS console Amazon. Le statut de votre EKS module complémentaire doit être passé à Prêt à être installé.
8. (Facultatif) Fourniture d'un schéma de configuration EKS complémentaire

   Pour la version complémentaire, si vous choisissez la version v1.5.0 ou supérieure, Runtime Monitoring prend en charge la configuration de paramètres spécifiques de l' GuardDuty agent. Pour plus d'informations sur les plages de paramètres, consultezConfigurer les paramètres des EKS modules complémentaires.

a. Développez les paramètres de configuration facultatifs pour afficher les paramètres configurables ainsi que leur valeur et leur format attendus.

b. Définissez les paramètres. Les valeurs doivent être comprises dans la plage indiquée dansConfigurer les paramètres des EKS modules complémentaires.

c. Choisissez Enregistrer les modifications pour créer le module complémentaire en fonction de la configuration avancée.

d. Pour la méthode de résolution des conflits, l'option que vous choisissez sera utilisée pour résoudre un conflit lorsque vous mettez à jour la valeur d'un paramètre à une valeur autre que celle par défaut. Pour plus d'informations sur les options répertoriées, consultez resolveConflictsla EKSAPIréférence Amazon.

9. Choisissez Suivant.
10. Dans la page Vérifier et créer, vérifiez tous les détails, puis choisissez Créer.
11. Revenez aux détails du cluster et choisissez l'onglet Ressources.
12. Vous pouvez afficher les nouveaux modules avec le préfixe aws-guardduty-agent.

API/CLI

Vous pouvez configurer l'agent EKS complémentaire Amazon (`aws-guardduty-agent`) à l'aide de l'une des options suivantes :

- Courez CreateAddonpour votre compte.
-

> **Note**
>
> Pour le module complémentaire`version`, si vous choisissez la version v1.5.0 ou supérieure, Runtime Monitoring prend en charge la configuration de paramètres spécifiques de l' GuardDuty agent. Pour de plus amples informations, veuillez consulter Configurer les paramètres des EKS modules complémentaires.

Utilisez les valeurs suivantes pour les paramètres de demande :

- Pour `addonName`, saisissez `aws-guardduty-agent`.

Vous pouvez utiliser l' AWS CLI exemple suivant lorsque vous utilisez des valeurs configurables prises en charge pour les versions d'addon v1.5.0 et supérieures. Assurez-vous

de remplacer les valeurs d'espace réservé surlignées en rouge et celles `Example.json` associées aux valeurs configurées.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Exemple.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Pour plus d'informations sur les `addonVersion` pris en charge, veuillez consulter Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty .
- Vous pouvez également utiliser AWS CLI. Pour plus d'informations, consultez create-addon.

Mise à jour manuelle de l'agent de sécurité

Lorsque vous gérez l'agent GuardDuty de sécurité manuellement, il vous incombe de le mettre à jour pour votre compte. Pour recevoir des notifications concernant les nouvelles versions de l'agent, vous pouvez vous abonner à un RSS flux deGuardDuty historique des versions de l'agent.

Vous pouvez mettre à jour l'agent de sécurité vers la dernière version pour bénéficier du support et des améliorations supplémentaires. Si la version actuelle de votre agent arrive à la fin du support standard, pour continuer à utiliser Runtime Monitoring (ou EKS Runtime Monitoring), vous devez mettre à jour la version actuelle de votre agent. Pour plus d'informations sur les versions publiées, consultezGuardDuty agent de sécurité pour les EKS clusters Amazon.

Prérequis

Avant de mettre à jour la version de l'agent de sécurité, assurez-vous que la version de l'agent que vous prévoyez d'utiliser maintenant est compatible avec votre version de Kubernetes. Pour de plus amples informations, veuillez consulter Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty .

Console

1. Ouvrez la EKS console Amazon à l'adresse https://console.aws.amazon.com/eks/home#/clusters.
2. Choisissez le nom de votre cluster.
3. Choisissez Modules complémentaires.
4. Sous Modules complémentaires, sélectionnez GuardDutyRuntime Monitoring.
5. Choisissez Modifier pour mettre à jour les informations de l'agent.
6. Sur la page Configurer la surveillance du temps GuardDuty d'exécution, mettez à jour les détails.
7. (Facultatif) Mise à jour des paramètres de configuration des modules complémentaires

   Si la version de votre EKS module complémentaire est 1.5.0 ou supérieure, vous pouvez également mettre à jour les paramètres de configuration du module complémentaire.

   a. Développez les paramètres de configuration facultatifs pour afficher le schéma de configuration.
   b. Mettez à jour les valeurs des paramètres en fonction de la plage fournie dansConfigurer les paramètres des EKS modules complémentaires.
   c. Choisissez Enregistrer les modifications pour démarrer la mise à jour.
   d. Pour la méthode de résolution des conflits, l'option que vous choisissez sera utilisée pour résoudre un conflit lorsque vous mettez à jour la valeur d'un paramètre à une valeur autre que celle par défaut. Pour plus d'informations sur les options répertoriées, consultez resolveConflictsla EKSAPIréférence Amazon.

API/CLI

Pour mettre à jour l'agent GuardDuty de sécurité pour vos EKS clusters Amazon, consultez Mettre à jour un module complémentaire.

> **Note**
>
> Pour le module complémentaire`version`, si vous choisissez la version v1.5.0 ou supérieure, Runtime Monitoring prend en charge la configuration de paramètres spécifiques de l' GuardDuty agent. Pour plus d'informations sur les plages de paramètres, consultezConfigurer les paramètres des EKS modules complémentaires.

Vous pouvez utiliser l' AWS CLI exemple suivant lorsque vous utilisez des valeurs configurables prises en charge pour les versions d'addon v1.5.0 et supérieures. Assurez-vous de remplacer les valeurs d'espace réservé surlignées en rouge et celles `Example.json` associées aux valeurs configurées.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Exemple.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Si la version de votre EKS module complémentaire Amazon est 1.5.0 ou supérieure et que vous avez configuré le schéma du module complémentaire, vous pouvez vérifier si les valeurs apparaissent correctement pour votre cluster. Pour de plus amples informations, veuillez consulter Vérification des mises à jour du schéma de configuration.

Vérification des mises à jour du schéma de configuration

Après avoir configuré les paramètres, effectuez les étapes suivantes pour vérifier que le schéma de configuration a été mis à jour :

1. Ouvrez la EKS console Amazon à l'adresse https://console.aws.amazon.com/eks/home#/clusters.
2. Dans le panneau de navigation, choisissez Clusters.
3. Sur la page Clusters, sélectionnez le nom du cluster dont vous souhaitez vérifier les mises à jour.
4. Sélectionnez l'onglet Ressources.
5. Dans le volet Types de ressources, sous Charges de travail, sélectionnez DaemonSets.
6. Sélectionnez aws-guardduty-agent.
7. Sur la aws-guardduty-agentpage, choisissez l'affichage brut pour afficher la réponse non formatée. JSON Vérifiez que les paramètres configurables affichent la valeur que vous avez fournie.

Après avoir vérifié, passez à la GuardDuty console. Sélectionnez le correspondant Région AWS et consultez l'état de couverture de vos EKS clusters Amazon. Pour de plus amples informations, veuillez consulter Couverture pour les EKS clusters Amazon.

Configuration de la surveillance du temps EKS d'exécution (APIuniquement)

Avant de configurer la surveillance du temps EKS d'exécution dans votre compte, assurez-vous que vous utilisez l'une des plateformes vérifiées qui prend en charge la version de Kubernetes actuellement utilisée. Pour en savoir plus, consultez Validation des exigences architecturales.

GuardDuty a consolidé l'expérience de console pour la surveillance du EKS temps d'exécution dans la surveillance du temps d'exécution. GuardDuty recommande Vérifier l'état de configuration de EKS Runtime Monitoring etMigration de la surveillance du temps EKS d'exécution vers la surveillance du temps d'exécution.

Dans le cadre de la migration vers Runtime Monitoring, assurez-vous deDésactiver la surveillance de l'EKSexécution. Ceci est important car si vous choisissez ultérieurement de désactiver la surveillance du temps d'exécution et que vous ne le désactivez EKS pas, vous continuerez de devoir payer des frais d'utilisation pour EKS ce type de surveillance.

Configuration de la surveillance du temps d'EKSexécution pour un compte autonome

Pour les comptes associés à AWS Organizations, veuillez consulter Configuration de la surveillance du temps EKS d'exécution pour les environnements à comptes multiples.

Choisissez votre méthode d'accès préférée pour activer la surveillance du temps EKS d'exécution pour votre compte.

API/CLI

Sur la base de Approches de gestion des agents GuardDuty de sécurité, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les EKS clusters)	1. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon de votre compte. 2. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorI d` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITO RING` et `EKS_ADDON_MANAGEMENT` :

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	3.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à votre EKS cluster avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte.

Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`.

Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`.

GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon qui n'ont pas été exclus de la surveillance.

Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorI d` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

L'exemple suivant active `EKS_RUNTIME_MONITO RING` et `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-detector --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --
```

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " *ENABLED*", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " *ENABLED*"}]]'

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des EKS clusters sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon marqués avec la `true` paire `GuardDuty Managed -`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	1. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Configuration de la surveillance du temps EKS d'exécution pour les environnements à comptes multiples

Dans les environnements à comptes multiples, seul le compte d' GuardDuty administrateur délégué peut activer ou désactiver la surveillance du temps EKS d'exécution pour les comptes membres et

gérer la gestion des GuardDuty agents pour les EKS clusters appartenant aux comptes membres de leur organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration à partir de leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter Managing multiple accounts.

Configuration de la surveillance du temps EKS d'exécution pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour activer la surveillance du temps EKS d'exécution et gérer l'agent de GuardDuty sécurité pour les EKS clusters appartenant au compte d' GuardDuty administrateur délégué.

API/CLI

Sur la base de Approches de gestion des agents GuardDuty de sécurité, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les EKS clusters)	Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	3.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à votre EKS cluster avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte.

Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`.

Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`.

GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon qui n'ont pas été exclus de la surveillance.

Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-detector --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --
```

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	features '[{"Name" : "EKS_RUNTIME_MONIT ORING", "Status" : " *ENABLED*", "Addition alConfiguration" : [{"Name" : "EKS_ADDO N_MANAGEMENT", "Status" : " *ENABLED*"}]]'

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des EKS clusters sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon marqués avec la `true` paire `GuardDuty Managed -`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	1. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Activer automatiquement la surveillance du EKS temps d'exécution pour tous les comptes membres

Choisissez votre méthode d'accès préférée pour activer la surveillance du EKS temps d'exécution pour tous les comptes membres. Cela inclut le compte d' GuardDuty administrateur délégué, les comptes de membres existants et les nouveaux comptes qui rejoignent l'organisation. Choisissez

l'approche que vous préférez pour gérer l'agent de GuardDuty sécurité pour les EKS clusters appartenant à ces comptes membres.

API/CLI

Sur la base de Approches de gestion des agents GuardDuty de sécurité, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveill ez tous les EKS clusters)	Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMem berDetectorsAPIopération en utilisant votre propre *`detector ID`*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.a ws.amazon.com/guardduty/console ou exécutez le ListDetec torsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Note Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDuty Managed -false`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDuty Managed` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Ajoutez toujours la balise d'exclusion à votre EKS cluster avant de définir le paramètre `STATUS` of

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	`EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon qui n'ont pas été exclus de la surveillance. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	> **Note** > Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des EKS clusters sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDuty Managed -true`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDuty Managed` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon marqués avec la `true` paire `GuardDutyManaged` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	compte, cet ID de compte est répertorié avec un résumé du problème.
Gestion manuelle de l'agent de sécurité	1. Exécutez-le updateDetectorAPIen utilisant votre propre identifiant de détecteur régional et en transmettant le nom `EKS_RUNTIME_MONITORING` et le statut de l'`features`objet en tant que`ENABLED`. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Configuration de la surveillance du temps EKS d'exécution pour tous les comptes de membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la surveillance du temps EKS d'exécution et gérer l'agent de GuardDuty sécurité pour les comptes de membres actifs existants de votre organisation.

API/CLI

Sur la base de Approches de gestion des agents GuardDuty de sécurité, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les EKS clusters)	Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *detector ID*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "Addition`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "*ENABLED*"}]]' **Note** Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDuty Managed -false`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDuty Managed` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Ajoutez toujours la balise d'exclusion à votre EKS cluster avant de définir le paramètre `STATUS` of

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	`EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon qui n'ont pas été exclus de la surveillance. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	> **Note** > Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des EKS clusters sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDuty Managed -true`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDuty Managed` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *detector ID*.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon marqués avec la `true` paire `GuardDutyManaged` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	compte, cet ID de compte est répertorié avec un résumé du problème.
Gestion manuelle de l'agent de sécurité	1. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *detector ID*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Activer automatiquement la surveillance du EKS temps d'exécution pour les nouveaux membres

Le compte d' GuardDuty administrateur délégué peut activer automatiquement la surveillance du temps EKS d'exécution et choisir une approche pour gérer l'agent GuardDuty de sécurité pour les nouveaux comptes qui rejoignent votre organisation.

API/CLI

Sur la base de Approches de gestion des agents GuardDuty de sécurité, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les EKS clusters)	Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos nouveaux comptes, lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *detector ID*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active à la fois `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` pour un seul compte. Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	3. **Note** Ajoutez toujours la balise d'exclusion à votre EKS cluster avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos nouveaux comptes, lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *`detector ID`*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon qui n'ont pas été exclus de la surveillance. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active à la fois `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` pour un seul compte. Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des EKS clusters sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos nouveaux comptes,

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *detector ID*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon marqués avec la `true` paire `GuardDuty Managed -`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` pour un seul compte. Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	ration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "AutoEnable": "NEW"}]]' Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	1. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos nouveaux comptes, lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *detector ID*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` pour un seul compte. Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème. 2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Activer la surveillance du temps EKS d'exécution pour les comptes de membres actifs individuels

API/CLI

Sur la base de Approches de gestion des agents GuardDuty de sécurité, vous pouvez choisir une approche préférée et suivre les étapes indiquées dans le tableau suivant.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gérez l'agent de sécurité via GuardDuty (surveillez tous les EKS clusters)	Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveillez tous les EKS clusters mais excluez certains d'entre eux (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	3.

> **Note**
>
> Ajoutez toujours la balise d'exclusion à votre EKS cluster avant de définir le paramètre `STATUS of EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les EKS clusters de votre compte.

Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.

Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `ENABLED`.

GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon qui n'ont pas été exclus de la surveillance.

Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

L'exemple suivant active `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --
detector-id  12abc34d567e8fa901bc2d34e56
789f0  --account-ids  111122223333  --feature
```

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "*ENABLED*", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " *ENABLED*"}]]' **Note** Vous pouvez également transmettre une liste de comptes IDs séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des EKS clusters sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au EKS cluster que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, consultez la section Utilisation des balises à l'aide de CLIAPI, ou eksctl dans le guide de EKSl'utilisateur Amazon. 2. Pour empêcher la modification des balises, sauf par les entités approuvées, appliquez la stratégie décrite dans Empêcher la modification de balises sauf par des mandataires autorisés dans le Guide de l'utilisateur AWS Organizations . Dans cette stratégie, remplacez les informations suivantes : • Remplacez *ec2:CreateTags* avec `eks:TagResource` . • Remplacez *ec2:DeleteTags* avec `eks:UntagResource` . • Remplacez *access-project* avec `GuardDutyManaged` • Remplacez *123456789012* avec l' Compte AWS identifiant de l'entité de confiance. Lorsque vous avez plusieurs entités approuvées, utilisez l'exemple suivant pour ajouter plusieurs `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres,

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *detector ID*. Définissez l'état pour EKS_ADDON_MANAGEMENT en tant que DISABLED. GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour tous les EKS clusters Amazon marqués avec la true paire GuardDuty Managed -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le detectorId correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active EKS_RUNTIME_MONITORING et désactive EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Gestion manuelle de l'agent de sécurité	1. Pour activer de manière sélective la surveillance du temps EKS d'exécution pour vos comptes membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *detector ID*. Définissez l'état pour `EKS_ADDON_MANAGEMENT` en tant que `DISABLED`. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI. L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le EKS cluster Amazon.

Migration de la surveillance du temps EKS d'exécution vers la surveillance du temps d'exécution

Avec le lancement de GuardDuty Runtime Monitoring, la couverture de détection des menaces a été étendue aux ECS conteneurs Amazon et aux EC2 instances Amazon. EKSL'expérience de surveillance du temps d'exécution est désormais consolidée dans la surveillance du temps d'exécution. Vous pouvez activer la surveillance du temps d'exécution et gérer des agents de GuardDuty sécurité individuels pour chaque type de ressource (EC2instance Amazon, ECS EKS cluster Amazon et cluster Amazon) dont vous souhaitez surveiller le comportement d'exécution.

GuardDuty a consolidé l'expérience de console pour la surveillance du EKS temps d'exécution dans la surveillance du temps d'exécution. GuardDuty recommande Vérifier l'état de configuration de EKS Runtime Monitoring etMigration de la surveillance du temps EKS d'exécution vers la surveillance du temps d'exécution.

Dans le cadre de la migration vers Runtime Monitoring, assurez-vous deDésactiver la surveillance de l'EKSexécution. Ceci est important car si vous choisissez ultérieurement de désactiver la surveillance du temps d'exécution et que vous ne le désactivez EKS pas, vous continuerez de devoir payer des frais d'utilisation pour EKS ce type de surveillance.

Pour passer de la surveillance du temps EKS d'exécution à la surveillance du temps d'exécution

1. La GuardDuty console prend en charge la surveillance du temps EKS d'exécution dans le cadre de la surveillance du temps d'exécution.

   Vous pouvez commencer à utiliser la surveillance du temps d'exécution Vérifier l'état de configuration de EKS Runtime Monitoring au niveau de votre organisation et de vos comptes.

   Assurez-vous de ne pas désactiver la surveillance du temps EKS d'exécution avant de l'activer. Si vous désactivez la surveillance du temps EKS d'exécution, la gestion des EKS modules complémentaires Amazon sera également désactivée. Procédez aux étapes suivantes dans l'ordre indiqué.
2. Assurez-vous de respecter tous lesConditions préalables à l'activation de la surveillance du temps d'exécution.
3. Activez la surveillance du temps d'exécution en répliquant les mêmes paramètres de configuration de l'organisation pour la surveillance du temps d'exécution que pour la surveillance du temps EKS d'exécution. Pour de plus amples informations, veuillez consulter Activer la surveillance du temps d'exécution.

- Si vous avez un compte autonome, vous devez activer la surveillance du temps d'exécution.

  Si votre agent GuardDuty de sécurité est déjà déployé, les paramètres correspondants sont automatiquement répliqués et vous n'avez pas besoin de les configurer à nouveau.
- Si votre organisation possède des paramètres d'activation automatique, veillez à reproduire les mêmes paramètres d'activation automatique pour la surveillance du temps d'exécution.
- Si vous avez une organisation dont les paramètres sont configurés individuellement pour les comptes de membres actifs existants, assurez-vous d'activer la surveillance du temps d'exécution et de configurer l'agent de GuardDuty sécurité pour ces membres individuellement.

4. Après avoir vérifié que les paramètres de surveillance du temps d'exécution et de l'agent de GuardDuty sécurité sont corrects, désactivez le contrôle du temps EKS d'exécution à l'aide de la commande API ou de la AWS CLI commande.
5. (Facultatif) Si vous souhaitez nettoyer les ressources associées à l'agent GuardDuty de sécurité, consultezImpact de la désactivation et du nettoyage des ressources.

Si vous souhaitez continuer à utiliser la surveillance du EKS temps d'exécution sans activer la surveillance du temps d'exécution, consultezConfiguration de la surveillance du temps EKS d'exécution (APIuniquement).

Vérifier l'état de configuration de EKS Runtime Monitoring

Utilisez les AWS CLI commandes suivantes APIs pour vérifier l'état de configuration existant de EKS Runtime Monitoring.

Pour vérifier l'état de la configuration existante de EKS Runtime Monitoring dans votre compte

- Exécutez GetDetectorpour vérifier l'état de configuration de votre propre compte.
- Vous pouvez également exécuter la commande suivante en utilisant AWS CLI :

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

  Assurez-vous de remplacer l'identifiant du détecteur de votre région Compte AWS et de la région actuelle. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

Pour vérifier l'état de la configuration existante de EKS Runtime Monitoring pour votre organisation (en tant que compte d' GuardDuty administrateur délégué uniquement)

- Exécutez DescribeOrganizationConfigurationpour vérifier l'état de configuration de votre organisation.

  Vous pouvez également exécuter la commande suivante à l'aide de AWS CLI :

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
  ```

  Assurez-vous de remplacer l'identifiant du détecteur par celui de votre compte d' GuardDuty administrateur délégué et de la région par votre région actuelle. Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

Désactivation de la surveillance de l'EKSexécution après la migration vers la surveillance du temps d'exécution

Après avoir vérifié que les paramètres existants de votre compte ou de votre organisation ont été répliqués dans Runtime Monitoring, vous pouvez désactiver EKS Runtime Monitoring.

Pour désactiver la surveillance du EKS temps d'exécution

- Pour désactiver la surveillance du temps EKS d'exécution dans votre propre compte

  Gérez le UpdateDetectorAPIavec votre propre région *`detector-id`*.

  Vous pouvez également utiliser la AWS CLI commande suivante. Remplacez *`12abc34d567e8fa901bc2d34e56789f0`* avec votre propre région *`detector-id`*.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
  ```

- Pour désactiver la surveillance du temps EKS d'exécution pour les comptes des membres de votre organisation

  Exécutez le UpdateMemberDetectorsAPIavec le régional *`detector-id`* du compte d' GuardDuty administrateur délégué de l'organisation.

Vous pouvez également utiliser la AWS CLI commande suivante. Remplacez *12abc34d567e8fa901bc2d34e56789f0* avec le régional *detector-id* du compte d' GuardDuty administrateur délégué de l'organisation et *111122223333* avec l' Compte AWS identifiant du compte membre pour lequel vous souhaitez désactiver cette fonctionnalité.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- Pour mettre à jour les paramètres d'activation automatique de EKS Runtime Monitoring pour votre organisation

  Effectuez l'étape suivante uniquement si vous avez configuré les paramètres d'activation automatique de EKS Runtime Monitoring pour les nouveaux (NEW) ou pour tous les (ALL) comptes membres de l'organisation. Si vous l'avez déjà configuré en tant queNONE, vous pouvez ignorer cette étape.

  > **Note**
  >
  > La configuration d'activation automatique de EKS Runtime Monitoring de telle EKS sorte que la surveillance du Runtime ne sera activée automatiquement pour aucun compte de membre existant ou lorsqu'un nouveau compte de membre rejoint votre organisation. NONE

  Exécutez le UpdateOrganizationConfigurationAPIavec le régional *detector-id* du compte d' GuardDuty administrateur délégué de l'organisation.

  Vous pouvez également utiliser la AWS CLI commande suivante. Remplacez *12abc34d567e8fa901bc2d34e56789f0* avec le régional *detector-id* du compte d' GuardDuty administrateur délégué de l'organisation. Remplacez le *EXISTING_VALUE* avec votre configuration actuelle pour l'activation automatique GuardDuty.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

Évaluation de la couverture d'exécution de vos ressources

Une fois que vous avez activé la surveillance du temps d'exécution et que l'agent de GuardDuty sécurité est déployé sur votre ressource, il GuardDuty fournit des statistiques de couverture pour le type de ressource correspondant et un état de couverture individuel pour les ressources appartenant à votre compte. L'état de couverture est déterminé en vérifiant que vous avez activé la surveillance du temps d'exécution, que votre point de VPC terminaison Amazon a été créé et que l'agent de GuardDuty sécurité pour la ressource correspondante a été déployé. Un état de couverture sain indique que lorsqu'un événement d'exécution est lié à votre ressource, GuardDuty vous êtes en mesure de recevoir ledit événement d'exécution via le point de VPC terminaison Amazon et de surveiller le comportement. En cas de problème lors de la configuration de Runtime Monitoring, de la création d'un point de VPC terminaison Amazon ou du déploiement de l'agent GuardDuty de sécurité, l'état de couverture apparaît comme étant « non fonctionnel ». Lorsque l'état de couverture est défaillant, il ne GuardDuty sera pas en mesure de recevoir ou de surveiller le comportement d'exécution de la ressource correspondante, ni de générer des résultats de surveillance du temps d'exécution.

Les rubriques suivantes vous aideront à consulter les statistiques de couverture, à configurer EventBridge les notifications et à résoudre les problèmes de couverture pour un type de ressource spécifique.

Table des matières

Couverture pour l'EC2instance Amazon

Pour une EC2 ressource Amazon, la couverture du temps d'exécution est évaluée au niveau de l'instance. Vos EC2 instances Amazon peuvent exécuter plusieurs types d'applications et de charges de travail, entre autres dans votre AWS environnement. Cette fonctionnalité prend également en charge les EC2 instances Amazon ECS gérées par Amazon et si vous avez des ECS clusters Amazon exécutés sur une EC2 instance Amazon, les problèmes de couverture au niveau de l'instance apparaîtront dans le cadre de la couverture EC2 d'exécution Amazon.

Rubriques

- Consultation des statistiques de couverture
- Configuration des notifications de modification de l'état de couverture
- Résolution des problèmes de couverture

Consultation des statistiques de couverture

Les statistiques de couverture pour les EC2 instances Amazon associées à vos propres comptes ou aux comptes de vos membres correspondent au pourcentage d'EC2instances saines par rapport à l'ensemble des EC2 instances sélectionnées Région AWS. L'équation suivante représente cela comme suit :

(Instances saines/Toutes les instances) *100

Si vous avez également déployé l'agent de GuardDuty sécurité pour vos ECS clusters Amazon, tout problème de couverture au niveau de l'instance associé aux ECS clusters Amazon exécutés sur une EC2 instance Amazon apparaîtra comme un problème de couverture du temps d'exécution des EC2 instances Amazon.

Choisissez l'une des méthodes d'accès pour consulter les statistiques de couverture de vos comptes.

Console

- Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
- Dans le volet de navigation, choisissez Runtime Monitoring.
- Choisissez l'onglet Couverture du temps d'exécution.
- Dans l'onglet Couverture du temps d'exécution de l'EC2instance, vous pouvez consulter les statistiques de couverture agrégées en fonction de l'état de couverture de chaque EC2 instance Amazon disponible dans le tableau de liste des instances.
  - Vous pouvez filtrer le tableau de la liste des instances selon les colonnes suivantes :
    - ID de compte
    - Type de gestion des agents
    - Version de l'agent
    - État de couverture
    - ID de l'instance
    - Cluster ARN

- Si l'état de couverture de l'une de vos EC2 instances est considéré comme étant insalubre, la colonne Problème contient des informations supplémentaires sur la raison de ce statut insalubre.

API/CLI

- Exécutez-le ListCoverageAPIavec votre propre identifiant de détecteur valide, votre région actuelle et votre point de terminaison de service. Vous pouvez filtrer et trier la liste des instances à l'aide de cette méthodeAPI.
  - Vous pouvez modifier l'exemple de `filter-criteria` à l'aide de l'une des options suivantes pour `CriterionKey` :
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`
  - Lorsque le `filter-criteria` inclut `RESOURCE_TYPE` comme EC2, Runtime Monitoring ne prend pas en charge l'utilisation de ISSUEcommeAttributeName. Si vous l'utilisez, la API réponse se traduira par`InvalidInputException`.

    Vous pouvez modifier l'exemple de `AttributeName` dans `sort-criteria` à l'aide des options suivantes :
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `INSTANCE_ID`
    - `UPDATED_AT`
  - Vous pouvez modifier le *`max-results`* (jusqu'à 50).
  - Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Exécutez le GetCoverageStatisticsAPIpour récupérer les statistiques agrégées de couverture en fonction dustatisticsType.
  - Vous pouvez modifier l'exemple de `statisticsType` sur l'une des options suivantes :
    - `COUNT_BY_COVERAGE_STATUS`— Représente les statistiques de couverture pour les EKS clusters agrégées par statut de couverture.
    - `COUNT_BY_RESOURCE_TYPE`— Statistiques de couverture agrégées en fonction du type de AWS ressource figurant dans la liste.
    - Vous pouvez modifier l'exemple de `filter-criteria` dans la commande. Vous pouvez utiliser les options suivantes pour `CriterionKey` :
      - `ACCOUNT_ID`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `AGENT_VERSION`
      - `MANAGEMENT_TYPE`
      - `INSTANCE_ID`
      - `CLUSTER_ARN`
  - Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Si l'état de couverture de votre EC2 instance est défectueux, consultezRésolution des problèmes de couverture.

Configuration des notifications de modification de l'état de couverture

L'état de couverture de votre EC2 instance Amazon peut apparaître comme étant insalubre. Pour savoir quand l'état de couverture change, nous vous recommandons de le surveiller régulièrement et de résoudre les problèmes s'il devient insalubre. Vous pouvez également créer une EventBridge règle Amazon pour recevoir une notification lorsque le statut de couverture passe de Malsain à Sain ou autre. Par défaut, il le GuardDuty publie dans le EventBridge bus pour votre compte.

Exemple de schéma de notification

Dans une EventBridge règle, vous pouvez utiliser les exemples d'événements et de modèles d'événements prédéfinis pour recevoir une notification de l'état de couverture. Pour plus d'informations sur la création d'une EventBridge règle, consultez la section Créer une règle dans le guide de EventBridge l'utilisateur Amazon.

En outre, vous pouvez créer un modèle d'événement personnalisé à l'aide de l'exemple de schéma de notification suivant. Assurez-vous de remplacer les valeurs de votre compte. Pour être averti lorsque le statut de couverture de votre EC2 instance Amazon passe de `Healthy` à`Unhealthy`, le `detail-type` *`GuardDuty Runtime Protection Unhealthy`*. Pour être averti lorsque le statut de couverture passe de `Unhealthy` à`Healthy`, remplacez la valeur de `detail-type` par *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Compte AWS ID",
  "time": "event timestamp (string)",
  "region": "Région AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
```

```
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Résolution des problèmes de couverture

Si l'état de couverture de votre EC2 instance Amazon n'est pas satisfaisant, vous pouvez en consulter la raison dans la colonne Problème.

Si votre EC2 instance est associée à un EKS cluster et que l'agent de sécurité EKS a été installé manuellement ou via une configuration automatique de l'agent, pour résoudre le problème de couverture, consultezCouverture pour les EKS clusters Amazon.

Le tableau suivant répertorie les types de problèmes et les étapes de résolution des problèmes correspondantes.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Aucun signalement par un agent	En attente de SSM notification	La réception de la SSM notification peut prendre quelques minutes. Assurez-vous que l'EC2instance Amazon est SSM gérée. Pour plus d'informations, consultez les étapes décrites dans la section Méthode 1 - À l'aide de AWS Systems Manager dansInstallation manuelle de l'agent de sécurité.
	(Vide exprès)	Si vous gérez l'agent GuardDuty de sécurité manuellement, assurez-vous d'avoir suivi les étapes ci-dessous sGestion manuelle de l'agent de sécurité pour une EC2 instance Amazon.

Type de problème	Message d'émission	Étapes de résolution des problèmes
		Si vous avez activé la configuration automatique des agents : • Votre EC2 instance est SSM gérée. • Consultez régulièrement le statut de votre agent de sécurité. Pour de plus amples informations, veuillez consulter Validation de l'état d'installation GuardDuty de l'agent de sécurité.
		Vérifiez que le VPC point de terminaison de votre EC2 instance Amazon est correctement configuré. Pour de plus amples informations, veuillez consulter Comment puis-je vérifier que la configuration du VPC point de terminaison est correcte ?.
		Si votre organisation dispose d'une politique de contrôle des services (SCP), vérifiez que la limite des autorisations ne restreint pas les `guardduty:SendSecurityTelemetry` autorisations. Pour de plus amples informations, veuillez consulter Validation de la politique de contrôle des services de votre organisation.
	Agent déconnecté	• Consultez le statut de votre agent de sécurité. Pour de plus amples informations, veuillez consulter Validation de l'état d'installation GuardDuty de l'agent de sécurité. • Consultez les journaux des agents de sécurité pour identifier la cause première potentielle. Les journaux fournissent des erreurs détaillées que vous pouvez utiliser pour résoudre le problème vous-même. Les fichiers journaux sont disponibles sous `/var/log/amzn-guardduty-agent/` . Fais `sudo journalctl -u amazon-guardduty-agent` .

Type de problème	Message d'émission	Étapes de résolution des problèmes
SSMLa création de l'association a échoué	GuardDuty SSMl'association existe déjà dans votre compte	1. Supprimez manuellement l'association existante. Pour plus d'informations, consultez la section Suppression d'associations dans le guide de AWS Systems Manager l'utilisateur. 2. Après avoir supprimé l'association, désactivez puis réactivez la configuration GuardDuty automatique de l'agent pour AmazonEC2.
	Votre compte comporte trop d'SSMassociations	Choisissez l'une des deux options suivantes : • Supprimez toutes les SSM associations non utilisées. Pour plus d'informations, consultez la section Suppression d'associations dans le guide de AWS Systems Manager l'utilisateur. • Vérifiez si votre compte est éligible à une augmentation de quota. Pour plus d'informations, consultez la section Quotas du service Systems Manager dans le Références générales AWS.
SSMLa mise à jour de l'association a échoué	GuardDuty SSMl'association n'existe pas dans votre compte	GuardDuty SSMl'association n'est pas présente dans votre compte. Désactivez puis réactivez la surveillance du temps d'exécution.
SSMLa suppression de l'association a échoué	GuardDuty SSMl'association n'existe pas dans votre compte	L'SSMassociation n'est pas présente dans votre compte. Si l'SSMassociation a été supprimée intentionnellement, aucune action n'est nécessaire.

Type de problème	Message d'émission	Étapes de résolution des problèmes
SSML'exécution de l'association d'instances a échoué	Les exigences architecturales ou autres prérequis ne sont pas respectés.	Pour plus d'informations sur les distributions de systèmes d'exploitation vérifiées, consultezConditions requises pour le support des EC2 instances Amazon. Si le problème persiste, les étapes suivantes vous aideront à l'identifier et éventuellement à le résoudre : 1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/. 2. Dans le volet de navigation, sous Gestion des nœuds, sélectionnez State Manager. 3. Filtrez par propriété Nom du document et entrez AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Sélectionnez l'ID d'association correspondant et consultez son historique d'exécution. 5. À l'aide de l'historique des exécutions, visualisez les échecs, identifiez la cause première potentielle et essayez de la résoudre.
VPCÉchec de la création du terminal	VPCla création de terminaux n'est pas prise en charge pour le partage VPC *vpcId*	La surveillance du temps d'exécution prend en charge l'utilisation d'un partage VPC au sein d'une organisation. Pour de plus amples informations, veuillez consulter Utilisation partagée VPC avec des agents de sécurité automatisés.

Type de problème	Message d'émission	Étapes de résolution des problèmes
	Uniquement lors de l'utilisation du partage VPC avec une configuration d'agent automatisée ID du compte du propriétaire *111122223333* pour le partage VPC *vpcId* n'a activé ni la surveillance du temps d'exécution, ni la configuration automatique des agents, ni les deux	Le compte VPC propriétaire partagé doit activer la surveillance du temps d'exécution et la configuration automatique des agents pour au moins un type de ressource (Amazon EKS ou Amazon ECS (AWS Fargate)). Pour de plus amples informations, veuillez consulter Prérequis spécifiques à la surveillance du temps d' GuardDutyexécution.

Type de problème	Message d'émission	Étapes de résolution des problèmes
	L'activation du DNS mode privé nécessite `enableDnsSupport` à la fois `enableDnsHostnames` VPC des attributs définis sur `true` *vpcId* (Service : Ec2, code d'état 400, numéro de demande : *a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*).	Assurez-vous que les VPC attributs suivants sont définis sur `true` — `enableDnsSupport` et`enableDnsHostnames` . Pour plus d'informations, consultez DNSles attributs de votre VPC. Si vous utilisez VPC la console Amazon https://console.aws.amazon.com/vpc/pour créer AmazonVPC, assurez-vous de sélectionner à la fois Activer les DNS noms d'hôte et Activer la DNS résolution. Pour plus d'informations, consultez VPCla section Options de configuration.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de la suppression du VPC terminal partagé	La suppressi on du point de VPC terminaison partagé n'est pas autorisée pour l'ID de compte *111122223 333* , partagé VPC *vpcId*, numéro de compte du propriétaire *555555555 555* .	Étapes potentielles : • La désactivation du statut de surveillance du temps d'exécution du compte VPC participant partagé n'a aucun impact sur la politique de point de VPC terminais on partagé ni sur le groupe de sécurité existant dans le compte propriétaire. Pour supprimer le point de VPC terminaison et le groupe de sécurité partagés, vous devez désactive r la surveillance du temps d'exécution ou l'état de configuration automatique de l'agent dans le compte VPC propriétaire partagé. • Le compte de VPC participant partagé ne peut pas supprimer le point de VPC terminaison partagé et le groupe de sécurité hébergés dans le compte de VPC propriétaire partagé.
L'agent ne fait pas de rapport	(Vide exprès)	Le type de problème a atteint la fin du support. Si le problème persiste et que ce n'est pas déjà fait, activez l'agent GuardDuty automatique pour AmazonEC2. Si le problème persiste, pensez à désactiver la surveilla nce du temps d'exécution pendant quelques minutes, puis réactivez-la.

Couverture pour les ECS clusters Amazon

La couverture d'exécution des ECS clusters Amazon inclut les tâches exécutées sur les instances de ECS conteneur Amazon AWS Fargate (Fargate) et les instances de conteneurs Amazon [1].

Pour un ECS cluster Amazon qui s'exécute sur Fargate, la couverture d'exécution est évaluée au niveau de la tâche. La couverture du ECS temps d'exécution des clusters inclut les tâches Fargate qui ont commencé à s'exécuter une fois que vous avez activé la surveillance du temps d'exécution

et la configuration automatisée des agents pour Fargate (uniquement). ECS Par défaut, une tâche Fargate est immuable. GuardDuty ne sera pas en mesure d'installer l'agent de sécurité pour surveiller les conteneurs sur les tâches déjà en cours d'exécution. Pour inclure une telle tâche Fargate, vous devez arrêter puis recommencer la tâche. Assurez-vous de vérifier si le service associé est pris en charge.

Pour plus d'informations sur le ECS conteneur Amazon, consultez la section Création de capacités.

Table des matières

Consultation des statistiques de couverture

Les statistiques de couverture ECS des ressources Amazon associées à votre propre compte ou à vos comptes de membres sont le pourcentage de ECS clusters Amazon sains par rapport à tous les ECS clusters Amazon sélectionnés Région AWS. Cela inclut la couverture des ECS clusters Amazon associés à la fois aux instances Fargate et EC2 Amazon. L'équation suivante représente cela comme suit :

(Clusters sains/Tous les clusters) x 100

Considérations

- Les statistiques de couverture du ECS cluster incluent l'état de couverture des tâches Fargate ECS ou des instances de conteneur associées à ce cluster. ECS L'état de couverture des tâches Fargate inclut les tâches qui sont en cours d'exécution ou dont l'exécution a récemment été terminée.
- Dans l'onglet Couverture d'exécution du ECS cluster, le champ Instances de conteneur couvertes indique l'état de couverture des instances de conteneur associées à votre ECS cluster Amazon.

  Si votre ECS cluster Amazon contient uniquement des tâches Fargate, le nombre s'affiche sous la forme 0/0.
- Si votre ECS cluster Amazon est associé à une EC2 instance Amazon qui ne dispose pas d'un agent de sécurité, le ECS cluster Amazon aura également un statut de couverture défaillant.

Pour identifier et résoudre le problème de couverture de l'EC2instance Amazon associée, consultez la section relative Résolution des problèmes de couverture aux EC2 instances Amazon.

Choisissez l'une des méthodes d'accès pour consulter les statistiques de couverture de vos comptes.

Console

- Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
- Dans le volet de navigation, choisissez Runtime Monitoring.
- Choisissez l'onglet Couverture du temps d'exécution.
- Dans l'onglet Couverture d'exécution des ECS clusters, vous pouvez consulter les statistiques de couverture agrégées en fonction de l'état de couverture de chaque ECS cluster Amazon disponible dans le tableau de liste des clusters.
  - Vous pouvez filtrer le tableau de liste des clusters selon les colonnes suivantes :
    - ID de compte
    - Nom du cluster
    - Type de gestion des agents
    - État de couverture
- Si l'état de couverture de l'un de vos ECS clusters Amazon est considéré comme insalubre, la colonne Problème inclut des informations supplémentaires sur la raison de ce statut insalubre.

  Si vos ECS clusters Amazon sont associés à une EC2 instance Amazon, accédez à l'onglet Couverture du EC2 temps d'exécution de l'instance et filtrez par le champ Nom du cluster pour afficher le problème associé.

API/CLI

- Exécutez-le ListCoverageAPIavec votre propre identifiant de détecteur valide, votre région actuelle et votre point de terminaison de service. Vous pouvez filtrer et trier la liste des instances à l'aide de cette méthodeAPI.
  - Vous pouvez modifier l'exemple de `filter-criteria` à l'aide de l'une des options suivantes pour `CriterionKey` :
    - `ACCOUNT_ID`

- ECS_CLUSTER_NAME
- COVERAGE_STATUS
- MANAGEMENT_TYPE

- Vous pouvez modifier l'exemple de `AttributeName` dans `sort-criteria` à l'aide des options suivantes :
  - ACCOUNT_ID
  - COVERAGE_STATUS
  - ISSUE
  - ECS_CLUSTER_NAME
  - UPDATED_AT

    Le champ est mis à jour uniquement lorsqu'une nouvelle tâche est créée dans le ECS cluster Amazon associé ou en cas de modification du statut de couverture correspondant.
- Vous pouvez modifier le *`max-results`* (jusqu'à 50).
- Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Exécutez le GetCoverageStatisticsAPIpour récupérer les statistiques agrégées de couverture en fonction du`statisticsType`.
  - Vous pouvez modifier l'exemple de `statisticsType` sur l'une des options suivantes :
    - COUNT_BY_COVERAGE_STATUS— Représente les statistiques de couverture pour les ECS clusters agrégées par statut de couverture.
    - COUNT_BY_RESOURCE_TYPE— Statistiques de couverture agrégées en fonction du type de AWS ressource figurant dans la liste.
    - Vous pouvez modifier l'exemple de `filter-criteria` dans la commande. Vous pouvez utiliser les options suivantes pour `CriterionKey` :
      - ACCOUNT_ID

- `ECS_CLUSTER_NAME`
- `COVERAGE_STATUS`
- `MANAGEMENT_TYPE`
- `INSTANCE_ID`

- Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Pour plus d'informations sur les problèmes de couverture, consultezRésolution des problèmes de couverture.

Configuration des notifications de modification de l'état de couverture

L'état de couverture de votre ECS cluster Amazon peut apparaître comme étant insalubre. Pour savoir quand l'état de couverture change, nous vous recommandons de le surveiller régulièrement et de résoudre les problèmes s'il devient insalubre. Vous pouvez également créer une EventBridge règle Amazon pour recevoir une notification lorsque le statut de couverture passe de Malsain à Sain ou autre. Par défaut, il le GuardDuty publie dans le EventBridge bus pour votre compte.

Exemple de schéma de notification

Dans une EventBridge règle, vous pouvez utiliser les exemples d'événements et de modèles d'événements prédéfinis pour recevoir une notification de l'état de couverture. Pour plus d'informations sur la création d'une EventBridge règle, consultez la section Créer une règle dans le guide de EventBridge l'utilisateur Amazon.

En outre, vous pouvez créer un modèle d'événement personnalisé à l'aide de l'exemple de schéma de notification suivant. Assurez-vous de remplacer les valeurs de votre compte. Pour être averti lorsque le statut de couverture de votre ECS cluster Amazon passe de `Healthy` à`Unhealthy`, le `detail-type` *`GuardDuty Runtime Protection Unhealthy`*. Pour être averti lorsque le statut de couverture passe de `Unhealthy` à`Healthy`, remplacez la valeur de `detail-type` par *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Compte AWS ID",
  "time": "event timestamp (string)",
  "region": "Région AWS",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Résolution des problèmes de couverture

Si l'état de couverture de votre ECS cluster Amazon n'est pas satisfaisant, vous pouvez en connaître la raison dans la colonne Problème.

Le tableau suivant fournit les étapes de résolution recommandées pour les problèmes liés à Fargate (ECSAmazon uniquement). Pour plus d'informations sur les problèmes de couverture des EC2

instances Amazon, consultez Résolution des problèmes de couverture la section relative aux EC2 instances Amazon.

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
L'agent ne fait pas de rapport	L'agent ne présente pas de rapports pour les tâches dans `TaskDefinition - '` *`TASK_DEFINITION`* `'`	Vérifiez que le VPC point de terminaison pour la tâche de votre ECS cluster Amazon est correctement configuré . Pour de plus amples informations, veuillez consulter Comment puis-je vérifier que la configuration du VPC point de terminaison est correcte ?. Si votre organisation dispose d'une politique de contrôle des services (SCP), vérifiez que la limite des autorisations ne restreint pas les `guardduty:SendSecurityTelemetry` autorisations. Pour de plus amples informations, veuillez consulter Validation de la politique de contrôle des services de votre organisation.
	`VPC_ISSUE` `; for task in TaskDefinition - '` *`TASK_DEFINITION`* `'`	Consultez les détails du VPC problème dans les informations supplémentaires.
L'agent est sorti	ExitCode: `EXIT_CODE` pour les tâches dans `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Consultez les détails du problème dans les informations supplémentaires.
	Motif : *`REASON`* pour les tâches dans `TaskDefin`	

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
	`ition - ' TASK_DEFINITION '`	
	ExitCode: `EXIT_CODE` avec raison : »*EXIT_CODE* 'pour les tâches dans `TaskDefinition - 'TASK_DEFINITION '`	

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées

	L'agent est sorti : Raison `CannotPullContainerError` : le manifeste de l'image d'extraction a été réessayé...	Le rôle d'exécution des tâches doit disposer des autorisations Amazon Elastic Container Registry (AmazonECR) suivantes :
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		Pour de plus amples informations, veuillez consulter Fournir ECR les autorisations et les détails du sous-réseau.
		Après avoir ajouté les ECR autorisations Amazon, vous devez redémarrer la tâche.
		Si le problème persiste, consultezMon AWS Step Functions flux de travail échoue de façon inattendue.

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
VPCÉchec de la création du terminal	L'activation du DNS mode privé nécessite `enableDnsSupport` à la fois `enableDnsHostnames` VPC des attributs définis sur `true` *`vpcId`* (Service :ECS, code d'état 400, numéro de demande : *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assurez-vous que les VPC attributs suivants sont définis sur `true` — `enableDnsSupport` et`enableDnsHostnames` . Pour plus d'informations, consultez DNSles attributs dans votre VPC. Si vous utilisez VPC la console Amazon https://console.aws.amazon.com/vpc/pour créer AmazonVPC, assurez-vous de sélectionner à la fois Activer les DNS noms d'hôte et Activer la DNS résolution. Pour plus d'informations, consultez VPCla section Options de configuration.
Agent non provisionné	Invocation non prise en charge par *`SERVICE`* for task (s) dans `TaskDefinition - '` *`TASK_DEFINITION`* `'`	Cette tâche a été invoquée par une personne *`SERVICE`* qui n'est pas prise en charge.
	CPUArchitecture non prise en charge '*`TYPE`*'pour les tâches dans `TaskDefinition - '` *`TASK_DEFINITION`* `'`	Cette tâche est exécutée sur une CPU architecture non prise en charge. Pour plus d'informations sur les CPU architectures prises en charge, consultez Validation des exigences architecturales.
	`TaskExecutionRole` absent de `TaskDefinition - '`*`TASK_DEFINITION`* `'`	Le rôle d'exécution de la ECS tâche est absent. Pour plus d'informations sur la fourniture du rôle d'exécution des tâches et des autorisations requises, consultez Fournir ECR les autorisations et les détails du sous-réseau.

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
	Configuration réseau « *CONFIGURATION_DETAILS* » manquante pour les tâches dans `TaskDefinition - '` *TASK_DEFINITION* `'`	Des problèmes de configuration réseau peuvent survenir en raison d'une VPC configuration manquante ou de sous-réseaux manquants ou vides. Vérifiez que la configuration de votre réseau est correcte. Pour de plus amples informations, veuillez consulter Fournir ECR les autorisations et les détails du sous-réseau. Pour plus d'informations, consultez les paramètres de définition des ECS tâches Amazon dans le manuel Amazon Elastic Container Service Developer Guide.

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
Autres	Problème non identifié, pour les tâches dans `TaskDefinition - 'TASK_DEFINITION '`	Utilisez les questions suivantes pour identifier la cause première du problème : • La tâche a-t-elle démarré avant que vous n'activiez le Runtime Monitoring ? Sur AmazonECS, les tâches sont immuables. Pour évaluer le comportement d'exécution d'une tâche Fargate en cours d'exécution, assurez-vous que la surveillance du temps d'exécution est déjà activée, puis redémarrez la tâche GuardDuty pour ajouter le sidecar du conteneur. • Cette tâche fait-elle partie d'un déploiement de service qui a débuté avant que vous n'activiez le Runtime Monitoring ? Dans l'affirmative, vous pouvez redémarrer le service ou le mettre à jour `forceNewDeployment` en suivant les étapes décrites dans la section Mettre à jour un service. Vous pouvez également utiliser UpdateServiceou AWS CLI. • La tâche a-t-elle été lancée après avoir exclu le ECS cluster de la surveillance du temps d'exécution ? Lorsque vous modifiez la GuardDuty balise prédéfinie de `GuardDuty`

Type de problème	Informations supplémentaires	Étapes de dépannage recommandées
		`Managed - true` à `GuardDuty Managed -false`, il ne GuardDuty recevra pas les événements d'exécution pour le ECS cluster. • Votre service contient-il une tâche dont l'ancien format est `taskArn` ? GuardDuty Runtime Monitoring ne prend pas en charge la couverture des tâches dont l'ancien format est`taskArn`. Pour plus d'informations sur Amazon Resource Names (ARNs) pour les ECS ressources Amazon, consultez Amazon Resource Names (ARNs) et IDs.

Couverture pour les EKS clusters Amazon

Après avoir activé la surveillance du temps d'exécution et installé l'agent de GuardDuty sécurité (module complémentaire) manuellement EKS ou par le biais d'une configuration automatique de l'agent, vous pouvez commencer à évaluer la couverture de vos EKS clusters.

Table des matières

Consultation des statistiques de couverture

Les statistiques de couverture pour les EKS clusters associés à vos propres comptes ou à vos comptes membres sont le pourcentage de EKS clusters sains par rapport à tous les EKS clusters sélectionnés Région AWS. L'équation suivante représente cela comme suit :

(Clusters sains/Tous les clusters) x 100

Choisissez l'une des méthodes d'accès pour consulter les statistiques de couverture de vos comptes.

Console

- Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
- Dans le volet de navigation, choisissez Runtime Monitoring.
- Choisissez l'onglet Couverture d'exécution des EKS clusters.
- Dans l'onglet Couverture d'exécution des EKS clusters, vous pouvez consulter les statistiques de couverture agrégées selon l'état de couverture disponible dans le tableau de liste des clusters.
  - Vous pouvez filtrer le tableau Liste des clusters selon les colonnes suivantes :
    - Nom du cluster
    - ID de compte
    - Type de gestion des agents
    - État de couverture
    - Version du module complémentaire
- Si l'état de couverture de l'un de vos EKS clusters est insalubre, la colonne Problème peut inclure des informations supplémentaires sur la raison de ce statut insalubre.

API/CLI

- Exécutez-le ListCoverageAPIavec votre propre identifiant de détecteur, votre région et votre point de terminaison de service valides. Vous pouvez filtrer et trier la liste des clusters à l'aide de cette méthodeAPI.
  - Vous pouvez modifier l'exemple de `filter-criteria` à l'aide de l'une des options suivantes pour `CriterionKey` :
    - `ACCOUNT_ID`

    - CLUSTER_NAME
    - RESOURCE_TYPE
    - COVERAGE_STATUS
    - ADDON_VERSION
    - MANAGEMENT_TYPE
  - Vous pouvez modifier l'exemple de AttributeName dans sort-criteria à l'aide des options suivantes :
    - ACCOUNT_ID
    - CLUSTER_NAME
    - COVERAGE_STATUS
    - ISSUE
    - ADDON_VERSION
    - UPDATED_AT
  - Vous pouvez modifier le *max-results* (jusqu'à 50).
  - Pour trouver le detectorId correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Exécutez le GetCoverageStatisticsAPIpour récupérer les statistiques agrégées de couverture en fonction dustatisticsType.
  - Vous pouvez modifier l'exemple de statisticsType sur l'une des options suivantes :
    - COUNT_BY_COVERAGE_STATUS— Représente les statistiques de couverture pour les EKS clusters agrégées par statut de couverture.
    - COUNT_BY_RESOURCE_TYPE— Statistiques de couverture agrégées en fonction du type de AWS ressource figurant dans la liste.
    - Vous pouvez modifier l'exemple de filter-criteria dans la commande. Vous pouvez utiliser les options suivantes pour CriterionKey :
      - ACCOUNT_ID

    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`
- Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Si l'état de couverture de votre EKS cluster n'est pas satisfaisant, consultezRésolution des problèmes de EKS couverture.

Configuration des notifications de modification de l'état de couverture

L'état de couverture d'un EKS cluster de votre compte peut être indiqué comme étant insalubre. Pour détecter les cas où l'état de couverture devient Défectueux, nous vous recommandons de surveiller régulièrement l'état de couverture et de résoudre les problèmes, si l'état est Défectueux Vous pouvez également créer une EventBridge règle Amazon pour vous avertir lorsque le statut de couverture passe de `Healthy` ou non `Unhealthy` à. Par défaut, il le GuardDuty publie dans le EventBridgebus pour votre compte.

Exemple de schéma de notification

Dans une EventBridge règle, vous pouvez utiliser les exemples d'événements et de modèles d'événements prédéfinis pour recevoir une notification de l'état de couverture. Pour plus d'informations sur la création d'une EventBridge règle, consultez la section Créer une règle dans le guide de EventBridge l'utilisateur Amazon.

En outre, vous pouvez créer un modèle d'événement personnalisé à l'aide de l'exemple de schéma de notification suivant. Assurez-vous de remplacer les valeurs de votre compte. Pour être averti lorsque le statut de couverture de votre EKS cluster Amazon passe de `Healthy` à`Unhealthy`, le `detail-type` *`GuardDuty Runtime Protection Unhealthy`*. Pour être averti lorsque le

statut de couverture passe de `Unhealthy` à`Healthy`, remplacez la valeur de `detail-type` par *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Compte AWS ID",
  "time": "event timestamp (string)",
  "region": "Région AWS",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Résolution des problèmes de EKS couverture

Si l'état de couverture de votre EKS cluster est le suivant`Unhealthy`, vous pouvez afficher l'erreur correspondante soit dans la colonne Problème de la GuardDuty console, soit en utilisant le type de CoverageResourcedonnées.

Lorsque vous utilisez des balises d'inclusion ou d'exclusion pour surveiller vos EKS clusters de manière sélective, la synchronisation des balises peut prendre un certain temps. Cela peut avoir un impact sur l'état de couverture du EKS cluster associé. Vous pouvez réessayer de supprimer et

d'ajouter la balise correspondante (inclusion ou exclusion). Pour plus d'informations, consultez la section Marquage de vos EKS ressources Amazon dans le guide de l'EKSutilisateur Amazon.

La structure d'un problème de couverture est `Issue type:Extra information`. Généralement, les problèmes comportent des informations supplémentaires facultatives qui peuvent inclure une exception spécifique côté client ou une description du problème. Sur la base d'informations supplémentaires, les tableaux suivants fournissent les étapes recommandées pour résoudre les problèmes de couverture de vos EKS clusters.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
La création de l'addon a échoué	L'addon n'`aws-guardduty-agent` est pas compatible avec la version actuelle du cluster *`ClusterName`* . L'addon spécifié n'est pas pris en charge.	Assurez-vous que vous utilisez l'une de ces versions de Kubernetes prenant en charge le déploiement du module complémentaire. `aws-guardduty-agent` EKS Pour de plus amples informations, veuillez consulter Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty . Pour plus d'informations sur la mise à jour de votre version de Kubernetes, consultez Mettre à jour une version de Kubernetes d'un EKS cluster Amazon.
La création de l'addon a échoué Échec de la mise à jour de l'addon État de l'addon malsain	EKSProblème lié à l'addon - : `AddonIssueCode` `AddonIssueMessage`	Pour plus d'informations sur les étapes recommandées pour un code de problème

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
		spécifique à un module complémentaire, consultezTroubleshooting steps for Addon creation/ updatation error with Addon issue code. Pour obtenir la liste des codes d'erreur liés aux modules complémentaires que vous pourriez rencontrer dans le cadre de ce problème, consultez AddonIssue.
VPCÉchec de la création du terminal	VPCla création de terminaux n'est pas prise en charge pour le partage VPC *vpcId*	Runtime Monitoring prend désormais en charge l'utilisation d'un partage VPC au sein d'une organisation. Assurez-vous que vos comptes répondent à tous les prérequis. Pour de plus amples informations, veuillez consulter Conditions préalables à l'utilisation du partage VPC.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
	Uniquement lors de l'utilisation du partage VPC avec une configuration d'agent automatisée ID du compte du propriétaire *111122223333* pour le partage VPC *vpcId* n'a activé ni la surveillance du temps d'exécution, ni la configuration automatique des agents, ni les deux.	Le compte VPC propriétaire partagé doit activer la surveillance du temps d'exécution et la configuration automatique des agents pour au moins un type de ressource (Amazon EKS ou Amazon ECS (AWS Fargate)). Pour de plus amples informations, veuillez consulter Prérequis spécifiques à la surveillance du temps d'GuardDutyexécution.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
	L'activation du DNS mode privé nécessite `enableDnsSupport` à la fois `enableDnsHostnames` VPC des attributs définis sur `true` *`vpcId`* (Service : Ec2, code d'état 400, numéro de demande : *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assurez-vous que les VPC attributs suivants sont définis sur `true` — `enableDnsSupport` et`enableDnsHostnames` . Pour plus d'informations, consultez DNSles attributs dans votre VPC. Si vous utilisez VPC la console Amazon https://console.aws.amazon.com/vpc/pour créer AmazonVPC, assurez-vous de sélectionner à la fois Activer les DNS noms d'hôte et Activer la DNS résolution. Pour plus d'informations, consultez VPCla section Options de configuration.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
Échec de la suppression du VPC terminal partagé	La suppression du point de VPC terminaison partagé n'est pas autorisée pour l'ID de compte *111122223333* , partagé VPC *vpcId*, numéro de compte du propriétaire *555555555555* .	Étapes potentielles : • La désactivation du statut de surveillance du temps d'exécution du compte VPC participant partagé n'a aucun impact sur la politique de point de VPC terminaison partagé ni sur le groupe de sécurité existant dans le compte propriétaire. Pour supprimer le point de VPC terminaison et le groupe de sécurité partagés, vous devez désactiver la surveillance du temps d'exécution ou l'état de configuration automatique de l'agent dans le compte VPC propriétaire partagé. • Le compte de VPC participant partagé ne peut pas supprimer le point de VPC terminaison partagé et le groupe de sécurité hébergés dans le compte de VPC propriétaire partagé.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
EKSClusters locaux	EKSles addons ne sont pas pris en charge sur les clusters d'avant-postes locaux.	Non exploitable. Pour plus d'informations, consultez Amazon EKS sur les AWS avant-postes.
EKSAutorisation d'activation de la surveillance du temps d'exécution non accordée	(peut afficher ou non des informations supplémentaires)	1. Si des informations supplémentaires sont disponibles pour ce problème, corrigez la cause première et passez à l'étape suivante. 2. Activez la surveillance du temps EKS d'exécution pour la désactiver puis la réactiver. Assurez-vous que l' GuardDuty agent est également déployé, que ce soit automatiquement GuardDuty ou manuellement.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
EKSSurveillance du temps d'exécution : activation du provisionnement des ressources en cours	(peut afficher ou non des informations supplémentaires)	Non exploitable. Une fois que vous avez activé la surveillance du temps EKS d'exécution, l'état de couverture peut être maintenu `Unhealthy` jusqu'à la fin de l'étape de provisionnement des ressources. L'état de couverture est surveillé et mis à jour périodiquement.
Autres (tout autre problème)	Erreur due à un échec d'autorisation	Activez la surveillance du temps EKS d'exécution pour la désactiver puis la réactiver. Assurez-vous que l' GuardDuty agent est également déployé, automatiquement GuardDuty ou manuellement.

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
EKSProblème d'extension - `InsufficientNumberOfReplicas` : L'extension n'est pas saine car elle ne contient pas le nombre de répliques souhaité.	• À l'aide du message du problème, vous pouvez identifier et corriger la cause première. Vous pouvez commencer par décrire votre cluster. Par exemple, `kubectl`

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
	`describe pods`à utiliser pour identifier la cause première de la défaillance du pod. Après avoir corrigé la cause première, réessayez l'étape (création ou mise à jour d'un module complémentaire). • Si le problème persiste, vérifiez que le VPC point de terminaison de votre EKS cluster Amazon est correctement configuré. Pour de plus amples informations, veuillez consulter Comment puis-je vérifier que la configuration du VPC point de terminaison est correcte ?.
EKSProblème d'addon - `Admission RequestDenied` : le webhook d'admissi on `"validate.kyverno.svc-fail"` a refusé la demande : politique de violation `DaemonSet/amazon-guardduty/ aws-guardduty-agent` des ressource s : : restrict-image-registries :... `autogen-v alidate-registries`	1. Le EKS cluster Amazon ou l'administrateur de sécurité doivent revoir la politique de sécurité qui bloque la mise à jour de l'addon. 2. Vous devez soit désactiver le contrôleur (webhook), soit lui demander d'accepter les demandes d'AmazonEKS.
EKSProblème d'extension - `Configura tionConflict` : Conflits détectés lors de la tentative de candidature. Ne continuer a pas en raison du mode résolution des conflits. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.tem plate.spec.containers[name= "aws-guardduty-agent"].image`	Lors de la création ou de la mise à jour de l'addon, fournissez l'indicateur de `OVERWRITE` résolution des conflits. Cela remplacer a potentiellement toutes les modifications apportées directement aux ressources associées dans Kubernetes à l'aide de Kubernetes. API Vous pouvez d'abord supprimer l'addon, puis le réinstaller.

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes

EKSProblème lié à l'addon - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Vous devez ajouter `eks:addon-cluster-admin ClusterRoleBinding` manuellement l'autorisation manquante. Ajoutez ce qui suit `yaml` à `eks:addon-cluster-admin` :
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	Vous pouvez désormais l'appliquer `yaml` à votre EKS cluster Amazon à l'aide de la commande suivante :
	`kubectl apply -f eks-addon-cluster-admin.yaml`

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
EKSProblème lié à l'addon - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Vous devez soit désactiver le contrôleur, soit lui demander d'accepter les demandes du EKS cluster Amazon. Avant de créer ou de mettre à jour le module complémentaire, vous pouvez également créer un espace de GuardDuty noms et l'étiqueter comme `owner` suit.

Questions fréquemment posées (FAQs)

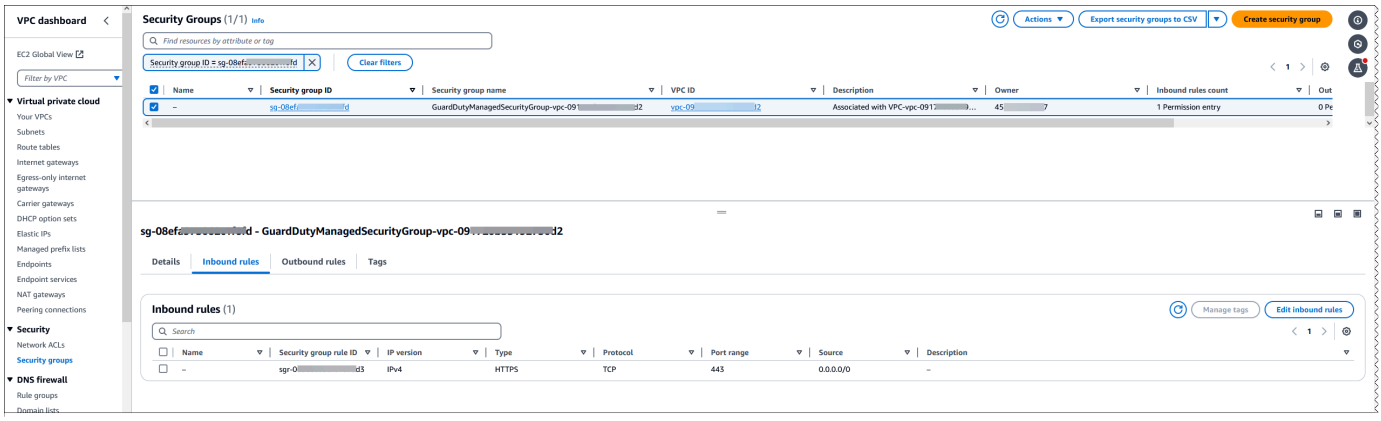
Table des matières

Comment puis-je vérifier que la configuration du VPC point de terminaison est correcte ?

Suivez les étapes suivantes pour vérifier que la configuration du VPC point de terminaison correspondant à votre type de ressource est correctement configurée dans le compte VPC propriétaire :

1. Connectez-vous à la VPC console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sous Cloud privé virtuel, choisissez Points de terminaison.

3. Dans le tableau Endpoints, sélectionnez la ligne dont le nom du service est similaire à com.amazonaws.***us-east-1***.guardduty-data. La région (`us-east-1`) peut être différente pour votre terminal.
4. Un panneau contenant les détails du point de terminaison apparaîtra. Sous l'onglet Groupes de sécurité, sélectionnez le lien ID de groupe associé pour plus de détails.
5. Dans le tableau des groupes de sécurité, sélectionnez la ligne associée à l'ID du groupe de sécurité pour afficher les détails.
6. Dans l'onglet Règles entrantes, assurez-vous qu'il existe une politique d'entrée avec la plage de ports 443 et la source 0.0.0.0/0. Les règles de trafic entrant contrôlent le trafic entrant autorisé à atteindre l'instance. L'image suivante montre les règles entrantes pour un groupe de sécurité associé à celui VPC utilisé par l'agent GuardDuty de sécurité.



Si vous ne possédez pas encore de groupe de sécurité dont le port entrant 443 est activé, créez un groupe de sécurité dans le guide de l'EC2utilisateur Amazon.

En cas de problème lors de la restriction des autorisations entrantes à votre VPC (ou à votre cluster), fournissez le support au port 443 entrant depuis n'importe quelle adresse IP (0.0.0.0/0).

Pourquoi le statut de couverture de ma ressource s'applique-t-il **`Unhealthy`** ?

Si vous venez de déployer l'agent de GuardDuty sécurité (soit par le biais d'une configuration automatique de l'agent, soit manuellement) ou si vous avez suivi les étapes recommandées pour résoudre un problème de couverture, le rétablissement de l'état de couverture peut prendre quelques minutes. Vous pouvez vérifier régulièrement l'état de la couverture ou configurer Amazon EventBridge (EventBridge) pour recevoir une notification lorsque le statut de couverture change.

En outre, vous pouvez également vérifier que la configuration du VPC point de terminaison de votre ressource est correcte. Pour de plus amples informations, veuillez consulter Comment puis-je vérifier que la configuration du VPC point de terminaison est correcte ?.

Qui peut consulter l'état de la couverture d'exécution d'une ressource qui m'appartient Compte AWS ?

En tant que compte membre ou compte autonome, vous pouvez consulter les statistiques de couverture des ressources associées à vos propres comptes. En tant que compte GuardDuty administrateur délégué d'une organisation, vous pouvez consulter les statistiques de couverture des ressources associées à votre compte et des comptes de membres appartenant à votre organisation.

Comment puis-je vérifier si l'agent GuardDuty de sécurité est en cours d'exécution sur une tâche Fargate ?

L'agent GuardDuty de sécurité fonctionne comme un conteneur annexe pour les tâches Fargate.

Choisissez une méthode préférée pour valider si le conteneur du sidecar est affiché pendant l'exécution de la tâche.

Amazon ECS console

1. Ouvrez la console à la https://console.aws.amazon.com/ecs/version 2.
2. Dans le panneau de navigation, choisissez Clusters.
3. Sur la page Clusters, sélectionnez le nom du cluster associé pour plus de détails.
4. Choisissez l'onglet Tasks.
5. Sélectionnez le lien de tâche associé pour afficher les détails de la tâche.
6. Sur la page des détails des tâches, le tableau Conteneurs inclut les détails du sidecar. L'ID d'exécution du conteneur aura un préfixe correspondant à votre identifiant de tâche.

CLI

Exécutez `describe-tasks` et recherchez le conteneur dont le nom est défini sur `aws-gd-agent` et lastStatusdéfini sur`RUNNING`.

L'exemple suivant montre la sortie du cluster par défaut pour la tâche `aws:ecs:`*`us-east-1`*`:`*`123456789012`*`:`*`task/0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE`*

Sortie

Le conteneur nommé aws-gd-agentest dans l'RUNNINGétat.

```
"containers": [
      {
        "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/4df26bb4-
f057-467b-a079-96167EXAMPLE",
        "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/0b69d5c0-
d655-4695-98cd-5d2d5EXAMPLE",
        "lastStatus": "RUNNING",
        "healthStatus": "UNKNOWN",
        "memory": "1 GB",
        "name": "aws-gd-agent"
      }
    ]
```

Pour plus d'informations, consultez describe-tasks.

Autres questions de résolution des problèmes

Pour d'autres questions de résolution des problèmes concernant vos tâches Fargate, consultez la section Résolution des problèmes liés à la surveillance du temps d'exécution FAQs dans le manuel Amazon Elastic Container Service Developer Guide.

Configuration CPU et surveillance de la mémoire

Après avoir activé la surveillance du temps d'exécution et vérifié que l'état de couverture de votre cluster est sain, vous pouvez configurer et consulter les indicateurs d'analyse.

Les rubriques suivantes peuvent vous aider à évaluer les performances de l'agent déployé par rapport aux limites de mémoire CPU et de mémoire de l' GuardDuty agent.

Configuration de la surveillance sur le ECS cluster Amazon

Les étapes suivantes du guide de l' CloudWatch utilisateur Amazon peuvent vous aider à évaluer les performances de l'agent déployé par rapport aux limites de mémoire CPU et de mémoire de l' GuardDuty agent :

1. Configuration de Container Insights sur Amazon ECS pour les métriques relatives aux clusters et aux niveaux de service
2. Statistiques d'Amazon ECS Container Insights

Configuration de la surveillance sur le EKS cluster Amazon

Une fois que l'agent de GuardDuty sécurité a été déployé et que vous avez déterminé que l'état de couverture de votre cluster est sain, vous pouvez configurer et consulter les métriques Container Insight.

Évaluer les performances de l'agent de sécurité

1. Configuration de Container Insights sur Amazon EKS et Kubernetes dans le guide de l'utilisateur Amazon CloudWatch
2. Les statistiques d'Amazon EKS et de Kubernetes Container Insights dans le guide de l'utilisateur Amazon CloudWatch

Gérez les performances avec l'agent de sécurité v1.5.0 et versions ultérieures

> Avec l'agent de sécurité v1.5.0 et versions ultérieures, lorsque les informations indiquent que l' GuardDuty agent associé atteint les limites assignées, vous pouvez configurer des paramètres spécifiques. Pour de plus amples informations, veuillez consulter Configurer les paramètres des EKS modules complémentaires.

Types d'événements d'exécution collectés qui GuardDuty utilisent

L'agent GuardDuty de sécurité collecte les types d'événements suivants et les envoie au GuardDuty backend à des fins de détection et d'analyse des menaces. GuardDuty ne vous permet pas d'accéder à ces événements. En cas GuardDuty de détection d'une menace potentielle et de génération d'un résultat de surveillance du temps d'exécution, vous pouvez consulter les détails de la découverte correspondante. Pour plus d'informations sur l' GuardDuty utilisation des types d'événements collectés, consultezRefus d’utiliser vos données pour améliorer le service.

Événements de processus

Nom de champ	Description
Nom du processus	Nom du processus observé.

Nom de champ	Description
Chemin d'accès du processus	Chemin absolu de l'exécutable du processus.
ID du processus.	ID attribué au processus par le système d'exploitation.
Espace de noms PID	ID de processus du processus dans un espace de PID noms secondaire autre que l'espace de PID noms au niveau de l'hôte. Pour les processus se trouvant à l'intérieur d'un conteneur, il s'agit de l'ID de processus observé à l'intérieur du conteneur.
ID d'utilisateur du processus	ID unique de l'utilisateur qui a exécuté le processus.
Procédé UUID	L'identifiant unique attribué au processus par GuardDuty.
Procédé GID	ID de processus du groupe de processus.
Procédé EGID	ID de groupe effectif du groupe de processus.
Procédé EUID	ID utilisateur effectif du processus.
Nom d'utilisateur du processus	Nom d'utilisateur qui a exécuté le processus.
Heure de début du processus	L'heure de création du processus. Ce champ est au format de chaîne de UTC date (`2023-03-22T19:37:20.168Z`).
Exécutable du processus SHA -256	Hachage `SHA256` de l'exécutable du processus .
Chemin du script de processus	Chemin du fichier de script qui a été exécuté.
Variable d'environnement de processus	Variable d'environnement mise à la dispositi on du processus. Seuls `LD_PRELOAD` et `LD_LIBRARY_PATH` sont collectés.

Nom de champ	Description
Répertoire de travail Process Present (PWD)	Référentiel de travail actuel du processus.
Processus parent	Détails de processus du processus parent. Un processus parent est un processus qui a créé le processus observé.
Arguments de ligne de commande Actuellement, ce champ est limité à des versions d'agent spécifiques correspondant au type de ressource : • Fargate (ECSAmazon uniquement GuardDuty) avec l'agent de sécurité v1.0.0 et versions ultérieures. • EC2Instances Amazon avec agent GuardDuty de sécurité v1.0.0 et versions ultérieures. • EKSClusters Amazon avec agent de sécurité v1.4.0 et versions ultérieures. Pour de plus amples informations, veuillez consulter GuardDuty historique des versions de l'agent.	Arguments de ligne de commande fournis au moment de l'exécution du processus. Ce champ peut contenir des données client sensibles.

Événements de conteneur

Nom de champ	Description
Nom de conteneur	Nom du conteneur. Lorsqu'il est disponible, ce champ affiche la valeur de l'étiquette `io.kubenetes.container.name` .

Nom de champ	Description
Récipient UID	L'ID unique du conteneur attribué par l'environnement d'exécution du conteneur.
Exécution de conteneur	Exécution du conteneur (tel que `docker` ou `containerd`) utilisé pour exécuter le conteneur.
ID de l'image de conteneur	ID de l'image du conteneur.
Nom d'image de conteneur	Nom de l'image du conteneur.

AWS Fargate événements de tâches (Amazon ECS uniquement)

Nom de champ	Description
Nom de la ressource Amazon de la tâche (ARN)	Celui ARN de la tâche.
Nom du cluster	Nom du ECS cluster Amazon.
Nom de famille	Le nom de famille de la définition de tâche. Le `family` est utilisé comme nom pour la définition de tâche utilisée pour lancer la tâche.
Service Name	Le nom du ECS service Amazon, si la tâche a été lancée dans le cadre d'un service.
Type de lancement	L'infrastructure sur laquelle s'exécute votre tâche. Pour la surveillance du temps d'exécution avec le type de ressource as`ECSCluster` , le type de lancement peut être l'un `EC2` ou l'autre`FARGATE`.
CPU	Le nombre d'CPUunités utilisées par la tâche tel qu'il est exprimé dans la définition de la tâche.

Événements du pod Kubernetes

Nom de champ	Description
ID de pod	L'ID du pod Kubernetes.
Nom de pod	Nom du pod Kubernetes.
Espace de noms de pod	Nom de l'espace de noms Kubernetes auquel appartient la charge de travail Kubernetes.
Nom de cluster Kubernetes	Nom du cluster Kubernetes.

DNSévénements

Nom de champ	Description
Type de socket	Type de socket pour indiquer la sémantique de communication. Par exemple, `SOCK_RAW`.
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses `AF_INET` est utilisée pour le protocole IP v4.
ID de direction	ID de direction de la connexion.
Numéro de protocole	Le numéro de protocole de couche 4, tel que 17 pour UDP et 6 pourTCP.
DNSIP du point de terminaison distant	Adresse IP distante de la connexion.
DNSPort de point de terminaison distant	Numéro de port de la connexion.
DNSIP du point de terminaison local	Adresse IP locale de la connexion.

Nom de champ	Description
DNSPort du point de terminaison local	Numéro de port de la connexion.
DNSCharge utile	Charge utile des DNS paquets contenant des DNS requêtes et des réponses.

Événements ouverts

Nom de champ	Description
Filepath	Chemin du fichier ouvert lors dans cet événement.
Indicateurs	Décrit le mode d'accès aux fichiers, tel que lecture seule, écriture seule et lecture-écriture.

Événement du module de charge

Nom de champ	Description
Nom de module	Nom du module chargé dans le noyau.

Événements Mprotect

Nom de champ	Description
Plage d'adresses	Plage d'adresses pour laquelle les protections d'accès ont été modifiées.
Régions de mémoire	Spécifie la région de l'espace d'adressage d'un processus, tel que pile et tas.
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.

Événements de montage

Nom de champ	Description
Cible de montage	Chemin où la source de montage est montée.
Source de montage	Chemin sur l'hôte qui est monté sur la cible de montage.
Type de système de fichiers	Représente le type de montagefileSystem.
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.

Événements du lien

Nom de champ	Description
Chemin du lien	Chemin où le lien physique est créé.
Chemin cible	Chemin du fichier vers lequel pointe le lien physique.

Événements Symlink

Nom de champ	Description
Chemin du lien	Chemin où le lien symbolique est créé.
Chemin cible	Chemin du fichier vers lequel pointe le lien symbolique.

Événements Dup

Nom de champ	Description
Descripteur d'ancien fichier	Descripteur de fichier qui représente un objet de fichier ouvert.

Nom de champ	Description
Descripteur de nouveau fichier	Descripteur de nouveau fichier dupliqué du descripteur d'ancien fichier. Aussi bien le descripteur d'un ancien fichier que celui de nouveau fichier représentent le même objet de fichier ouvert.
IP du point de terminaison distant Dup	Adresse IP distante de socket réseau représentée par le descripteur de nouveau fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.
Port du point de terminaison distant Dup	Port distant de socket réseau représenté par le descripteur de nouveau fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.
Adresse IP du point de terminaison local Dup	Adresse IP locale de socket réseau représentée par le descripte ur d'ancien fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.
Port du point de terminaison local Dup	Port local de socket réseau représenté par le descripteur d'ancien fichier. Applicable uniquement lorsque le descripteur d'ancien fichier représente un socket réseau.

Événement de mappage de mémoire

Nom de champ	Description
Filepath	Chemin du fichier auquel la mémoire est mappée.

Événements de socket

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses `AF_INET` est utilisée pour la version IP du protocole 4.

Nom de champ	Description
Type de socket	Type de socket pour indiquer la sémantique de communication. Par exemple, `SOCK_RAW`.
Numéro de protocole	Spécifie un protocole particulier au sein de la famille d'adresse s. Il existe généralement un protocole unique dans les familles d'adresses. Par exemple, la famille d'adresses `AF_INET` utilise uniquement le protocole IP.

Événements de connexion

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses `AF_INET` est utilisée pour le protocole IP v4.
Type de socket	Type de socket pour indiquer la sémantique de communication. Par exemple, `SOCK_RAW`.
Numéro de protocole	Spécifie un protocole particulier au sein de la famille d'adresse s. Il existe généralement un protocole unique dans les familles d'adresses. Par exemple, la famille d'adresses `AF_INET` utilise uniquement le protocole IP.
Filepath	Chemin du fichier socket si la famille d'adresses est `AF_UNIX`.
IP du point de terminaison distant	Adresse IP distante de la connexion.
Port du point de terminaison distant	Numéro de port de la connexion.
Adresse IP du point de terminaison local	Adresse IP locale de la connexion.

Nom de champ	Description
Port du point de terminaison local	Numéro de port de la connexion.

Événements Process VM Readv

Nom de champ	Description
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.
Cible PID	ID du processus à partir duquel la mémoire est lue.
Processus cible UUID	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.

Événements Process VM Writev

Nom de champ	Description
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.
Cible PID	ID du processus dans lequel la mémoire est écrite.
Processus cible UUID	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.

Événements Ptrace

Nom de champ	Description
Cible PID	ID du processus cible.
Processus cible UUID	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.
Indicateurs	Représente les options qui contrôlent le comportement de cet événement.

Lier des événements

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses `AF_INET` est utilisée pour le protocole IP v4.
Type de prise	Type de socket pour indiquer la sémantique de communication. Par exemple, `SOCK_RAW`.
Numéro de protocole	Le numéro de protocole de couche 4, tel que 17 pour UDP et 6 pourTCP.
IP du point de terminaison local	Adresse IP locale de la connexion.
Port du point de terminaison local	Numéro de port de la connexion.

Écoutez les événements

Nom de champ	Description
Famille d'adresses	Représente le protocole de communication associé à l'adresse. Par exemple, la famille d'adresses `AF_INET` est utilisée pour le protocole IP v4.
Type de prise	Type de socket pour indiquer la sémantique de communication. Par exemple, `SOCK_RAW`.
Numéro de protocole	Le numéro de protocole de couche 4, tel que 17 pour UDP et 6 pourTCP.
IP du point de terminaison local	Adresse IP locale de la connexion.
Port du point de terminaison local	Numéro de port de la connexion.

Renommer les événements

Nom de champ	Description
Filepath	Chemin où se trouve le fichier renommé.
Cible	Le nouveau chemin du fichier.

Organisez UID des événements

Nom de champ	Description
Nouveau EUID	Le nouvel ID utilisateur effectif du processus.
Nouveau UID	Le nouvel ID utilisateur du processus.

Événements Chmod

Nom de champ	Description
Filepath	Chemin du fichier qui invoque cet événement.
Mode de fichier	Les autorisations d'accès mises à jour pour le fichier associé.

GuardDuty Agent d'hébergement de ECR référentiels Amazon

Les sections suivantes répertorient les référentiels Amazon Elastic Container Registry (AmazonECR) où GuardDuty héberge l'agent de sécurité déployé sur vos ECS clusters Amazon EKS et Amazon.

Table des matières

Référentiel pour la version 1.6.0 ou supérieure de l'EKSagent

Le tableau suivant indique les ECR référentiels Amazon hébergeant l'agent EKS complémentaire Amazon version (`aws-guardduty-agent`) 1.6.0 ou ultérieure, pour chacun d'entre eux. Région AWS

Région AWS	ECRRéférentiel Amazon URI
USA Ouest (Oregon)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`
Europe (Paris)	`602401143452.dkr.ecr.eu-west-3.amazonaws.com`
Asie-Pacifique (Mumbai)	`602401143452.dkr.ecr.ap-south-1.amazonaws.com`
Asie-Pacifique (Hyderabad)	`900889452093.dkr.ecr.ap-south-2.amazonaws.com`

Région AWS	ECRRéférentiel Amazon URI
Canada (Centre)	602401143452.dkr.ecr.ca-central-1.amazonaws.com
Canada Ouest (Calgary)	761377655185.dkr.ecr.ca-west-1.amazonaws.com
Moyen-Orient (UAE)	759879836304.dkr.ecr.me-central-1.amazonaws.com
Europe (Londres)	602401143452.dkr.ecr.eu-west-2.amazonaws.com
USA Ouest (Californie du Nord)	602401143452.dkr.ecr.us-west-1.amazonaws.com
USA Est (Virginie du Nord)	602401143452.dkr.ecr.us-east-1.amazonaws.com
USA Est (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com
Europe (Ireland)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
South America (São Paulo)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
Europe (Stockholm)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
Europe (Francfort)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
Europe (Zurich)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
Asie-Pacifique (Singapour)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com

Région AWS	ECRRéférentiel Amazon URI
Asie-Pacifique (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
Asie-Pacifique (Jakarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
Asie-Pacifique (Tokyo)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
Asie-Pacifique (Séoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
Asie-Pacifique (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
Asie-Pacifique (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com
Moyen-Orient (Bahreïn)	759879836304.dkr.ecr.me-south-1.amazonaws.com
Europe (Milan)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
Europe (Espagne)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
Afrique (Le Cap)	877085696533.dkr.ecr.af-south-1.amazonaws.com
Asie-Pacifique (Melbourne)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
Israël (Tel Aviv)	066635153087.dkr.ecr.il-central-1.amazonaws.com

Référentiel pour les versions 1.5.0 et antérieures de l'EKSagent

Le tableau suivant indique les ECR référentiels Amazon hébergeant l'agent EKS complémentaire Amazon version (`aws-guardduty-agent`) 1.5.0 et antérieures, pour chacun d'entre eux. Région AWS

Région AWS	ECRRéférentiel Amazon URI
USA Ouest (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europe (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Asie-Pacifique (Mumbai)	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`
Asie-Pacifique (Hyderabad)	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`
Canada (Centre)	`001188825231.dkr.ecr.ca-central-1.amazonaws.com`
Moyen-Orient (UAE)	`601769779514.dkr.ecr.me-central-1.amazonaws.com`
Europe (Londres)	`109118265657.dkr.ecr.eu-west-2.amazonaws.com`
USA Ouest (Californie du Nord)	`373421517865.dkr.ecr.us-west-1.amazonaws.com`
USA Est (Virginie du Nord)	`031903291036.dkr.ecr.us-east-1.amazonaws.com`
USA Est (Ohio)	`591382732059.dkr.ecr.us-east-2.amazonaws.com`
Europe (Ireland)	`673884943994.dkr.ecr.eu-west-1.amazonaws.com`

Région AWS	ECRRéférentiel Amazon URI
South America (São Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europe (Stockholm)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europe (Francfort)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europe (Zurich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asie-Pacifique (Singapour)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asie-Pacifique (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asie-Pacifique (Jakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asie-Pacifique (Tokyo)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Asie-Pacifique (Séoul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asie-Pacifique (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Asie-Pacifique (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Moyen-Orient (Bahreïn)	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europe (Milan)	528450769569.dkr.ecr.eu-south-1.amazonaws.com

Région AWS	ECRRéférentiel Amazon URI
Europe (Espagne)	`531047660167.dkr.ecr.eu-south-2.amazonaws.com`
Afrique (Le Cap)	`379032919888.dkr.ecr.af-south-1.amazonaws.com`
Asie-Pacifique (Melbourne)	`750462861327.dkr.ecr.ap-southeast-4.amazonaws.com`
Israël (Tel Aviv)	`292660727137.dkr.ecr.il-central-1.amazonaws.com`

Référentiel pour GuardDuty agent sur AWS Fargate (Amazon ECS uniquement)

Le tableau suivant indique les ECR référentiels Amazon qui hébergent l' GuardDuty agent pour AWS Fargate (Amazon ECS uniquement) pour chacun Région AWS d'entre eux.

Région AWS	ECRRéférentiel Amazon URI
USA Ouest (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europe (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Mumbai)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Canada (Centre)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Moyen-Orient (UAE)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`

Région AWS	ECRRéférentiel Amazon URI
Europe (Londres)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate`
USA Ouest (Californie du Nord)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate`
USA Est (Virginie du Nord)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate`
USA Est (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate`
Europe (Ireland)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate`
South America (São Paulo)	`758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Europe (Stockholm)	`591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate`
Europe (Francfort)	`323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europe (Zurich)	`529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Singapour)	`174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Sydney)	`005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Jakarta)	`510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate`

Région AWS	ECRRéférentiel Amazon URI
Asie-Pacifique (Tokyo)	`533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Séoul)	`914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Osaka)	`273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Hong Kong)	`258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Moyen-Orient (Bahreïn)	`536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europe (Milan)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europe (Espagne)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Afrique (Le Cap)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asie-Pacifique (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israël (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty historique des versions de l'agent

Les sections suivantes fournissent la version finale de GuardDuty l'agent déployé sur les EC2 instances Amazon, les ECS clusters Amazon et les EKS clusters Amazon

GuardDuty agent de sécurité pour les EC2 instances Amazon

Version d'agent	Notes de mise à jour	Date de disponibilité
v1.3.0	Optimisation et améliorations générales des performances Inclut la prise en charge de la capture de signaux de sécurité supplémentaires pour le futurTypes de recherche liés à la surveillance du temps.	19 août 2024
v1.2.0	Supporte les distributions du système d'exploitation Ubuntu 20.04, Ubuntu 22.04, Debian 11 et Debian 12 Supporte les noyaux 6.5 et 6.8 Optimisation et améliorations générales des performances	13 juin 2024
v1.1.0	Prend en charge la configura tion GuardDuty automatiq ue des agents dans le cadre de la surveillance du temps d'exécution pour les EC2 instances Amazon Prend en charge les nouveaux signaux de sécurité et les résultats publiés avec l'annonce de la disponibilité générale de Runtime Monitorin g pour les EC2 instances	26 mars 2024

Version d'agent	Notes de mise à jour	Date de disponibilité
	Optimisation et améliorations générales des performances	
v1.0.2	Compatible avec la dernière version d'Amazon ECSAMIs.	2 février 2024
v1.0.1	Les versions de l'agent publiées avant la v1.0.2 sont incompatibles avec Amazon ECS AMIs lancé après le 31 janvier 2024. Optimisation et améliorations générales des performances	23 janvier 2024
v1.0.0	Version initiale de l'RPMinstallation Les versions de l'agent publiées avant la v1.0.2 sont incompatibles avec Amazon ECS AMIs lancé après le 31 janvier 2024.	26 novembre 2023

RPM S3 bucket example script

La clé publique, la signature de x86_64RPM, la signature d'arm64 RPM et le lien d'accès correspondant aux RPM scripts hébergés dans les buckets Amazon S3 peuvent être créés à partir des modèles suivants. Remplacez la valeur du Région AWS, l'ID de AWS compte et la version de l' GuardDuty agent pour accéder aux RPM scripts. Les modèles suivants incluent la dernière version de l'agent pour les EC2 instances Amazon.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/publickey.pem
```

- GuardDuty RPMsignature de l'agent de sécurité :

Signature de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig
```

Signature d'arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- Liens d'accès aux RPM scripts du compartiment Amazon S3 :

  Lien d'accès pour x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm
```

  Lien d'accès pour arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.rpm
```

Debian S3 bucket example script

La clé publique, la signature avec arm64 et le lien d'accès correspondant aux scripts hébergés dans les buckets Amazon S3 peuvent être créés à partir des modèles suivants. Remplacez la valeur du Région AWS, l'ID de AWS compte et la version de l' GuardDuty agent pour accéder aux scripts. Les modèles suivants incluent la dernière version de l'agent pour les EC2 instances Amazon.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/publickey.pem
```

- GuardDuty signature de l'agent de sécurité :

  Signature d'amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.sig
```

Signature d'arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- Liens d'accès aux scripts du compartiment Amazon S3 :

  Lien d'accès pour amd64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.deb
  ```

  Lien d'accès pour arm64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.deb
  ```

Région AWS	Nom de la région	AWS ID de compte
eu-west-1	Europe (Irlande)	694911143906
us-east-1	USA Est (Virginie du Nord)	593207742271
us-east-2	USA Est (Ohio)	733349766148
eu-west-3	Europe (Paris)	665651866788
us-east-2	USA Est (Ohio)	307168627858
eu-central-1	Europe (Francfort)	323658145986
ap-northeast-2	Asie-Pacifique (Séoul)	914738172881
eu-north-1	Europe (Stockholm)	591436053604
ap-east-1	Asie-Pacifique (Hong Kong)	258348409381
me-south-1	Moyen-Orient (Bahreïn)	536382113932
eu-west-2	Europe (Londres)	892757235363

ap-northeast-1	Asie-Pacifique (Tokyo)	533107202818
ap-southeast-1	Asie-Pacifique (Singapour)	174946120834
ap-south-1	Asie-Pacifique (Mumbai)	251508486986
ap-southeast-3	Asie-Pacifique (Jakarta)	510637619217
sa-east-1	Amérique du Sud (São Paulo)	758426053663
ap-northeast-3	Asie-Pacifique (Osaka)	273192626886
eu-south-1	Europe (Milan)	266869475730
af-south-1	Afrique (Le Cap)	197869348890
ap-southeast-2	Asie-Pacifique (Sydney)	005257825471
me-central-1	Moyen-Orient (UAE)	000014521398
us-west-1	USA Ouest (Californie du Nord)	684579721401
ca-central-1	Canada (Centre)	354763396469
ap-south-2	Asie-Pacifique (Hyderabad)	950823858135
eu-south-2	Europe (Espagne)	919611009337
eu-central-2	Europe (Zurich)	529164026651
ap-southeast-4	Asie-Pacifique (Melbourne)	251357961535
il-central-1	Israël (Tel Aviv)	870907303882

GuardDuty agent de sécurité pour AWS Fargate (Amazon ECS uniquement)

Le tableau suivant présente l'historique des versions de l'agent GuardDuty de sécurité pour Fargate (ECSAmazon uniquement).

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.3.0	x86_64 () : AMD64 `sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831` Graviton (ARM64) : `sha256:ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1`	Optimisation et améliorations générales des performances. Inclut la prise en charge de la capture de signaux de sécurité supplémentaires pour le futur GuardDutyTypes de recherche liés à la surveillance du temps.	9 août 2024
v1.2.0	x86_64 () : AMD64 `sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93` Graviton (ARM64) : `sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd`	Optimisation et améliorations générales des performances.	31 mai 2024
v1.1.0	x86_64 () : AMD64 `sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657`	Prend en charge les nouveaux signaux et découvertes de sécurité.	01 mai 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
	Graviton (ARM64) : `sha256:0d 4b61648d7bdeab8ab8 d94684f805498927c7 d437d318204dcccfe8 c9383dc7`	Optimisation et améliorations générales des performances.	
v1.0.1	x86_64 () : AMD64 `sha256:9f 8cd438fb66f62d09bf c641286439f7ed5177 988a314a6021ef4ff8 80642e68` Graviton (ARM64) : `sha256:82 c66bb615bd0d1e96db 77b1f1fb51dc03220c aa593b1962249571bf 7147d1b7`	Optimisation et améliorations générales des performances.	26 janvier 2024
v1.0.0	x86_64 () : AMD64 `sha256:35 9b8b014e5076c625da a1056090e522631587 a7afa3b2e055edda6b d1141017` Graviton (ARM64) : `sha256:b9 438690fa8a86067180 a11658bec0f4f838ae 3fbd225d04b9306250 648b3984`	Version initiale de l'agent de GuardDuty sécurité pour AWS Fargate (Amazon ECS uniquement).	26 novembre 2023

GuardDuty agent de sécurité pour les EKS clusters Amazon

Le tableau suivant présente l'historique des versions de l' GuardDuty agent EKS complémentaire Amazon.

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.7.0	x86_64 () : AMD64 `sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec` Graviton (ARM64) : `sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a`	Optimisation et améliorations générales des performances. Inclut la prise en charge de la capture de signaux de sécurité supplémentaires pour le futurTypes de recherche liés à la surveillance du temps.	17 août 2024	–
v1.6.1	x86_64 () : AMD64 `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Graviton (ARM64) : `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Optimisation et améliorations générales des performances.	14 mai 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.6.0	x86_64 () : AMD64 `sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010` Graviton (ARM64) : `sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`	• Prend en charge la configuration GuardDuty automatique des agents pour les EC2 ressources EKS/. • Soutient les nouveaux signaux et résultats de sécurité. Pour plus d'informations, consultez Types d'événements d'exécution collectés qui GuardDuty utilisent et Types de recherche	29 avril 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
		liés à la surveillance du temps. • Optimisation et améliorations générales des performances.		

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.5.0	x86_64 () : AMD64 `sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d` Graviton (ARM64) : `sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6`	• Optimisation et améliorations générales des performances. • Améliorations de sécurité, y compris les nouveaux types d'événements ci-dessous sTypes d'événement d'exécution collectés. • Améliorations des performances liées à CPU l'utilisation.	07 mars 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.4.1	x86_64 () : AMD64 `sha256:66d4919277637426 60faa87cc2c39bb97b 7873039157ae8b90bc 999cb73d0b9c` Graviton (ARM64) : `sha256:537a330b2dd82357 024fb6daeb8761034 b7defd43b10dffe0792 c9e6d0778b40`	Optimisation et améliorations générales des performances.	16 janvier 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.4.0	x86_64 () : AMD64 `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64) : `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	Les points de montage du manifeste permettent une meilleure collecte de données AppArmor configuration dans le manifeste Collecter les arguments de la ligne de commande Optimisation et améliorations générales des performances	21 décembre 2(	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.3.1	x86_64 () : AMD64 `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64) : `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Correctifs et mises à jour de sécurité importants.	23 octobre 202	–
v1.3.0	x86_64 () : AMD64 `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64) : `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Compatible avec la plateforme Ubuntu Compatible avec Kubernetes version 1.28 Améliorations des performances générales et amélioration de la stabilité.	05 octobre 202	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.2.0	x86_64 () : AMD64 `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64) : `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Outre les instances AMD64 basées, la version v1.2.0 prend désormais également en charge les instances ARM64 basées. Prise en charge ajoutée et vérifiée pour Bottlerocket Compatible avec Kubernetes version 1.27 Améliorations des performances générales et améliorations de la stabilité.	16 juin 2023	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	En plus de Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty, cette version de l'agent prend également en charge Kubernetes version 1.26. Améliorations des performances générales et améliorations de la stabilité.	2 mai 2023	14 mai 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Version initiale de l'agent EKS complémentaire Amazon.	30 mars 2023	14 mai 2024

[1] Pour plus d'informations sur la mise à jour de la version actuelle de votre agent qui approche de la fin du support standard, consultezMise à jour manuelle de l'agent de sécurité.

Impact de la désactivation et du nettoyage des ressources

Cette section s'applique Compte AWS si vous choisissez de désactiver la surveillance du temps d'exécution ou uniquement la configuration GuardDuty automatique de l'agent pour un type de ressource.

Désactivation de la configuration GuardDuty automatique des agents

GuardDuty ne supprime pas l'agent de sécurité déployé sur votre ressource. Cependant, GuardDuty cessera de gérer les mises à jour de l'agent de sécurité.

GuardDuty continue de recevoir les événements d'exécution de votre type de ressource. Pour éviter tout impact sur vos statistiques d'utilisation, veillez à supprimer l'agent de GuardDuty sécurité de votre ressource.

Le fait qu'un utilisateur Compte AWS utilise ou non un point de VPC terminaison partagé GuardDuty ne supprime pas le VPC point de terminaison. Si nécessaire, vous devrez supprimer le point de VPC terminaison manuellement.

Désactivation de la surveillance de l'exécution et de la surveillance de l'EKSexécution

Cette section s'applique à vous dans les scénarios suivants :

- Vous n'avez jamais activé la surveillance du temps EKS d'exécution séparément et vous avez maintenant désactivé la surveillance du temps d'exécution.
- Vous désactivez à la fois la surveillance du temps d'exécution et la surveillance du temps EKS d'exécution. Si vous n'êtes pas sûr de l'état de configuration de EKS Runtime Monitoring, consultezVérifier l'état de configuration de EKS Runtime Monitoring.

> **Désactiver la surveillance du temps d'exécution sans désactiver EKS la surveillance du temps d'exécution**
>
> Dans ce scénario, à un moment donné, vous avez activé la surveillance du temps EKS d'exécution, puis ultérieurement, vous avez également activé la surveillance du temps d'exécution sans désactiver la surveillance du temps EKS d'exécution.
> Désormais, lorsque vous désactivez la surveillance du temps d'exécution, vous devez également désactiver la surveillance du temps EKS d'exécution ; dans le cas contraire, vous continuerez à supporter des coûts d'utilisation pour la surveillance du temps EKS d'exécution.

Si les scénarios listés précédemment s'appliquent à vous, alors vous GuardDuty effectuerez les actions suivantes sur votre compte :

- GuardDuty supprime celui VPC qui possède la `true` balise `GuardDutyManaged` :. C'est celui VPC que j' GuardDuty ai créé pour gérer l'agent de sécurité automatisé.
- GuardDuty supprime le groupe de sécurité marqué comme `GuardDutyManaged` :`true`.
- Pour un partage VPC qui a été utilisé par au moins un compte participant, GuardDuty ni le point de VPC terminaison ni le groupe de sécurité associé à la VPC ressource partagée ne sont supprimés.
- Pour une EKS ressource Amazon, GuardDuty supprime l'agent de sécurité. Cela est indépendant du fait qu'il soit géré manuellement ou par le biais GuardDuty.

  Pour une ECS ressource Amazon, étant donné qu'une ECS tâche est immuable, il est GuardDuty impossible de désinstaller l'agent de sécurité de cette ressource. Cela dépend de la façon dont vous gérez l'agent de sécurité, manuellement ou automatiquement GuardDuty. Une fois que vous avez désactivé la surveillance du GuardDuty temps d'exécution, aucun conteneur annexe n'est attaché lorsqu'une nouvelle ECS tâche commence à s'exécuter. Pour plus d'informations sur l'utilisation des tâches Fargate, consultezECS. Comment fonctionne la surveillance du temps d'exécution avec Fargate (Amazon uniquement) ECS

  Pour une EC2 ressource Amazon, GuardDuty désinstalle l'agent de sécurité de toutes les EC2 instances Amazon gérées par Systems Manager (SSM) uniquement lorsqu'il répond aux conditions suivantes :

  - Votre ressource n'est pas étiquetée avec la balise `GuardDutyManaged` : `false` exclusion.
  - GuardDuty doit être autorisé à accéder aux balises dans les métadonnées de l'instance. Pour cette EC2 ressource, l'accès aux balises dans les métadonnées de l'instance est défini sur Autoriser.

Lorsque vous arrêtez de gérer manuellement l'agent de sécurité

Quelle que soit l'approche que vous utilisez pour déployer et gérer l'agent de GuardDuty sécurité, pour arrêter de surveiller les événements d'exécution dans votre ressource, vous devez supprimer l'agent GuardDuty de sécurité. Lorsque vous souhaitez arrêter de surveiller les événements d'exécution à partir d'un type de ressource dans un compte, vous pouvez également supprimer le point de VPC terminaison Amazon.

Processus de nettoyage des ressources des agents de sécurité

Pour supprimer un point de VPC terminaison Amazon

- Sans partage VPC : lorsque vous ne souhaitez plus surveiller une ressource d'un compte, pensez à supprimer le point de VPC terminaison Amazon.
- Avec un partage VPC : lorsqu'un compte VPC propriétaire partagé supprime la VPC ressource partagée qui était toujours utilisée, l'état de couverture de la surveillance du temps d'exécution (et, le cas échéant, de la surveillance du temps EKS d'exécution) des ressources de votre compte de VPC propriétaire partagé et du compte participant peut devenir malsain. Pour plus d'informations sur l'état de couverture, consultezÉvaluation de la couverture d'exécution de vos ressources.

  Pour plus d'informations, veuillez consulter la section Suppression d'un point de terminaison d'interface.

Pour supprimer le groupe de sécurité

- Sans partage VPC : lorsque vous ne souhaitez plus surveiller un type de ressource dans un compte, pensez à supprimer le groupe de sécurité associé à AmazonVPC.
- Avec un partage VPC : lorsque le compte du VPC propriétaire partagé supprime le groupe de sécurité, tout compte participant utilisant actuellement le groupe de sécurité associé au partage VPC peut devenir insalubre pour le statut de couverture de la surveillance du temps d'exécution pour les ressources de votre compte VPC propriétaire partagé et du compte participant. Pour de plus amples informations, veuillez consulter Évaluation de la couverture d'exécution de vos ressources.

  Pour plus d'informations, voir Supprimer un groupe de sécurité.

Pour supprimer l'agent de GuardDuty sécurité d'un EKS cluster

Pour supprimer de votre EKS cluster l'agent de sécurité que vous ne souhaitez plus surveiller, consultez la section Suppression d'un module complémentaire.

La suppression de l'agent EKS complémentaire ne supprime pas l'`amazon-guarddutyespace` de noms du EKS cluster. Pour supprimer l'espace de noms `amazon-guardduty`, veuillez consulter Suppression d'un espace de noms.

Pour supprimer l'**`amazon-guarddutyespace de noms (EKScluster)`**

La désactivation de la configuration automatique des agents ne supprime pas automatiquement l'`amazon-guarddutyespace de noms de votre EKS cluster. Pour supprimer l'espace de noms amazon-guardduty`, veuillez consulter Suppression d'un espace de noms.

GuardDuty Protection contre les logiciels malveillants pour EC2

Malware Protection for vous EC2 aide à détecter la présence potentielle de malwares en analysant les volumes Amazon Elastic Block Store (AmazonEBS) attachés aux instances et aux charges de travail des conteneurs Amazon Elastic Compute Cloud (AmazonEC2). Malware Protection for EC2 fournit des options d'analyse qui vous permettent de décider si vous souhaitez inclure ou exclure des EC2 instances Amazon et des charges de travail de conteneur spécifiques au moment de l'analyse. Il offre également la possibilité de conserver les instantanés des EBS volumes Amazon attachés aux EC2 instances Amazon ou aux charges de travail des conteneurs dans vos GuardDuty comptes. Les instantanés ne sont conservés que lorsqu'un logiciel malveillant est détecté et qu'une protection contre les logiciels malveillants est générée pour les EC2 résultats.

La protection contre les programmes malveillants pour EC2 est une amélioration facultative et est conçue de manière à ne pas affecter les performances de vos ressources. GuardDuty Pour plus d'informations sur le EC2 fonctionnement de Malware Protection for Within GuardDuty, consultezFonctionnalité de la protection contre les logiciels malveillants pour EC2. Pour plus d'informations sur la disponibilité de la protection contre les programmes malveillants EC2 dans différents Régions AWS pays, voirRégions et points de terminaison.

> **Remarque**
>
> GuardDuty Malware Protection for EC2 ne prend pas en charge Fargate avec Amazon ou AmazonEKS. ECS

Malware Protection for EC2 propose deux types d'analyses pour détecter les activités potentiellement malveillantes dans vos EC2 instances Amazon et les charges de travail de vos conteneurs : une analyse des programmes malveillants GuardDuty initiée et une analyse des programmes malveillants à la demande. Le tableau suivant montre la comparaison entre les deux types d'analyse.

Factor	GuardDuty-analyse des logiciels malveillants initiée	Analyse des programmes malveillants à la demande
Comment invoquer l'analyse ?	Une fois que vous avez activé le scan anti-malware	Vous pouvez lancer une analyse des programmes

Factor	GuardDuty-analyse des logiciels malveillants initiée	Analyse des programmes malveillants à la demande
	GuardDuty initié GuardDuty , chaque fois qu'un résultat indique la présence potentiel le d'un malware dans une EC2 instance Amazon ou une charge de travail de conteneur , lance GuardDuty automatiq uement un scan anti-malw are sans agent sur les EBS volumes Amazon attachés à votre ressource potentiel lement affectée. Pour de plus amples informations, veuillez consulter GuardDuty-analyse des logiciels malveillants initiée.	malveillants à la demande en fournissant le nom de ressource Amazon (ARN) associé à votre EC2 instance Amazon ou à la charge de travail de votre conteneur . Vous pouvez lancer une analyse des programmes malveillants à la demande même si aucune GuardDuty recherche n'est générée pour votre ressource. Pour de plus amples informations, veuillez consulter Analyse des logiciels malveillants à la demande.
Configuration requise	Pour utiliser le scan GuardDuty anti-malware initié, vous devez l'activer pour votre compte. Pour de plus amples informations, veuillez consulter Configuration de l' GuardDuty analyse des programmes malveillants initiée.	Votre compte doit avoir été GuardDuty activé. Pour utiliser l'analyse des programmes malveillants à la demande, aucune configuration n'est requise au niveau des fonctionnalités.

Factor	GuardDuty-analyse des logiciels malveillants initiée	Analyse des programmes malveillants à la demande
Durée d'attente pour lancer une nouvelle analyse	Chaque fois que l'un d'entre eux est GuardDuty généréRésultats qui invoquent une analyse des programmes malveillants GuardDuty initiée par un programme malveillant, une analyse des logiciels malveillants n'est lancée automatiquement qu'une fois toutes les 24 heures.	Vous pouvez lancer une analyse des programmes malveillants à la demande sur la même ressource à tout moment une heure après le début de l'analyse précédente.
Disponibilité de la période d'essai gratuite de 30 jours	Lorsque vous activez l'analyse des programmes malveillants GuardDuty initiée pour la première fois dans votre compte, vous pouvez bénéficier d'une période d'essai gratuite de 30 jours*. Pour plus d'informations sur l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant, consultezessai gratuit de 30 jours.	Il n'y a pas de période d'essai gratuite* avec analyse des programmes malveillants à la demande pour les GuardDuty comptes nouveaux ou existants.

Factor	GuardDuty-analyse des logiciels malveillants initiée	Analyse des programmes malveillants à la demande
Options d'analyse	Une fois que vous avez configuré l'analyse des programmes malveillants GuardDuty initiée, Malware Protection for vous permet EC2 également de sélection ner les ressources à analyser ou à ignorer. Malware Protection for EC2 ne lance pas d'analyse automatique des ressources que vous choisissez d'exclure de l'analyse.	L'analyse des programmes malveillants à la demande prend en charge une balise globale —`GuardDuty Excluded` . Options d'analyse avec balises définies par l'utilisateurne s'applique pas à l'analyse des programmes malveillants à la demande car vous fournissez la ressource ARN manuellem ent.

*Vous devrez payer des frais d'utilisation pour créer des instantanés de EBS volume et conserver des instantanés. Pour plus d'informations sur la configuration de votre compte afin de conserver les instantanés, consultezConservation des instantanés.

Fonctionnalité de la protection contre les logiciels malveillants pour EC2

Volume de stockage par blocs élastiques (EBS)

Cette section explique comment Malware Protection forEC2, y compris le scan anti-malware GuardDuty initié et le scan anti-malware à la demande, analyse les EBS volumes Amazon associés à vos EC2 instances Amazon et à vos charges de travail de conteneur. Avant de poursuivre, tenez compte des personnalisations suivantes :

- Options d'analyse : Malware Protection for EC2 offre la possibilité de spécifier des balises afin d'inclure ou d'exclure les EC2 instances Amazon et les EBS volumes Amazon du processus d'analyse. Seule l'analyse des programmes malveillants GuardDuty initiée prend en charge les options d'analyse avec des balises définies par l'utilisateur. L'analyse des programmes malveillants GuardDuty initiée et l'analyse des programmes malveillants à la demande prennent en charge le

`GuardDutyExcluded` tag global. Pour de plus amples informations, veuillez consulter Options d'analyse avec balises définies par l'utilisateur.

- Conservation des instantanés : Malware Protection for EC2 propose une option permettant de conserver les instantanés de vos EBS volumes Amazon dans votre AWS compte. Cette option est désactivée par défaut. Vous pouvez opter pour la conservation des instantanés pour les analyses de programmes malveillants GuardDuty lancées ou à la demande. Pour de plus amples informations, veuillez consulter Conservation des instantanés.

Lorsque vous GuardDuty générez un résultat indiquant la présence potentielle d'un logiciel malveillant dans une EC2 instance Amazon ou une charge de travail de conteneur et que vous avez activé le type de scan GuardDuty initié dans Malware Protection forEC2, un scan GuardDuty anti-malware initié peut être invoqué sur la base de vos options d'analyse.

Pour lancer une analyse des programmes malveillants à la demande sur les EBS volumes Amazon associés à une EC2 instance Amazon, fournissez le nom de ressource Amazon (ARN) de l'EC2instance Amazon.

En réponse à une analyse des programmes malveillants à la demande ou à une analyse des programmes malveillants GuardDuty lancée automatiquement, GuardDuty crée des instantanés des EBS volumes pertinents attachés à la ressource potentiellement affectée et les partage avec le. GuardDuty compte de service À partir de ces instantanés, GuardDuty crée un EBS volume de réplique chiffré dans le compte de service.

Pour plus d'informations sur la méthodologie de détection des GuardDuty programmes malveillants et les moteurs d'analyse qu'elle utilise, consultezGuardDuty moteur d'analyse pour la détection des malwares.

Une fois l'analyse terminée, GuardDuty supprime les EBS volumes de réplication chiffrés et les instantanés de vos EBS volumes. Si un logiciel malveillant est détecté et que vous avez activé le paramètre de conservation des instantanés, les instantanés de vos EBS volumes ne seront pas supprimés et seront automatiquement conservés dans votre AWS compte. Lorsqu'aucun logiciel malveillant n'est détecté, les instantanés de vos EBS volumes ne sont pas conservés, quel que soit le paramètre de conservation des instantanés. Par défaut, le paramètre de conservation des instantanés est désactivé. Pour plus d'informations sur les coûts des instantanés et leur conservation, consultez les EBStarifs Amazon.

GuardDuty conservera chaque EBS volume de réplique du compte de service pendant 55 heures au maximum. En cas de panne de service ou de défaillance d'un EBS volume répliqué et de son

analyse des programmes malveillants, ce EBS volume GuardDuty sera conservé pendant sept jours au maximum. La période de rétention prolongée des volumes sert à trier et à traiter la panne ou la panne. GuardDuty Malware Protection for EC2 supprimera les EBS volumes de réplication du compte de service une fois la panne ou la panne corrigée, ou une fois la période de conservation prolongée expirée.

EBSVolumes Amazon pris en charge pour l'analyse des programmes malveillants

Dans tous les appareils Régions AWS compatibles GuardDuty avec la EC2 fonctionnalité Malware Protection for, vous pouvez scanner les EBS volumes Amazon chiffrés ou non chiffrés. Vous pouvez avoir des EBS volumes Amazon chiffrés à l'aide de l'une ou l'autre clé Clé gérée par AWSou d'une clé gérée par le client. Actuellement, certains d'entre eux Régions AWS prennent en charge à la fois le chiffrement de vos EBS volumes Amazon, tandis que d'autres ne prennent en charge que les clés gérées par le client.

Pour plus d'informations lorsque cette fonctionnalité n'est pas encore prise en charge, voir China Regions

La liste suivante décrit la clé qui permet GuardDuty de savoir si vos EBS volumes Amazon sont chiffrés ou non :

- Les EBS volumes Amazon non chiffrés ou chiffrés avec Clé gérée par AWS — GuardDuty utilisent leur propre clé pour chiffrer les répliques des volumes AmazonEBS.

  Si votre compte appartient à un compte Région AWS qui ne prend pas en charge l'analyse de EBS volumes Amazon chiffrés avec la valeur par défaut Clé gérée par AWS pour EBS, consultezModifier l'ID de AWS KMS clé par défaut d'un EBS volume Amazon.
- Les EBSvolumes Amazon chiffrés à l'aide d'une clé gérée par le client GuardDuty utilisent la même clé pour chiffrer le EBS volume répliqué.

Malware Protection for EC2 ne prend pas en charge l'analyse EC2 des instances Amazon avec `productCode` as`marketplace`. Si une analyse des programmes malveillants est lancée pour une telle EC2 instance Amazon, elle sera ignorée. Pour plus d'informations, consultez `UNSUPPORTED_PRODUCT_CODE_TYPE` dans Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants.

Modifier l'ID de AWS KMS clé par défaut d'un EBS volume Amazon

Par défaut, le fait CreateVolumeAPId'invoquer le chiffrement défini sur `true` sans spécifier l'ID de KMS clé crée un EBS volume Amazon qui est chiffré avec la AWS KMS clé de EBS chiffrement par défaut. Toutefois, lorsqu'aucune clé de chiffrement n'est fournie explicitement, vous pouvez modifier la clé par défaut en invoquant ModifyEbsDefaultKmsKeyIdAPIou en utilisant la AWS CLI commande correspondante.

Pour modifier l'ID de clé EBS par défaut, ajoutez l'autorisation nécessaire suivante à votre IAM politique —`ec2:modifyEbsDefaultKmsKeyId`. Tout EBS volume Amazon nouvellement créé que vous choisissez de chiffrer, mais que vous ne spécifiez pas d'identifiant de KMS clé associé, utilisera l'ID de clé par défaut. Utilisez l'une des méthodes suivantes pour mettre à jour l'ID de clé EBS par défaut :

Pour modifier l'ID de KMS clé par défaut d'un EBS volume Amazon

Effectuez l'une des actions suivantes :

- À l'aide d'un API — Vous pouvez utiliser le ModifyEbsDefaultKmsKeyIdAPI. Pour plus d'informations sur la manière dont vous pouvez consulter l'état de chiffrement de votre volume, consultez Create Amazon EBS volume.
- Utilisation de la AWS CLI commande — L'exemple suivant modifie l'ID de KMS clé par défaut qui cryptera les EBS volumes Amazon si vous ne fournissez pas d'ID de KMS clé. Assurez-vous de remplacer la région par l'identifiant Région AWS de votre clé KM.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

La commande ci-dessus générera une sortie similaire à la sortie suivante :

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Pour plus d'informations, consultez modify-ebs-default-kms-key-id.

Personnalisations de la protection contre les programmes malveillants pour EC2

Cette section décrit comment vous pouvez personnaliser les options d'analyse pour vos EC2 instances Amazon ou vos charges de travail de conteneur lorsqu'une analyse de malware est invoquée, qu'elle soit lancée à la demande ou via GuardDuty.

Paramètres généraux

Conservation des instantanés

GuardDuty vous offre la possibilité de conserver les instantanés de vos EBS volumes dans votre AWS compte. Par défaut, le paramètre de conservation des instantanés est désactivé. Les instantanés ne seront conservés que si ce paramètre est activé avant le début de l'analyse.

Au début de l'analyse, GuardDuty génère les EBS volumes de réplication en fonction des instantanés de vos EBS volumes. Une fois que l'analyse est terminée et que le paramètre de conservation des instantanés est déjà activé dans votre compte, les instantanés de vos EBS volumes ne sont conservés que lorsqu'un logiciel malveillant est détecté et généréProtection contre les programmes malveillants pour les types de détection EC2. Que vous ayez activé ou non le paramètre de conservation des instantanés, lorsqu'aucun logiciel malveillant n'est détecté, les instantanés de vos volumes GuardDuty sont automatiquement supprimés. EBS

Coût d'utilisation des instantanés

Lors de l'analyse des logiciels malveillants, lors de la GuardDuty création des instantanés de vos EBS volumes Amazon, un coût d'utilisation est associé à cette étape. Si vous activez le paramètre de conservation des instantanés pour votre compte, lorsqu'un logiciel malveillant est détecté et que les instantanés sont conservés, vous devrez payer des frais d'utilisation. Pour plus d'informations sur le coût des instantanés et leur conservation, consultez les EBStarifs Amazon.

Choisissez votre méthode d'accès préférée pour activer le paramètre de conservation des instantanés.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Protection contre les programmes malveillants pour EC2.

3. Choisissez Paramètres généraux dans la partie inférieure de la console. Pour conserver les instantanés, activez Conservation des instantanés.

API/CLI

1. Exécutez UpdateMalwareScanSettingspour mettre à jour la configuration actuelle pour le paramètre de conservation des instantanés.
2. Vous pouvez également exécuter la AWS CLI commande suivante pour conserver automatiquement les instantanés lorsque GuardDuty Malware Protection for EC2 génère des résultats.

   Assurez-vous de remplacer le *detector-id* avec votre propre validedetectorId.
3. Pour trouver le detectorId correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

4. Si vous souhaitez désactiver la conservation des instantanés, remplacez RETENTION_WITH_FINDING par NO_RETENTION.

Options d'analyse avec balises définies par l'utilisateur

En utilisant l'analyse des programmes malveillants GuardDuty initiée par l'utilisateur, vous pouvez également spécifier des balises afin d'inclure ou d'exclure les EC2 instances Amazon et les EBS volumes Amazon du processus d'analyse et de détection des menaces. Vous pouvez personnaliser chaque analyse de programmes malveillants GuardDuty lancée en modifiant les balises dans la liste des balises d'inclusion ou d'exclusion. Chaque liste peut inclure jusqu'à 50 balises.

Si vous n'avez pas encore de balises définies par l'utilisateur associées à vos EC2 ressources, consultez la section Marquer vos EC2 ressources Amazon dans le guide de EC2 l'utilisateur Amazon ou baliser vos EC2 ressources Amazon dans le guide de l'EC2utilisateur Amazon.

> **Note**
>
> L'analyse des logiciels malveillants à la demande ne prend pas en charge les options d'analyse avec des balises définies par l'utilisateur. Elle prend en charge Balise `GuardDutyExcluded` globale.

Pour exclure les EC2 instances de l'analyse des programmes malveillants

Si vous souhaitez exclure une EC2 instance Amazon ou un EBS volume Amazon pendant le processus de numérisation, vous pouvez définir la `GuardDutyExcluded` balise sur n'importe quelle EC2 instance ou EBS volume Amazon, et vous GuardDuty ne le scannez pas. `true` Pour de plus amples informations sur la balise `GuardDutyExcluded`, veuillez consulter Autorisations de rôle liées à un service pour Malware Protection pour EC2. Vous pouvez également ajouter une balise d'EC2instance Amazon à une liste d'exclusion. Si vous ajoutez plusieurs balises à la liste des balises d'exclusion, toute EC2 instance Amazon contenant au moins l'une de ces balises sera exclue du processus d'analyse des programmes malveillants.

Choisissez votre méthode d'accès préférée pour ajouter une balise associée à une EC2 instance Amazon à une liste d'exclusion.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Protection contre les programmes malveillants pour EC2.
3. Développez la section Identifications d'inclusion/d'exclusion. Sélectionnez Add Tags (Ajouter des balises).
4. Choisissez Balises d'exclusion, puis Confirmer.
5. Spécifiez la paire **`Key`** et **`Value`** de la balise que vous souhaitez exclure. Il est facultatif de fournir la **`Value`**. Après avoir ajouté toutes les balises, choisissez Enregistrer.

> **Important**
>
> Les clés et valeurs d'étiquette sont sensibles à la casse. Pour plus d'informations, consultez les restrictions relatives aux balises dans le guide de EC2 l'utilisateur

Amazon ou les restrictions relatives aux balises dans le guide de EC2 l'utilisateur Amazon.

Si aucune valeur n'est fournie pour une clé et que l'EC2instance est étiquetée avec la clé spécifiée, cette EC2 instance sera exclue du processus d'analyse des programmes malveillants GuardDuty lancé par l'instance, quelle que soit la valeur attribuée à la balise.

API/CLI

- Mettez à jour les paramètres d'analyse des programmes malveillants en excluant une EC2 instance ou une charge de travail de conteneur du processus d'analyse.

  L' AWS CLI exemple de commande suivant ajoute une nouvelle balise à la liste des balises d'exclusion. Assurez-vous de remplacer l'exemple *detector-id* avec votre propre valide`detectorId`.

  `MapEquals` est une liste de paires `Key`/`Value`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

  Important

  Les clés et valeurs d'étiquette sont sensibles à la casse. Pour plus d'informations, consultez les restrictions relatives aux balises dans le guide de EC2 l'utilisateur Amazon ou les restrictions relatives aux balises dans le guide de EC2 l'utilisateur Amazon.

Pour inclure des EC2 instances dans l'analyse des programmes malveillants

Si vous souhaitez scanner une EC2 instance, ajoutez sa balise à la liste d'inclusion. Lorsque vous ajoutez une balise à une liste de balises d'inclusion, une EC2 instance qui ne contient aucune des balises ajoutées est ignorée de l'analyse des programmes malveillants. Si vous ajoutez plusieurs balises à la liste des balises d'inclusion, une EC2 instance contenant au moins une de ces balises est incluse dans l'analyse des programmes malveillants. Parfois, une EC2 instance peut être ignorée pendant le processus de numérisation. Pour de plus amples informations, veuillez consulter Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants.

Choisissez votre méthode d'accès préférée pour ajouter une balise associée à une EC2 instance à une liste d'inclusion.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Protection contre les programmes malveillants pour EC2.
3. Développez la section Identifications d'inclusion/d'exclusion. Sélectionnez Add Tags (Ajouter des balises).
4. Sélectionnez Identifications d'inclusion, puis Confirmer.
5. Choisissez Ajouter une nouvelle identification d'inclusion et spécifiez la paire **`Key`** et **`Value`** de la balise que vous souhaitez inclure. Il est facultatif de fournir la **`Value`**.

   Après avoir ajouté toutes les balises d'inclusion, choisissez Enregistrer.

   Si aucune valeur n'est fournie pour une clé, une EC2 instance est étiquetée avec la clé spécifiée, l'EC2instance sera incluse dans le processus d'EC2analyse de la protection contre les programmes malveillants, quelle que soit la valeur attribuée à la balise.

API/CLI

- Mettez à jour les paramètres d'analyse des programmes malveillants pour inclure une EC2 instance ou une charge de travail de conteneur dans le processus d'analyse.

  L' AWS CLI exemple de commande suivant ajoute une nouvelle balise à la liste des balises d'inclusion. Assurez-vous de remplacer l'exemple *`detector-id`* avec votre propre

validedetectorId. Remplacez l'exemple *TestKey* and *TestValue* avec la Value paire Key et de la balise associée à votre EC2 ressource.

MapEquals est une liste de paires Key/Value.

Pour trouver le detectorId correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> Les clés et valeurs d'étiquette sont sensibles à la casse. Pour plus d'informations, consultez les restrictions relatives aux balises dans le guide de EC2 l'utilisateur Amazon ou les restrictions relatives aux balises dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> La détection d'un nouveau tag peut prendre jusqu' GuardDuty à 5 minutes.

À tout moment, vous pouvez choisir Balises d'inclusion ou Balises d'exclusion, mais pas les deux. Si vous souhaitez passer d'une balise à l'autre, choisissez cette balise dans le menu déroulant lorsque vous ajoutez de nouvelles balises, puis confirmez votre sélection. Cette action efface toutes vos balises actuelles.

Balise **GuardDutyExcluded** globale

Par défaut, les instantanés de vos EBS volumes sont créés à l'aide d'une GuardDutyScanId balise. Ne supprimez pas cette balise car cela GuardDuty empêcherait l'accès aux instantanés. Dans Malware Protection, les deux types de scan EC2 ne scannent pas les EC2 instances Amazon ou les EBS volumes Amazon dont la GuardDutyExcluded balise est définie surtrue. S'il s'agit d'une

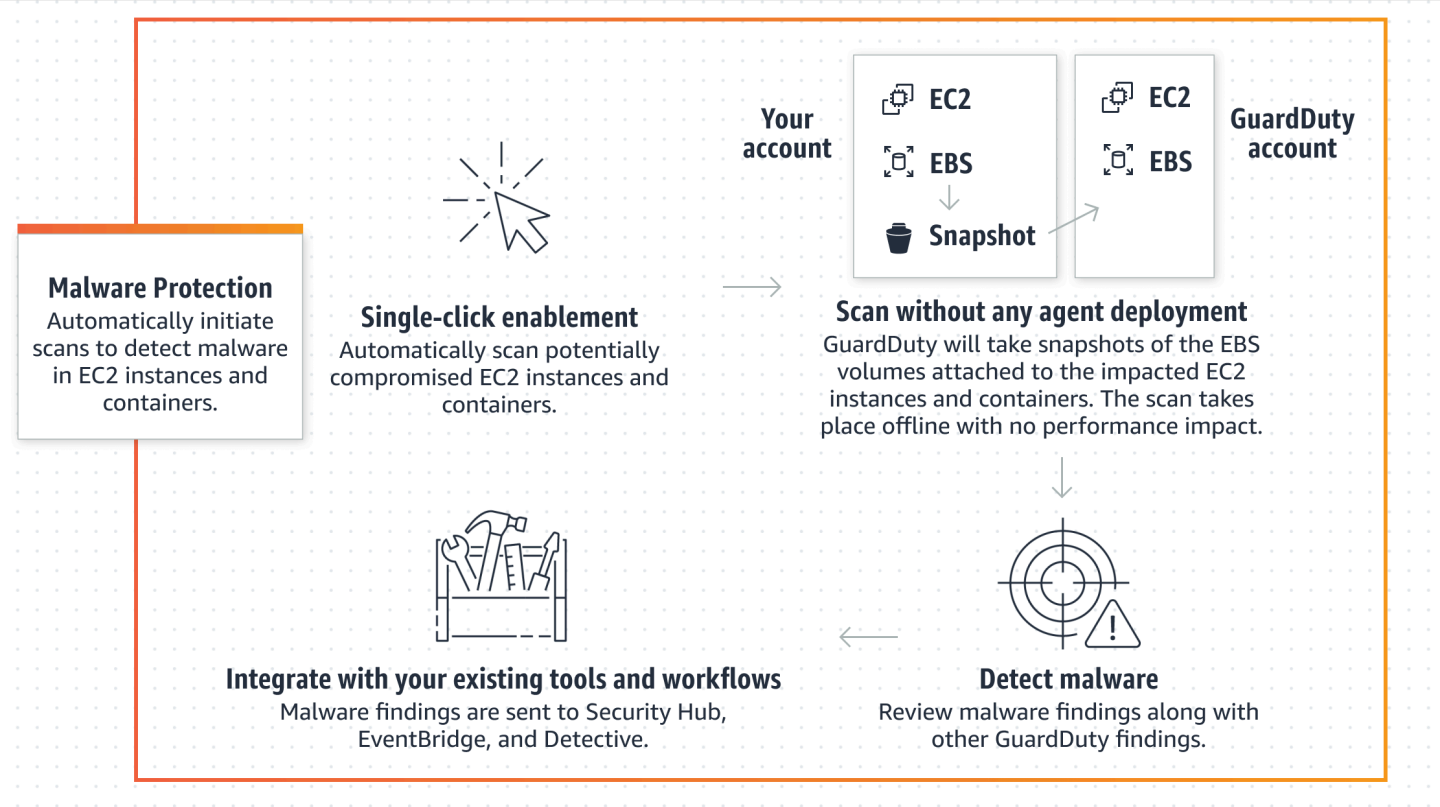
protection contre les logiciels malveillants destinée EC2 à analyser une telle ressource, un identifiant de scan sera généré mais l'analyse sera ignorée `EXCLUDED_BY_SCAN_SETTINGS` pour une raison. Pour de plus amples informations, veuillez consulter Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants.

GuardDuty-analyse des logiciels malveillants initiée

Lorsque l'analyse des programmes malveillants GuardDuty initiée est activée, chaque fois GuardDuty qu'une activité malveillante indique la présence potentielle d'un logiciel malveillant dans votre EC2 instance Amazon ou votre charge de travail de conteneur et GuardDuty génèreRésultats qui invoquent une analyse des programmes malveillants GuardDuty initiée par un programme malveillant, lance GuardDuty automatiquement une analyse sans agent sur les volumes Amazon Elastic Block Store (AmazonEBS) attachés à l'EC2instance Amazon potentiellement affectée ou à la charge de travail du conteneur afin de détecter la présence de logiciels malveillants. Les options d'analyse vous permettent d'ajouter des balises d'inclusion associées aux ressources que vous souhaitez analyser ou des balises d'exclusion associées aux ressources que vous souhaitez ignorer du processus d'analyse. Un lancement automatique de l'analyse tiendra toujours compte de vos options d'analyse. Vous pouvez également choisir d'activer le paramètre de conservation des instantanés afin de conserver les instantanés de vos EBS volumes uniquement si Malware Protection for EC2 détecte la présence de logiciels malveillants. Pour de plus amples informations, veuillez consulter Personnalisations de la protection contre les programmes malveillants pour EC2.

Pour chaque EC2 instance Amazon et chaque charge de travail de conteneur pour laquelle des résultats sont GuardDuty générés, une analyse automatique des malwares est GuardDuty lancée toutes les 24 heures. Pour plus d'informations sur la manière dont les EBS volumes Amazon attachés à votre EC2 instance Amazon ou à votre charge de travail de conteneur sont analysés, consultezFonctionnalité de la protection contre les logiciels malveillants pour EC2.

L'image suivante décrit le fonctionnement de l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant.



Pour plus d'informations sur la méthodologie de détection des GuardDuty programmes malveillants et les moteurs d'analyse qu'elle utilise, consultezGuardDuty moteur d'analyse pour la détection des malwares.

Lorsqu'un logiciel malveillant est détecté, GuardDuty génèreProtection contre les programmes malveillants pour les types de détection EC2. S'il GuardDuty ne génère aucun résultat indiquant la présence d'un logiciel malveillant sur la même ressource, aucune analyse des programmes malveillants GuardDuty initiée ne sera invoquée. Vous pouvez également lancer une analyse des logiciels malveillants à la demande sur la même ressource. Pour de plus amples informations, veuillez consulter Analyse des logiciels malveillants à la demande.

essai gratuit de 30 jours

Vous pouvez choisir d'activer ou de désactiver à tout moment l'analyse des programmes malveillants GuardDuty initiée par un logiciel compatible Région AWS . Compte AWS Si vous avez une organisation, chaque compte membre dispose de son propre essai gratuit de 30 jours.

Pour comprendre le fonctionnement de l'essai gratuit de 30 jours, considérez les scénarios suivants :

- Lorsque vous l'activez GuardDuty pour la première fois (nouveau GuardDuty compte), l'analyse des programmes malveillants GuardDuty initiée est également activée et est incluse dans l'essai gratuit de 30 jours associé au GuardDuty service.
- Un GuardDuty compte existant peut activer pour la première fois l'analyse des programmes malveillants GuardDuty initiée par le biais d'un essai gratuit de 30 jours. Lorsque vous activez cette fonctionnalité dans une autre région pour la première fois, vous bénéficiez d'un essai gratuit de 30 jours dans cette région.
- Si vous possédez déjà un GuardDuty compte qui utilisait la protection contre les programmes malveillants EC2 avant l'annonce de l'analyse des programmes malveillants à la demande et que ce GuardDuty compte utilise déjà le modèle tarifaire correspondant Région AWS, vous pouvez continuer à utiliser le scan antimalware GuardDuty initié par ce dernier.

> **Note**
>
> Même si vous bénéficiez d'une période d'essai gratuite de 30 jours, le coût d'utilisation standard pour la création des instantanés de EBS volume Amazon et leur conservation s'appliquent. Pour plus d'informations, consultez les EBStarifs Amazon.

Pour plus d'informations sur l'activation de l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant, consultezConfiguration de l' GuardDutyanalyse des programmes malveillants initiée.

Configuration de l' GuardDutyanalyse des programmes malveillants initiée

Configuration de l'analyse des programmes malveillants GuardDuty initiée par un compte autonome

Pour les comptes associés à AWS Organizations, vous pouvez automatiser ce processus via les paramètres de console, comme décrit dans la section suivante.

Pour activer ou désactiver l'analyse des programmes malveillants GuardDuty initiée

Choisissez votre méthode d'accès préférée pour configurer l'analyse des programmes malveillants GuardDuty initiée par un compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, sous Plans de protection, sélectionnez Protection contre les programmes malveillants pour EC2.
3. Le EC2 volet Protection contre les programmes malveillants indique l'état actuel de l'analyse des programmes malveillants GuardDuty lancée pour votre compte. Vous pouvez l'activer ou le désactiver à tout moment en sélectionnant respectivement Activer ou Désactiver.
4. Choisissez Save (Enregistrer).

API/CLI

- Exécutez l'updateDetectorAPIopération en utilisant votre propre identifiant de détecteur régional et en transmettant l'`dataSources`objet `EbsVolumes` réglé sur `true` ou`false`.

  Vous pouvez également activer ou désactiver l'analyse des programmes malveillants GuardDuty initiée à l'aide des outils de ligne de AWS commande en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser votre propre code valide *`detector ID`*.

  > **Note**
  >
  > L'exemple de code suivant active l'analyse des programmes malveillants GuardDuty initiée par l'utilisateur. Pour la désactiver, remplacez `true` par `false`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Configuration de l'analyse des programmes malveillants GuardDuty initiée par un utilisateur dans des environnements à comptes multiples

Dans un environnement multi-comptes, seuls les comptes GuardDuty administrateurs peuvent configurer une analyse des programmes malveillants GuardDuty initiée par un utilisateur. GuardDuty les comptes d'administrateur peuvent activer ou désactiver l'utilisation d'une analyse des programmes malveillants GuardDuty initiée par un utilisateur pour les comptes de leurs membres. Une fois que le compte administrateur a configuré le scan anti-malware GuardDuty lancé pour un compte membre, le compte membre suivra les paramètres du compte administrateur et ne pourra pas modifier ces paramètres via la console. GuardDuty les comptes d'administrateur qui gèrent les comptes de leurs membres avec AWS Organizations assistance peuvent choisir d'activer automatiquement l'analyse des programmes malveillants GuardDuty initiée sur tous les comptes existants et nouveaux de l'organisation. Pour de plus amples informations, veuillez consulter Gérer des GuardDuty comptes avec AWS Organizations.

Mise en place d'un accès fiable pour permettre une analyse des programmes malveillants GuardDuty initiée par un utilisateur

Si le compte d'administrateur GuardDuty délégué n'est pas le même que le compte de gestion de votre organisation, le compte de gestion doit activer l'analyse des programmes malveillants GuardDuty initiée par son organisation. De cette façon, le compte d'administrateur délégué peut créer Autorisations de rôle liées à un service pour Malware Protection pour EC2 les comptes membres gérés par le biais de AWS Organizations.

> **Note**
>
> Avant de désigner un compte d' GuardDuty administrateur délégué, consultezConsidérations et recommandations.

Choisissez votre méthode d'accès préférée pour autoriser le compte GuardDuty administrateur délégué à activer l'analyse des programmes malveillants GuardDuty initiée pour les comptes des membres de l'organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Pour vous connecter, utilisez le compte de gestion de votre AWS Organizations organisation.

2. a. Si vous n'avez pas désigné de compte d' GuardDuty administrateur délégué, alors :

   Sur la page Paramètres, sous Compte d' GuardDuty administrateur délégué, entrez les 12 chiffres **`account ID`** que vous souhaitez désigner pour administrer la GuardDuty politique de votre organisation. Choisisssez Delegate (Déléguer).

   b. i. Si vous avez déjà désigné un compte d' GuardDuty administrateur délégué différent du compte de gestion, alors :

   Sur la page Paramètres, sous Administrateur délégué, activez le paramètre Autorisations. Cette action permettra au compte GuardDuty administrateur délégué d'associer les autorisations pertinentes aux comptes des membres et d'activer l'analyse des programmes malveillants GuardDuty initiée par ces comptes membres.

   ii. Si vous avez déjà désigné un compte d' GuardDuty administrateur délégué identique au compte de gestion, vous pouvez activer directement l'analyse des programmes malveillants GuardDuty initiée pour les comptes des membres. Pour de plus amples informations, veuillez consulter Activation automatique de l'analyse des programmes malveillants GuardDuty initiée pour tous les comptes des membres.

> **Tip**
>
> Si le compte d' GuardDuty administrateur délégué est différent de votre compte de gestion, vous devez fournir des autorisations au compte d' GuardDuty administrateur délégué afin de permettre l'activation de l'analyse des programmes malveillants GuardDuty initiée par les comptes des membres.

3. Si vous souhaitez autoriser le compte GuardDuty administrateur délégué à activer l'analyse des programmes malveillants GuardDuty initiée pour les comptes des membres dans d'autres régions, modifiez votre Région AWS compte et répétez les étapes ci-dessus.

API/CLI

1. À l'aide des informations d'identification de votre compte de gestion, exécutez la commande suivante :

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Facultatif) Pour activer le scan des programmes malveillants GuardDuty lancé par le compte de gestion qui n'est pas un compte d'administrateur délégué, le compte de gestion le créera d'abord Autorisations de rôle liées à un service pour Malware Protection pour EC2 explicitement dans son compte, puis activera le scan de programmes malveillants GuardDuty initié par le compte d'administrateur délégué, comme pour tout autre compte de membre.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Vous avez désigné le compte d' GuardDuty administrateur délégué dans le compte actuellement sélectionné Région AWS. Si vous avez désigné un compte en tant que compte d' GuardDuty administrateur délégué dans une région, ce compte doit être votre compte d' GuardDuty administrateur délégué dans toutes les autres régions. Répétez l'étape ci-dessus pour toutes les autres régions.

Configuration de l'analyse des programmes malveillants GuardDuty initiée par un compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour activer ou désactiver l'analyse des programmes malveillants GuardDuty initiée pour un compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte de gestion.

2. Dans le volet de navigation, choisissez Malware Protection for EC2.
3. Sur la EC2 page Protection contre les programmes malveillants pour, choisissez Modifier à côté de l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant.
4. Effectuez l’une des actions suivantes :

   Utilisation d'Activer pour tous les comptes

   - Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
   - Choisissez Save (Enregistrer).

Utilisation de Configurer les comptes manuellement

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Choisissez Save (Enregistrer).

API/CLI

Exécutez l'updateDetectorAPIopération en utilisant votre propre identifiant de détecteur régional et en passant l'`features`objet au `name` `status` fur `EBS_MALWARE_PROTECTION` `ENABLED` et à mesure`DISABLED`.

Vous pouvez activer ou désactiver l'analyse des programmes malveillants GuardDuty initiée par le biais de la AWS CLI commande suivante. Assurez-vous d'utiliser un compte GuardDuty d'administrateur délégué valide *`detector ID`*.

> **Note**
>
> L'exemple de code suivant active l'analyse des programmes malveillants GuardDuty initiée par l'utilisateur. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Activation automatique de l'analyse des programmes malveillants GuardDuty initiée pour tous les comptes des membres

Choisissez votre méthode d'accès préférée pour activer la fonction d'analyse des logiciels malveillants GuardDuty initiée pour tous les comptes des membres. Cela inclut les comptes membres existants et les nouveaux comptes qui rejoignent l'organisation.

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l’une des actions suivantes :

   Utilisation de la EC2 page Protection contre les programmes malveillants

   1. Dans le volet de navigation, choisissez Malware Protection for EC2.
   2. Sur la EC2 page Protection contre les programmes malveillants pour, choisissez Modifier dans la section d'analyse des programmes malveillants GuardDuty initiée.
   3. Choisissez Activer pour tous les comptes. Cette action active automatiquement l'analyse des programmes malveillants GuardDuty initiée pour les comptes existants et nouveaux de l'organisation.
   4. Choisissez Save (Enregistrer).

   > **Note**
   >
   > La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

   Utilisation de la page Comptes

   1. Dans le panneau de navigation, choisissez Accounts (Comptes).
   2. Sur la page Comptes, choisissez les préférences d'activation automatique avant Ajouter des comptes par invitation.

3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes faisant l'objet d'une analyse GuardDutyantimalware initiée.
4. Sur la EC2 page Protection contre les programmes malveillants pour, choisissez Modifier dans la section d'analyse des programmes malveillants GuardDuty initiée.
5. Choisissez Activer pour tous les comptes. Cette action active automatiquement l'analyse des programmes malveillants GuardDuty initiée pour les comptes existants et nouveaux de l'organisation.
6. Choisissez Save (Enregistrer).

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de la page Comptes

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez les préférences d'activation automatique avant Ajouter des comptes par invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes faisant l'objet d'une analyse GuardDutyantimalware initiée.
4. Choisissez Save (Enregistrer).

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes, veuillez consulter Activer ou désactiver de manière sélective l'analyse des programmes malveillants GuardDuty initiée pour les comptes des membres.

API/CLI

- Pour activer ou désactiver de manière sélective l'analyse des programmes malveillants GuardDuty initiée pour vos comptes de membres, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.

- L'exemple suivant montre comment activer l'analyse des programmes malveillants GuardDuty initiée pour un seul compte membre. Pour désactiver un compte membre, remplacez `ENABLED` par `DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer l'analyse des programmes malveillants GuardDuty initiée par un utilisateur pour tous les comptes de membres actifs existants

Choisissez votre méthode d'accès préférée pour activer l'analyse des programmes malveillants GuardDuty initiée pour tous les comptes de membres actifs existants de l'organisation.

Pour configurer l'analyse des programmes malveillants GuardDuty initiée par un utilisateur pour tous les comptes de membres actifs existants

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le volet de navigation, choisissez Malware Protection for EC2.
3. Dans la section Protection contre les programmes malveillants pour EC2, vous pouvez consulter l'état actuel de la configuration de l'analyse des programmes malveillants GuardDuty initiée. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.

5. Choisissez Save (Enregistrer).

Activation automatique de l'analyse des programmes malveillants GuardDuty initiée pour les nouveaux comptes de membres

Les comptes de membres nouvellement ajoutés doivent être activés GuardDuty avant de sélectionner la configuration de l'analyse des programmes malveillants GuardDuty initiée par le client. Les comptes des membres gérés par invitation peuvent configurer manuellement une analyse des logiciels malveillants GuardDuty initiée pour leurs comptes. Pour de plus amples informations, veuillez consulter Step 3 - Accept an invitation.

Choisissez votre méthode d'accès préférée pour activer l'analyse des programmes malveillants GuardDuty initiée pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte d' GuardDuty administrateur délégué peut activer l'analyse des programmes malveillants GuardDuty initiée par les nouveaux comptes membres d'une organisation, à l'aide de la page Protection contre les programmes malveillants EC2 ou de la page Comptes.

Pour activer automatiquement l'analyse des programmes malveillants GuardDuty initiée pour les nouveaux comptes de membres

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l’une des actions suivantes :
   - À l'aide de la EC2 page Protection contre les programmes malveillants pour :

     1. Dans le volet de navigation, choisissez Malware Protection for EC2.
     2. Sur la EC2 page Protection contre les programmes malveillants pour, choisissez Modifier dans l'analyse des programmes malveillants GuardDuty lancée.
     3. Choisissez Configurer les comptes manuellement.
     4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, l'analyse des programmes malveillants GuardDuty initiée sera automatiquement

activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.

5. Choisissez Save (Enregistrer).

- Utilisation de la page Comptes :

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez les préférences d'activation automatique.
3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes dans le cadre d'une analyse des programmes malveillants GuardDuty initiée par un scan.
4. Choisissez Save (Enregistrer).

API/CLI

- Pour activer ou désactiver l'analyse des programmes malveillants GuardDuty lancée pour les nouveaux comptes membres, lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer l'analyse des programmes malveillants GuardDuty initiée pour un seul compte membre. Pour la désactiver, veuillez consulter Activer ou désactiver de manière sélective l'analyse des programmes malveillants GuardDuty initiée pour les comptes des membres. Si vous ne souhaitez pas l'activer pour tous les nouveaux comptes qui rejoignent l'organisation, définissez `AutoEnable` sur `NONE`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
 "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

  Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.
- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer ou désactiver de manière sélective l'analyse des programmes malveillants GuardDuty initiée pour les comptes des membres

Choisissez votre méthode d'accès préférée pour configurer de manière sélective le scan des logiciels malveillants GuardDuty lancé pour les comptes des membres.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sur la page Comptes, consultez la colonne d'analyse des programmes malveillants GuardDuty initiée pour connaître l'état de votre compte de membre.
4. Sélectionnez le compte pour lequel vous souhaitez configurer le scan GuardDuty anti-malware initié. Vous pouvez sélectionner plusieurs comptes à la fois.
5. Dans le menu Modifier les plans de protection, choisissez l'option appropriée pour l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant.

API/CLI

Pour activer ou désactiver de manière sélective l'analyse des programmes malveillants GuardDuty initiée pour vos comptes de membres, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.

L'exemple suivant montre comment activer l'analyse des programmes malveillants GuardDuty initiée pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

> **Note**
>
> Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Pour activer ou désactiver de manière sélective l'analyse des programmes malveillants GuardDuty initiée pour vos comptes de membres, exécutez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*. L'exemple suivant montre comment activer l'analyse des programmes malveillants GuardDuty initiée pour un seul compte membre. Pour la désactiver, remplacez `true` par `false`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer l'analyse des programmes malveillants GuardDuty initiée pour les comptes existants de l'organisation gérés sur invitation

La protection contre les GuardDuty programmes malveillants pour le rôle EC2 lié à un service (SLR) doit être créée dans les comptes des membres. Le compte administrateur ne peut pas activer la fonctionnalité d'analyse des programmes malveillants GuardDuty initiée dans les comptes membres qui ne sont pas gérés par AWS Organizations.

À l'heure actuelle, vous pouvez effectuer les étapes suivantes via la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/pour activer l'analyse des logiciels malveillants GuardDuty initiée pour les comptes de membres existants.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide des informations d'identification de votre compte administrateur.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sélectionnez le compte membre pour lequel vous souhaitez activer le scan GuardDuty anti-malware initié. Vous pouvez sélectionner plusieurs comptes à la fois.
4. Choisissez Actions.
5. Choisissez Dissocier le membre.
6. Dans votre compte membre, sélectionnez Protection contre les logiciels malveillants sous Plans de protection dans le volet de navigation.
7. Choisissez Activer l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant. GuardDuty créera un compte SLR pour le compte du membre. Pour plus d'informations surSLR, voirAutorisations de rôle liées à un service pour Malware Protection pour EC2.
8. Dans le compte de votre compte administrateur, sélectionnez Comptes dans le volet de navigation.
9. Choisissez le compte membre qui doit être ajouté à nouveau à l'organisation.
10. Choisissez Actions, puis Ajouter un membre.

API/CLI

1. Utilisez le compte administrateur pour exécuter DisassociateMembersAPIsur les comptes des membres qui souhaitent activer l'analyse des programmes malveillants GuardDuty initiée.
2. Utilisez votre compte de membre pour appeler afin d'UpdateDetectoractiver l'analyse des logiciels malveillants GuardDuty initiée.

   Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Utilisez le compte administrateur pour exécuter le CreateMembersAPIafin de réintégrer le membre dans l'organisation.

Résultats qui invoquent une analyse des programmes malveillants GuardDuty initiée par un programme malveillant

Une analyse des programmes malveillants GuardDuty initiée est lancée lorsqu'un comportement suspect est GuardDuty détecté, indiquant la présence d'un logiciel malveillant sur les charges de travail des EC2 instances ou des conteneurs Amazon.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (Sortant uniquement)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS

- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (Sortant uniquement)
- UnauthorizedAccess:EC2/SSHBruteForce (Sortant uniquement)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS

- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

Analyse des logiciels malveillants à la demande

L'analyse des programmes malveillants à la demande vous aide à détecter la présence de malwares sur les volumes Amazon Elastic Block Store (AmazonEBS) attachés à vos EC2 instances Amazon. Aucune configuration n'est nécessaire, vous pouvez lancer une analyse des programmes malveillants à la demande en fournissant le nom de ressource Amazon (ARN) de l'EC2instance Amazon que vous souhaitez analyser. Vous pouvez lancer une analyse des programmes malveillants à la demande via la GuardDuty console ouAPI. Avant d'initier une analyse des logiciels malveillants à la demande, vous pouvez définir votre paramètre Conservation des instantanés préféré. Les scénarios suivants peuvent vous aider à déterminer dans quels cas utiliser le type d'analyse des programmes malveillants à la demande avec GuardDuty :

- Vous souhaitez détecter la présence de logiciels malveillants dans vos EC2 instances Amazon sans activer le scan des programmes malveillants GuardDuty initié par ce dernier.
- Vous avez activé l'analyse des programmes malveillants GuardDuty initiée et une analyse a été lancée automatiquement. Après avoir suivi les mesures correctives recommandées pour la protection contre les programmes malveillants générée pour EC2 détecter le type, si vous souhaitez lancer une analyse sur la même ressource, vous pouvez lancer une analyse des programmes malveillants à la demande une heure après le début de l'analyse précédente.

  L'analyse des logiciels malveillants à la demande ne nécessite pas que 24 heures se soient écoulées depuis le lancement de la précédente analyse des logiciels malveillants. Une heure aurait dû s'écouler avant de lancer une analyse des logiciels malveillants à la demande sur la même ressource. Pour éviter de dupliquer une analyse des programmes malveillants sur la même EC2 instance, consultez. Nouvelle analyse de la même instance Amazon EC2

> **Note**
>
> L'analyse des programmes malveillants à la demande n'est pas incluse dans la période d'essai gratuite de 30 jours avec GuardDuty. Le coût d'utilisation s'applique au EBS volume total d'Amazon analysé pour chaque analyse de programmes malveillants. Pour plus

d'informations, consultez les GuardDuty tarifs Amazon. Pour plus d'informations sur le coût de création des instantanés des EBS volumes Amazon et leur conservation, consultez les EBStarifs Amazon.

Fonctionnement de l'analyse des logiciels malveillants à la demande

Grâce à l'analyse des programmes malveillants à la demande, vous pouvez lancer une demande d'analyse des programmes malveillants pour votre EC2 instance Amazon même lorsqu'elle est actuellement utilisée. Après avoir lancé une analyse des programmes malveillants à la demande, GuardDuty crée des instantanés des EBS volumes Amazon attachés à l'EC2instance Amazon dont le nom de ressource Amazon (ARN) a été fourni pour l'analyse. Ensuite, GuardDuty partage ces instantanés avec. GuardDuty compte de service GuardDuty crée des EBS volumes de réplication chiffrés à partir de ces instantanés du compte GuardDuty de service. Pour plus d'informations sur le mode de numérisation des EBS volumes Amazon, consultezVolume de stockage par blocs élastiques (EBS).

> **Note**
>
> GuardDuty crée les instantanés des données qui ont déjà été écrites sur les EBS volumes Amazon point-in-time lorsque vous lancez une analyse des programmes malveillants à la demande.

Si un logiciel malveillant est détecté et que vous avez activé le paramètre de conservation des instantanés, les instantanés de votre EBS volume sont automatiquement conservés dans votre. Compte AWS L'analyse des logiciels malveillants à la demande génère la Protection contre les programmes malveillants pour les types de détection EC2. Si aucun logiciel malveillant n'est détecté, quel que soit le paramètre de conservation des instantanés, les instantanés de vos EBS volumes sont supprimés.

Par défaut, les instantanés de vos EBS volumes sont créés à l'aide d'une `GuardDutyScanId` balise. Ne supprimez pas cette balise car cela GuardDuty empêcherait l'accès aux instantanés. Dans Malware Protection, les deux types de scan EC2 ne scannent pas les EC2 instances Amazon ou les EBS volumes Amazon dont la `GuardDutyExcluded` balise est définie sur`true`. S'il s'agit d'une protection contre les logiciels malveillants destinée EC2 à analyser une telle ressource, un identifiant de scan sera généré mais l'analyse sera ignorée `EXCLUDED_BY_SCAN_SETTINGS` pour une raison.

Pour de plus amples informations, veuillez consulter Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants.

AWS Organizations politique de contrôle des services — Accès refusé

À l'aide des politiques de contrôle des services (SCPs) dans AWS Organizations, le compte GuardDuty administrateur délégué peut restreindre les autorisations et refuser des actions telles que le lancement d'une analyse des programmes malveillants à la demande pour une EC2 instance Amazon appartenant à vos comptes.

En tant que compte GuardDuty membre, lorsque vous lancez une analyse des programmes malveillants à la demande pour vos EC2 instances Amazon, vous pouvez recevoir un message d'erreur. Vous pouvez vous connecter au compte de gestion pour comprendre pourquoi un SCP a été créé pour votre compte membre. Pour plus d'informations, consultez la section SCPEffets sur les autorisations.

Premiers pas avec l'analyse des logiciels malveillants à la demande

En tant que compte GuardDuty administrateur, vous pouvez lancer une analyse des programmes malveillants à la demande pour le compte de vos comptes de membres actifs dont les conditions préalables suivantes sont définies dans leurs comptes. Les comptes autonomes et les comptes de membres actifs GuardDuty peuvent également lancer une analyse des logiciels malveillants à la demande pour leurs propres EC2 instances Amazon.

Prérequis

- GuardDuty doit être activé à l' Régions AWS endroit où vous souhaitez lancer l'analyse des programmes malveillants à la demande.
- Assurez-vous que le AWS politique gérée : AmazonGuardDutyFullAccess est attaché à l'IAMutilisateur ou au IAM rôle. Vous aurez besoin de la clé d'accès et de la clé secrète associées à l'IAMutilisateur ou au IAM rôle.
- En tant que compte GuardDuty administrateur délégué, vous avez la possibilité de lancer une analyse des programmes malveillants à la demande pour le compte d'un membre actif.
- Si vous êtes un compte membre qui ne possède pas leAutorisations de rôle liées à un service pour Malware Protection pour EC2, le lancement d'une analyse des programmes malveillants à la demande pour une EC2 instance Amazon appartenant à votre compte créera automatiquement la protection contre SLR les logiciels malveillants pourEC2.

> **Important**
>
> Assurez-vous que personne ne supprime les SLRautorisations relatives à la protection contre les programmes malveillants EC2 lorsque l'analyse des programmes malveillants, qu'elle soit GuardDuty initiée ou à la demande, est toujours en cours. Cela empêchera l'analyse de se terminer correctement et de fournir un résultat d'analyse précis.

Avant de lancer une analyse des logiciels malveillants à la demande, assurez-vous qu'aucune analyse n'a été lancée sur la même ressource au cours de la dernière heure ; sinon, elle sera dédupliquée. Pour de plus amples informations, veuillez consulter Nouvelle analyse de la même ressource.

Lancement d'une analyse des logiciels malveillants à la demande

Choisissez votre méthode d'accès préférée pour lancer une analyse des logiciels malveillants à la demande.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Lancez l'analyse à l'aide de l'une des options suivantes :
   a. À l'aide de la EC2 page Protection contre les programmes malveillants pour :
      i. Dans le volet de navigation, sous Plans de protection, sélectionnez Protection contre les programmes malveillants pour EC2.
      ii. Sur la EC2 page Protection contre les programmes malveillants pour, indiquez l'EC2instance Amazon ARN [1] pour laquelle vous souhaitez lancer le scan.
   b. À l'aide de la page Analyses des logiciels malveillants :
      i. Dans le panneau de navigation, choisissez Analyses des logiciels malveillants.
      ii. Choisissez Démarrer le scan à la demande et indiquez l'EC2instance Amazon ARN [1] pour laquelle vous souhaitez lancer le scan.
      iii. S'il s'agit d'une nouvelle analyse, sélectionnez un ID d'EC2instance Amazon sur la page Malware Scans.

Développez le menu déroulant Démarrer l'analyse à la demande et choisissez Nouvelle analyse de l'instance sélectionnée.

3. Une fois que vous avez lancé une analyse à l'aide de l'une ou l'autre méthode, un ID de numérisation est généré. Vous pouvez utiliser cet ID de numérisation pour suivre la progression de l'analyse. Pour de plus amples informations, veuillez consulter Surveillance de l'état et des résultats de l'analyse des logiciels malveillants.

API/CLI

Invoquez StartMalwareScanqui accepte `resourceArn` l'EC2instance Amazon [1] pour laquelle vous souhaitez lancer une analyse des programmes malveillants à la demande.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Une fois que vous êtes parvenu à lancer une analyse, `StartMalwareScan` renvoie un `scanId`. Invoquez le DescribeMalwareScanssuivi de la progression de l'analyse lancée.

[1] Pour plus d'informations sur le format de votre EC2 instance AmazonARN, consultez Amazon Resource Name (ARN). Pour les EC2 instances Amazon, vous pouvez utiliser l'exemple de ARN format suivant en remplaçant les valeurs de la partition, de la région, de l' Compte AWS ID et de l'ID d'EC2instance Amazon. Pour plus d'informations sur la longueur de votre ID d'instance, consultez Resource IDs.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Nouvelle analyse de la même instance Amazon EC2

Qu'une analyse soit GuardDuty lancée ou à la demande, vous pouvez lancer une nouvelle analyse des programmes malveillants à la demande sur la même EC2 instance une heure après le début de l'analyse des programmes malveillants précédente. Si la nouvelle analyse des logiciels malveillants est lancée dans l'heure suivant le lancement de la précédente, votre demande entraînera l'erreur suivante et aucun ID de numérisation ne sera généré pour cette demande.

```
A scan was initiated on this resource recently. You can request a scan on
the same resource one hour after the previous scan start time.
```

Pour plus d'informations sur la façon d'initier une nouvelle analyse sur la même ressource, veuillez consulter Lancement d'une analyse des logiciels malveillants à la demande.

Pour suivre l'état des analyses des logiciels malveillants, veuillez consulter Surveillance de l'état de l'analyse et des résultats de la protection contre les GuardDuty logiciels malveillants pour EC2.

Surveillance de l'état de l'analyse et des résultats de la protection contre les GuardDuty logiciels malveillants pour EC2

Vous pouvez surveiller l'état d'analyse de chaque protection contre les GuardDuty programmes malveillants à des fins d'EC2analyse. Les valeurs possibles pour l'état de l'analyse sont `Completed`, `Running`, `Skipped` et `Failed`.

Une fois l'analyse terminée, le résultat de l'analyse est renseigné pour les analyses dont le statut est `Completed`. Les valeurs possibles pour Résultat de l'analyse sont `Clean` et `Infected`. À l'aide du type d'analyse, vous pouvez identifier si l'analyse des logiciels malveillants était `GuardDuty initiated` ou `On demand`.

Les résultats d'analyse de chaque analyse des logiciels malveillants ont une période de conservation de 90 jours. Choisissez votre méthode d'accès préférée pour suivre l'état de votre analyse des logiciels malveillants.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Analyses des logiciels malveillants.
3. Vous pouvez filtrer les analyses des programmes malveillants selon les propriétés suivantes disponibles dans les critères de filtre.

   - ID de numérisation
   - ID de compte
   - EC2instance ARN
   - Type d'analyse
   - État de l'analyse

   Pour plus d'informations sur les propriétés utilisées pour les critères de filtre, veuillez consulter Détails d'un résultat.

API/CLI

- Une fois que l'analyse des logiciels malveillants a obtenu un résultat d'analyse, vous pouvez filtrer les analyses de logiciels malveillants sur la base de `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` et `SCAN_START_TIME`.

  Les critères de `GUARDDUTY_FINDING_ID` filtrage sont disponibles lorsque le `SCAN_TYPE` est GuardDuty lancé. Pour plus d'informations sur les critères de filtre, veuillez consulter Détails d'un résultat.

- Vous pouvez modifier l'exemple *`filter-criteria`* dans la commande ci-dessous. À l'heure actuelle, vous pouvez filtrer sur la base d'une `CriterionKey` à la fois. Les options pour `CriterionKey` sont `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` et `SCAN_START_TIME`.

  Si vous utilisez le même `CriterionKey` que ci-dessous, assurez-vous de remplacer l'exemple `EqualsValue` par votre propre exemple valide AWS *`scan-id`*.

  Remplacez l'exemple de `detector-id` par votre propre *`detector-id`* valide. Vous pouvez modifier le *`max-results`* (jusqu'à 50) et le *`sort-criteria`*. `AttributeName`C'est obligatoire et doit l'être`scanStartTime`.

  ```
  aws guardduty describe-malware-scans --detector-
  id 60b87779336485625554d637e0e4bb3b2 --max-results 1 --sort-criteria
   '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
   '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
  {"EqualsValue":"123456789012"}}] }'
  ```

- La réponse de cette commande affiche au maximum un résultat avec des informations détaillées sur la ressource affectée et les résultats de logiciels malveillants (si `Infected`).

GuardDuty comptes de service par Région AWS

Lorsqu'un instantané est créé et partagé avec un compte de GuardDuty service, un nouvel événement est créé dans vos CloudTrail journaux. Cet événement indique le `snapshotId` et `userId` (compte GuardDuty de service correspondant Région AWS). Pour de plus amples informations, veuillez consulter Fonctionnalité de la protection contre les logiciels malveillants pour EC2.

L'exemple suivant est un extrait d'un CloudTrail événement qui montre le corps de la demande : `ModifySnapshotAttribute`

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

Le tableau suivant indique les comptes GuardDuty de service pour chaque région. `userId`Il s'agit du compte de GuardDuty service qui dépend de la région sélectionnée.

Région AWS	Code région	GuardDuty ID de compte de service (**`userId`**)
USA Est (Virginie du Nord)	us-east-1	652050842985
USA Est (Ohio)	us-east-2	178123968615
USA Ouest (Californie du Nord)	us-west-1	669213148797
USA Ouest (Oregon)	us-west-2	447226417196
Asie-Pacifique (Mumbai)	ap-south-1	913179291432
Asie-Pacifique (Osaka)	ap-northeast-3	089661699081
Asie-Pacifique (Séoul)	ap-northeast-2	039163547507
Asie-Pacifique (Tokyo)	ap-northeast-1	874749492622

Région AWS	Code région	GuardDuty ID de compte de service (**`userId`**)
Asie-Pacifique (Singapour)	ap-southeast-1	247460962669
Asie-Pacifique (Sydney)	ap-southeast-2	124839743349
Canada (Centre)	ca-central-1	175877067165
Canada Ouest (Calgary)	ca-west-1	894794104037
Europe (Francfort)	eu-central-1	002294850712
Europe (Irlande)	eu-west-1	283769539786
Europe (Londres)	eu-west-2	310125036783
Europe (Paris)	eu-west-3	866607715269
Europe (Stockholm)	eu-north-1	693780578038
Chine (Beijing)	cn-north-1	448721096076
Chine (Ningxia)	cn-northwest-1	480864352451
Amérique du Sud (São Paulo)	sa-east-1	546914126324
Asie-Pacifique (Hyderabad) (Inscription)	ap-south-2	682251015962
Asie-Pacifique (Melbourne) (Inscription)	ap-southeast-4	353488359550
Europe (Espagne) (Inscription)	eu-south-2	936182149045
Europe (Zurich) (Inscription)	eu-central-2	867642063380

Région AWS	Code région	GuardDuty ID de compte de service (**`userId`**)
Israël (Tel Aviv) (Inscription)	il-central-1	619233833001
Europe (Milan) (Inscription)	eu-south-1	977238331021
Asie-Pacifique (Hong Kong) (Inscription)	ap-east-1	249472122084
Moyen-Orient (Bahreïn) (Inscription)	me-south-1	404001805210
Afrique (Le Cap) (Inscription)	af-south-1	957664736811
Asie-Pacifique (Jakarta) (Inscription)	ap-southeast-3	452118225523
Moyen-Orient (UAE) (Opt-in)	me-central-1	828603743433

Protection contre les malwares pour les EC2 quotas

Malware Protection for EC2 dispose de la disponibilité par défaut suivante des différentes ressources utilisées par la fonctionnalité.

Portée	Par défaut	Commentaires
Extraction et analyse des données dans un fichier compressé ou archivé	5	Nombre maximal de niveaux imbriqués autorisés dans un fichier archivé.
Nombre de fichiers contenus dans un fichier archivé	1 000	Nombre maximum de fichiers pouvant être analysés dans une archive. Ce nombre est la

Portée	Par défaut	Commentaires
		somme du nombre de fichiers extraits de l'archive et du nombre de fichiers extraits de toutes les archives imbriquées.
Nombre de menaces	32	Le nombre maximum de menaces que vous pouvez consulter dans le panneau des résultats. GuardDuty Malware Protection for a EC2 peut-être détecté d'autres noms de menaces. Si le nombre de noms de menaces détectées est supérieur à la valeur par défaut, vous pouvez consulter les JSON détails en sélectionnant l'ID de recherche sous le nom de la recherche dans le panneau des détails de la GuardDuty console.
Nombre de fichiers par menace détectée	5	Le nombre maximum de fichiers identifiés par menace détectée. Par exemple, si 10 fichiers associés à une seule menace sont GuardDuty détectés, la menace affichera un maximum de 5 fichiers.

Portée	Par défaut	Commentaires
EBSvolumes par scan par instance	11	Nombre maximal de EBS volumes GuardDuty pouvant être scannés par EC2 instance. Si plus de 11 EBS volumes doivent être analysés, GuardDuty Malware Protection for les EC2 trie `deviceName` par ordre alphabétique et sélectionne les 11 premiers EBS volumes.
Taille du volume EBS	2048 GO	Associée à une EC2 instance Amazon et à une charge de travail de conteneur, GuardDuty Malware Protection for EC2 peut scanner chaque EBS volume Amazon d'une taille maximale de 2 048 Go. Ce quota s'applique à tous ceux pour Région AWS lesquels la prise en charge de la protection contre les programmes malveillants EC2 est disponible.

Portée	Par défaut	Commentaires
Types de système de fichiers pris en charge	GuardDuty Malware Protection for EC2 peut analyser les types de systèmes de fichiers suivants : • Système de fichiers de nouvelles technologies (NTFS) • Système de fichiers X (XFS) • Second extended (ext2) File System • Fourth extended (ext4) File System • Table d'allocation de fichiers (FAT) Système de fichiers • Table d'allocation de fichiers virtuelle (VFAT) Système de fichiers	S/O
Balises d'options d'analyse	50	Nombre maximum de balises de ressources que vous pouvez ajouter pour personnaliser les paramètres de vos options d'analyse des logiciels malveillants. Pour de plus amples informations, veuillez consulter Options d'analyse avec balises définies par l'utilisateur.

Portée	Par défaut	Commentaires
Recherche de la période de conservation	90	Nombre maximal de jours pendant lesquels une GuardDuty constatation est conservée. Pour obtenir les informations les plus récentes, veuillez consulter GuardDuty Quotas Amazon.
Période de conservation de l'analyse des logiciels malveillants	90	Nombre maximal de jours pendant lesquels GuardDuty Malware Protection EC2 conserve l'historique d'une analyse. Pour plus d'informations sur l'affichage des analyses des logiciels malveillants récentes, veuillez consulter Surveillance de l'état de l'analyse et des résultats de la protection contre les GuardDuty logiciels malveillants pour EC2.
Transactions par seconde (TPS) pour l'analyse des programmes malveillants à la demande	1	Nombre de demandes d'analyse des logiciels malveillants à la demande qui peuvent être initiées par seconde dans chaque région.
Limite de débordement pour l'analyse des logiciels malveillants à la demande	1	Nombre de demandes simultanées d'analyse des logiciels malveillants à la demande qui peuvent être initiées par seconde dans chaque région.

GuardDuty Protection contre les logiciels malveillants pour S3

Malware Protection for S3 vous aide à détecter la présence potentielle de malwares en scannant les objets récemment chargés dans le bucket Amazon Simple Storage Service (Amazon S3) que vous avez sélectionné. Lorsqu'un objet S3 ou une nouvelle version d'un objet S3 existant est chargé dans le compartiment que vous avez sélectionné, une analyse des programmes malveillants démarre GuardDuty automatiquement.

Protection contre les malwares pour S3 - Présentation et démonstration

Deux approches pour activer la protection contre les malwares pour S3

Vous pouvez activer Malware Protection pour S3 lorsque Compte AWS vous activez le GuardDuty service et que vous utilisez Malware Protection pour S3 dans le cadre de l' GuardDuty expérience globale, ou lorsque vous souhaitez utiliser la fonctionnalité Malware Protection pour S3 seule sans activer le GuardDuty service. Lorsque vous activez la protection contre les programmes malveillants pour S3 en tant que fonctionnalité indépendante, la GuardDuty documentation indique qu'elle utilise la protection contre les programmes malveillants pour S3 en tant que fonctionnalité indépendante.

Considérations relatives à l'utilisation indépendante de Malware Protection for S3

- GuardDuty résultats de sécurité — L'identifiant du détecteur est un identifiant unique associé à votre compte dans une région. Lorsque vous l'activez GuardDuty dans une ou plusieurs régions d'un compte, un identifiant de détecteur est créé automatiquement pour ce compte dans chaque région où vous l'activez GuardDuty. Pour plus d'informations, consultez la section Détecteur dans le Concepts et terminologie document.

  Lorsque vous activez la protection contre les programmes malveillants pour S3 indépendamment dans un compte, aucun identifiant de détecteur n'est associé à ce compte. Cela a un impact sur les GuardDuty fonctionnalités qui peuvent être mises à votre disposition. Par exemple, lorsqu'une analyse des programmes malveillants S3 détecte la présence d'un logiciel malveillant, aucun GuardDuty résultat n'est généré dans votre compte, Compte AWS car tous les GuardDuty résultats sont associés à un identifiant de détecteur.
- Vérifier si l'objet scanné est malveillant — Par défaut, GuardDuty publie les résultats de l'analyse des programmes malveillants sur votre bus d' EventBridge événements Amazon par

défaut et dans un espace de CloudWatch noms Amazon. Lorsque vous activez le balisage au moment de l'activation de Malware Protection for S3 pour un compartiment, l'objet S3 scanné reçoit une balise mentionnant le résultat de l'analyse. Pour plus d’informations sur le balisage, consultez Marquage facultatif des objets en fonction du résultat de l'analyse.

Considérations générales relatives à l'activation de la protection contre les programmes malveillants pour S3

Les considérations générales suivantes s'appliquent, que vous utilisiez Malware Protection pour S3 de manière indépendante ou dans le cadre de l' GuardDuty expérience :

- Vous pouvez activer la protection contre les programmes malveillants pour S3 pour un compartiment Amazon S3 appartenant à votre propre compte. En tant que compte d' GuardDuty administrateur délégué, vous ne pouvez pas activer cette fonctionnalité dans un compartiment Amazon S3 appartenant à un compte membre.
- Vous pouvez activer cette fonctionnalité dans les compartiments S3 appartenant à la même région que celle actuellement sélectionnée dans la GuardDuty console. GuardDuty ne prend pas en charge l'activation de cette fonctionnalité dans les compartiments S3 interrégionaux.
- En tant que compte d' GuardDuty administrateur délégué, vous recevrez une EventBridge notification Amazon chaque fois qu'un changement est apporté à un compartiment S3 configuré pour cette fonctionnalité par l'un des comptes membres de votre organisation. État des ressources du plan de protection contre les logiciels malveillants

Table des matières

- Affichage de l'utilisation et du coût de Malware Protection for S3
- Désactiver la protection contre les programmes malveillants pour S3 pour un compartiment protégé
- Supportabilité des fonctionnalités d'Amazon S3
- Quotas dans la protection contre les malwares pour S3

Tarification de la protection contre les programmes malveillants pour S3

Plan de niveau gratuit (coût de numérisation)

Chacun Compte AWS bénéficie d'un niveau gratuit de 12 mois qui inclut l'utilisation jusqu'à une limite mensuelle spécifique pour chaque région. Si votre consommation dépasse la limite spécifiée, vous commencerez à supporter les frais d'utilisation correspondant à la limite dépassée. Pour plus d'informations sur les limites spécifiées et un exemple de tarification, consultez GuardDuty la section Tarification des plans de protection.

- Tous les Comptes AWS utilisateurs existants peuvent utiliser le niveau gratuit de 12 mois pour cette fonctionnalité, qui commence le 11 juin 2024 et se termine le 11 juin 2025. Ce niveau gratuit prolongé de 12 mois pour votre compte s'applique à l'utilisation de Malware Protection pour S3, et à AWS service aucune autre GuardDuty fonctionnalité.

  Si un compte existant Compte AWS commence à utiliser Malware Protection for S3 après le 11 juin 2025 ou après la fin du niveau gratuit de 12 mois du compte, vous commencerez à supporter les frais d'utilisation associés.
- Si vous en avez un nouveau Compte AWS et que votre niveau gratuit de 12 mois commence après la disponibilité générale (11 juin 2024) de Malware Protection pour S3, votre période de niveau gratuit de 12 mois pour cette fonctionnalité sera la même que celle de 12 mois pour votre compte.

Pour plus d'informations sur le coût d'utilisation après l'activation de Malware Protection pour S3, consultezAffichage de l'utilisation et du coût de Malware Protection for S3.

Coût d'utilisation du balisage d'objets S3

Lorsque vous activez la protection contre les programmes malveillants pour S3, il est facultatif d'activer le balisage pour vos objets S3 scannés. Lorsque vous choisissez d'activer le balisage d'objets S3, un coût d'utilisation est associé. Pour plus d'informations sur les coûts, consultez l'onglet Gestion et informations sur la page de tarification d'Amazon S3.

Le coût d'utilisation du balisage d'objets S3 n'est pas inclus dans le plan Free Tier.

Amazon S3 APIs - GET et coût PUT d'utilisation

Vous devrez payer des frais d'utilisation lors de l' GuardDuty exécution d'Amazon S3 APIs en fonction du IAM rôle. Par exemple, après avoir assumé le IAM rôle, GuardDuty exécute le `PutObject` API pour ajouter l'objet de test au compartiment sélectionné. Cela permet GuardDuty d'évaluer le statut activé de la fonctionnalité.

Pour plus d'informations sur la tarification des API appels S3 sur votre compte Région AWS, consultez la section Demandes et extraction de données sous l'onglet Stockage et demandes de la page de tarification d'Amazon S3.

Comment fonctionne Malware Protection for S3 ?

Cette section décrit les composants de Malware Protection for S3 et son fonctionnement une fois que vous l'avez activée pour un compartiment S3.

Présentation

Vous pouvez activer la protection contre les programmes malveillants pour S3 pour un compartiment Amazon S3 qui appartient au vôtre Compte AWS. GuardDutyvous offre la possibilité d'activer cette fonctionnalité pour l'ensemble de votre compartiment ou de limiter la portée de l'analyse des programmes malveillants à des préfixes d'objets spécifiques, où GuardDuty analyse chaque objet téléchargé commençant par l'un des préfixes sélectionnés. Vous pouvez ajouter jusqu'à 5 préfixes. Lorsque vous activez la fonctionnalité pour un compartiment S3, ce compartiment est appelé compartiment protégé.

IAMautorisations de rôle

Malware Protection for S3 utilise un IAM rôle qui permet GuardDuty d'effectuer les actions d'analyse des programmes malveillants en votre nom. Ces actions incluent le fait d'être informé des nouveaux objets téléchargés dans le compartiment sélectionné, de scanner ces objets et éventuellement d'ajouter des balises à vos objets numérisés. Il s'agit d'une condition préalable à la configuration de votre compartiment S3 avec cette fonctionnalité.

Vous avez la possibilité de mettre à jour un IAM rôle existant ou d'en créer un nouveau à cette fin. Lorsque vous activez Malware Protection for S3 pour plusieurs compartiments, vous pouvez mettre

à jour le IAM rôle existant pour inclure le nom de l'autre compartiment, le cas échéant. Pour de plus amples informations, veuillez consulter Prérequis : créer ou mettre à jour une politique de IAM rôle.

Marquage facultatif des objets en fonction du résultat de l'analyse

Au moment d'activer Malware Protection for S3 pour votre compartiment, une étape facultative permet d'activer le balisage pour les objets S3 scannés. Le IAM rôle inclut déjà l'autorisation d'ajouter des balises à votre objet après le scan. Cependant, vous n' GuardDuty ajouterez des balises que si vous activez cette option au moment de la configuration.

Vous devez activer cette option avant qu'un objet ne soit chargé. Une fois le scan terminé, GuardDuty ajoute une balise prédéfinie à l'objet S3 scanné avec la paire clé:valeur suivante :

`GuardDutyMalwareScanStatus:`*`Potential scan result`*

Les valeurs potentielles des balises de résultats d'analyse incluent `NO_THREATS_FOUND`THREATS_FOUND,`UNSUPPORTED`,`ACCESS_DENIED`, et`FAILED`. Pour plus d'informations sur ces valeurs, consultezS3 object potential scan result values.

L'activation du balisage est l'un des moyens de connaître le résultat de l'analyse des objets S3. Vous pouvez également utiliser ces balises pour ajouter une politique de ressources S3 de contrôle d'accès (TBAC) basée sur des balises afin de pouvoir agir sur les objets potentiellement malveillants. Pour de plus amples informations, veuillez consulter Ajout TBAC d'une ressource de compartiment S3.

Nous vous recommandons d'activer le balisage au moment de configurer Malware Protection for S3 pour votre compartiment. Si vous activez le balisage après le téléchargement d'un objet et qu'il est possible que le scan soit lancé, GuardDuty vous ne pourrez pas ajouter de balises à l'objet numérisé. Pour plus d'informations sur les coûts associés au balisage d'objets S3, consultezTarification de la protection contre les programmes malveillants pour S3.

Procédure après avoir activé la protection contre les programmes malveillants pour S3 pour un compartiment

Une fois que vous avez activé Malware Protection pour S3, une ressource de plan de protection contre les malwares est créée exclusivement pour le compartiment S3 sélectionné. Cette ressource est associée à un identifiant de plan de protection contre les programmes malveillants, un identifiant unique pour votre ressource protégée. En utilisant l'une des IAM autorisations, GuardDuty il crée et gère une règle EventBridge gérée nomméeDO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*.

Comment GuardDuty traite-t-on vos données ? Garde-fous pour la protection des données

Malware Protection for S3 écoute les EventBridge notifications d'Amazon. Lorsqu'un objet est chargé dans le compartiment sélectionné ou dans l'un des préfixes, GuardDuty télécharge cet objet depuis le compartiment S3 à l'aide d'un, AWS PrivateLinkpuis le lit, le déchiffre et le scanne dans un environnement isolé de la même région. L'environnement de numérisation s'exécute dans un cloud privé virtuel verrouillé (VPC) sans accès à Internet. VPCIl est attaché à un groupe de règles de DNS pare-feu qui autorise la communication uniquement avec les domaines autorisés qui AWS en sont propriétaires. Pendant la durée de l'analyse, stocke GuardDuty temporairement l'objet S3 téléchargé dans l'environnement de numérisation chiffré à l'aide des clés AWS Key Management Service (AWS KMS).

Pour plus d'informations sur la méthodologie de détection des GuardDuty programmes malveillants et les moteurs d'analyse qu'elle utilise, consultezGuardDuty moteur d'analyse pour la détection des malwares.

Une fois l'analyse des programmes malveillants terminée, GuardDuty traite les métadonnées de l'analyse avec l'état de l'analyse, puis supprime la copie téléchargée de l'objet.

GuardDuty nettoie l'environnement de numérisation à chaque fois avant le début d'une nouvelle analyse. GuardDuty utilise une autorisation conditionnelle pour l'accès des opérateurs à l'environnement de numérisation, et chaque demande d'accès est examinée, approuvée et auditée.

Révision du résultat de l'analyse des objets S3

GuardDuty publie l'événement du résultat de l'analyse des objets S3 dans le bus d'événements EventBridge par défaut d'Amazon. GuardDuty envoie également les mesures de numérisation telles que le nombre d'objets scannés et le nombre d'octets scannés à Amazon CloudWatch. Si vous avez activé le balisage, vous GuardDuty ajouterez la balise prédéfinie `GuardDutyMalwareScanStatus` et un résultat de numérisation potentiel en tant que valeur de balise.

Pour de plus amples informations, veuillez consulter Surveillance dans le cadre de la protection contre les programmes malveillants pour S3.

Révision des résultats générés

L'examen des résultats dépend de l'utilisation ou non de Malware Protection for S3 avec GuardDuty. Réfléchissez aux scénarios suivants :

Utilisation de la protection contre les programmes malveillants pour S3 lorsque le GuardDuty service est activé (ID du détecteur)

Si l'analyse des programmes malveillants détecte un fichier potentiellement malveillant dans un objet S3, elle GuardDuty générera un résultat associé. Vous pouvez consulter les détails de la recherche et suivre les étapes recommandées pour éventuellement y remédier. En fonction de la fréquence de vos résultats d'exportation, les résultats générés sont exportés vers un compartiment S3 et un bus EventBridge d'événements.

Utilisation de Malware Protection pour S3 en tant que fonctionnalité indépendante (aucun identifiant de détecteur)

GuardDuty ne sera pas en mesure de générer des résultats car aucun identifiant de détecteur n'est associé. Pour connaître l'état de l'analyse des malwares sur les objets S3, vous pouvez consulter le résultat de l'analyse qui est GuardDuty automatiquement publié sur votre bus d'événements par défaut. Vous pouvez également consulter les CloudWatch mesures pour évaluer le nombre d'objets et d'octets qui GuardDuty ont été tentés de scanner. Vous pouvez configurer des CloudWatch alarmes pour être informé des résultats de l'analyse. Si vous avez activé le balisage des objets S3, vous pouvez également consulter l'état de l'analyse des programmes malveillants en vérifiant la clé de balise et la valeur de la `GuardDutyMalwareScanStatus` balise de résultat de l'analyse dans l'objet S3.

Fonctionnalités de protection contre les malwares pour S3

La liste suivante fournit un aperçu de ce à quoi vous pouvez vous attendre ou de ce que vous pouvez faire après avoir activé Malware Protection for S3 pour votre compartiment :

- Choisissez les éléments à analyser : scannez les fichiers au fur et à mesure qu'ils sont chargés dans tous les préfixes ou dans des préfixes spécifiques (jusqu'à 5) associés au compartiment S3 que vous avez sélectionné.
- Analyses automatiques des objets chargés : une fois que vous avez activé la protection contre les programmes malveillants pour S3 pour un compartiment, une analyse est GuardDuty automatiquement lancée pour détecter les logiciels malveillants potentiels dans un objet récemment chargé.
- Activez via la console, en utilisantAPI/AWS CLI, ou AWS CloudFormation — Choisissez une méthode préférée pour activer la protection contre les logiciels malveillants pour S3.

Vous pouvez activer la protection contre les programmes malveillants pour S3 en utilisant des plateformes d'infrastructure en tant que code (IaC) telles que Terraform. Pour plus d'informations, voir Ressource : `aws_guardduty_malware_protection_plan`.

- Formats de fichiers pris en charge, protection contre les programmes malveillants pour les quotas S3 et fonctionnalités Amazon S3 : Malware Protection for S3 prend en charge tous les formats de fichiers que vous pouvez télécharger dans les compartiments S3. Si le fichier téléchargé est protégé par mot de passe, l'analyse du fichier GuardDuty sera ignorée. Pour plus d'informations sur les quotas liés à la taille des objets, au niveau de profondeur d'archivage maximal et pour d'autres informations, consultezQuotas dans la protection contre les malwares pour S3.

  Pour savoir si une fonctionnalité Amazon S3 est prise en charge ou non, consultezSupportabilité des fonctionnalités d'Amazon S3.
- Prend en charge le balisage des objets S3 scannés : lorsque vous activezMarquage facultatif des objets en fonction du résultat de l'analyse, une balise indiquant l'état de l'analyse est ajoutée après chaque analyse de logiciels malveillants. GuardDuty Vous pouvez utiliser cette balise pour configurer le contrôle d'accès basé sur des balises (TBAC) pour les objets S3. Par exemple, vous pouvez restreindre l'accès aux objets S3 indiqués comme malveillants et dont la valeur de balise est égale à`THREATS_FOUND`.
- EventBridge Notifications Amazon : GuardDuty envoie des événements à Amazon EventBridge lorsque le statut des ressources du plan de protection contre les malwares change ou lorsqu'une analyse des programmes malveillants de l'objet S3 est terminée. Ces événements sont envoyés au bus d'événements par défaut. Vous pouvez utiliser ces événements pour écrire EventBridge des règles qui prennent des mesures, par exemple en surveillant le moment où ces événements se produisent. Pour de plus amples informations, veuillez consulter Surveillance avec Amazon EventBridge.
- CloudWatch métriques — Consultez CloudWatch les métriques pour activer les alarmes lors de l'état de certains programmes malveillants. Pour de plus amples informations, veuillez consulter Surveillance des statistiques relatives à l'état du scan à l'aide d'Amazon CloudWatch.

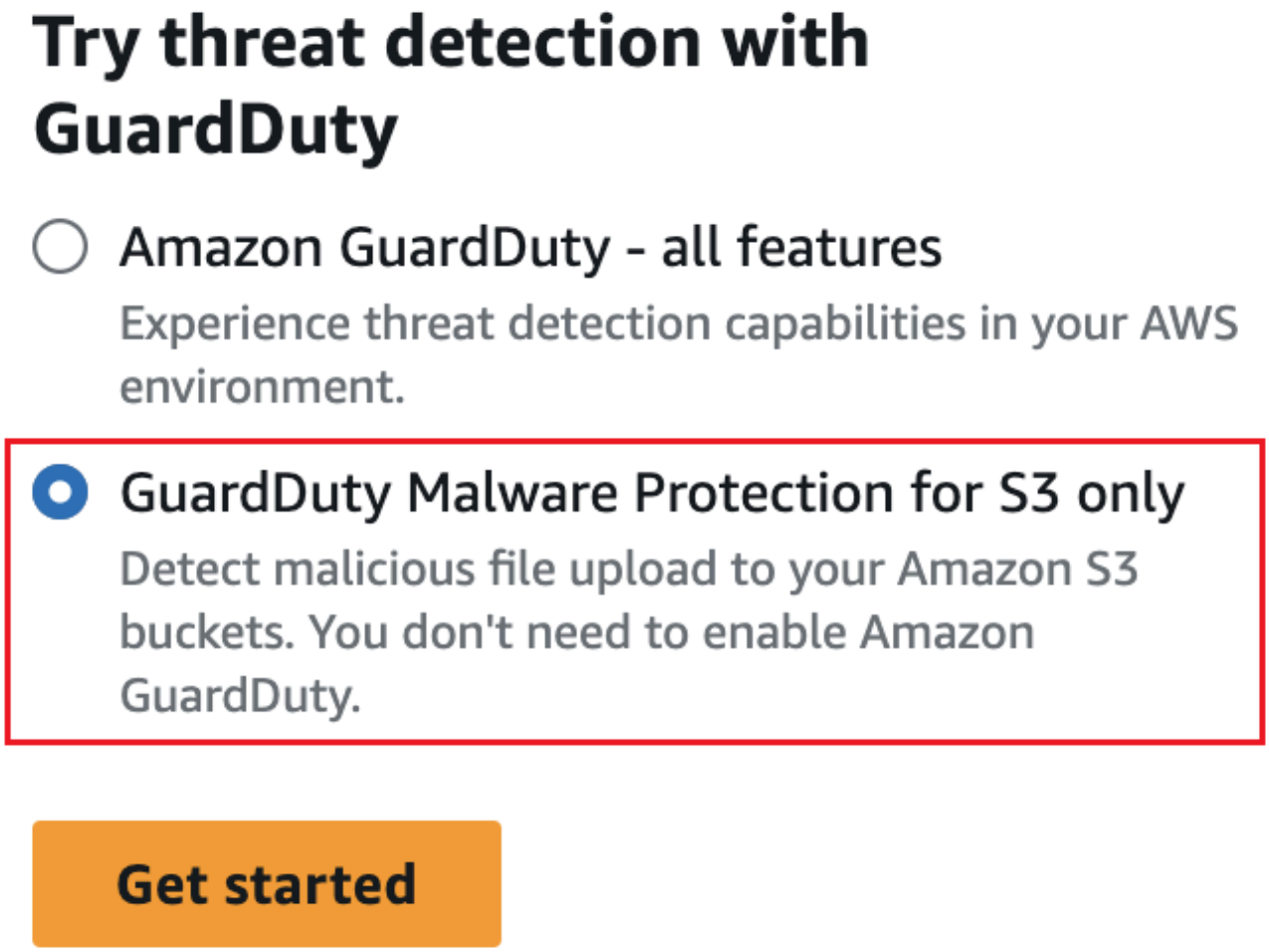
(Facultatif) Commencez à utiliser GuardDuty Malware Protection pour S3 de manière indépendante (console uniquement)

Utilisez cette étape facultative lorsque vous souhaitez commencer à utiliser l'option de détection des menaces Malware Protection for S3 indépendamment de l' GuardDuty état de votre Compte AWS.

Si vous l'avez déjà activée GuardDuty dans votre compte, vous pouvez ignorer cette étape et continuerConfiguration de la protection contre les programmes malveillants pour S3 pour votre compartiment.

Étapes pour démarrer avec Malware Protection pour la détection des menaces uniquement dans S3

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Sélectionnez GuardDuty Malware Protection pour S3 uniquement. Cela vous permet de détecter si un fichier récemment chargé dans votre compartiment Amazon Simple Storage Service (Amazon S3) contient potentiellement un logiciel malveillant.



3. Choisissez Démarrer. Vous pouvez maintenant suivre les étapes ci-dessousConfiguration de la protection contre les programmes malveillants pour S3 pour votre compartiment.

Configuration de la protection contre les programmes malveillants pour S3 pour votre compartiment

Cette section décrit les étapes à suivre pour ajouter une condition préalable et activer la protection contre les programmes malveillants pour S3 pour un compartiment Amazon S3 appartenant à votre propre compte. Les étapes décrites dans les sections suivantes restent les mêmes, que vous démarriez avec Malware Protection for S3 indépendamment ou que vous l'activiez dans le cadre du GuardDuty service.

Procédez comme suit chaque fois que vous souhaitez ajouter cette détection de menace à un compartiment S3.

1. Prérequis : créer ou mettre à jour une politique de IAM rôle
2. Activez la protection contre les programmes malveillants pour S3 pour votre compartiment

Prérequis : créer ou mettre à jour une politique de IAM rôle

Pour que Malware Protection for S3 puisse analyser et (éventuellement) ajouter des balises à vos objets S3, vous devez créer et associer un IAM rôle incluant les autorisations requises suivantes pour :

- Autorisez EventBridge les actions Amazon à créer et à gérer la règle EventBridge gérée afin que Malware Protection for S3 puisse écouter les notifications de vos objets S3.

  Pour plus d'informations, consultez les règles EventBridge gérées par Amazon dans le guide de EventBridge l'utilisateur Amazon.
- Autoriser Amazon S3 et EventBridge les actions à envoyer des notifications EventBridge pour tous les événements de ce compartiment

  Pour plus d'informations, consultez la section Activation d'Amazon EventBridge dans le guide de l'utilisateur Amazon S3.
- Autorisez les actions Amazon S3 à accéder à l'objet S3 chargé et à ajouter une balise prédéfinie à l'objet S3 scanné. `GuardDutyMalwareScanStatus` Lorsque vous utilisez un préfixe d'objet, ajoutez une `s3:prefix` condition uniquement aux préfixes ciblés. Cela GuardDuty empêche l'accès à tous les objets S3 de votre compartiment.

- Autorisez les actions KMS clés à accéder à l'objet avant de scanner et de placer un objet de test sur des compartiments avec le chiffrement KMS et SSE le KMS chiffrement pris en chargeDSSE.

> **Note**
>
> Cette étape est obligatoire chaque fois que vous activez la protection contre les programmes malveillants pour S3 pour un compartiment de votre compte. Si vous possédez déjà un IAM rôle, vous pouvez mettre à jour sa politique pour inclure les détails d'une autre ressource de compartiment S3. La Ajouter des autorisations IAM liées aux politiques rubrique fournit un exemple expliquant comment procéder.

Utilisez les règles suivantes pour créer ou mettre à jour un IAM rôle.

Politiques

- Ajouter des autorisations IAM liées aux politiques
- Ajouter une politique de relation de confiance

Ajouter des autorisations IAM liées aux politiques

Vous pouvez choisir de mettre à jour la politique intégrée d'un IAM rôle existant ou d'en créer un nouveauIAM. Pour plus d'informations sur les étapes, voir Création d'un IAM rôle ou Modification d'une politique d'autorisations de rôle dans le Guide de IAM l'utilisateur.

Ajoutez le modèle d'autorisations suivant à votre IAM rôle préféré. Remplacez les valeurs d'espace réservé suivantes par les valeurs appropriées associées à votre compte :

- Dans *amzn-s3-demo-bucket*, remplacez par le nom de votre compartiment Amazon S3.

  Pour utiliser le même IAM rôle pour plusieurs ressources de compartiment S3, mettez à jour une politique existante, comme illustré dans l'exemple suivant :

```
...
...
"Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"
```

```
                    ],
                    ...
                    ...
```

Assurez-vous d'ajouter une virgule (,) avant d'en ajouter un nouveau ARN associé au compartiment S3. Procédez ainsi chaque fois que vous faites référence à un compartiment S3 `Resource` dans le modèle de politique.

- Dans *111122223333*, remplacez-le par votre Compte AWS identifiant.
- Dans *us-east-1*, remplacez par votre Région AWS.
- Dans *APKAEIBAERJR2EXAMPLE*, remplacez-le par votre identifiant de clé géré par le client. Si votre bucket est chiffré à l'aide d'un AWS KMS key, remplacez la valeur de l'espace réservé par un*, comme indiqué dans l'exemple suivant :

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

IAMmodèle de politique de rôle

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ],
            "Condition": {
                "StringLike": {
                    "events:ManagedBy": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
```

```
        {
            "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
            "Effect": "Allow",
            "Action": [
                "events:DescribeRule",
                "events:ListTargetsByRule"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ]
        },
        {
            "Sid": "AllowPostScanTag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketNotification",
                "s3:GetBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "AllowPutValidationObject",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-
validation-object"
            ]
        },
        {
            "Sid": "AllowCheckBucketOwnership",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
           "Sid": "AllowMalwareScan",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowDecryptForMalwareScan",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                }
            }
        }
    ]
}
```

Ajouter une politique de relation de confiance

Associez la politique de confiance suivante à votre IAM rôle. Pour plus d'informations sur les étapes, consultez la section Modification d'une politique d'approbation des rôles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Activez la protection contre les programmes malveillants pour S3 pour votre compartiment

Cette section fournit des étapes détaillées sur la façon d'activer la protection contre les programmes malveillants pour S3 pour un compartiment sélectionné dans vos propres comptes.

Étapes pour activer la protection contre les programmes malveillants pour S3 pour un compartiment

- Entrez les détails du compartiment S3
- Activer le balisage pour les objets numérisés
- Autorisations
- (Facultatif) Marquez l'identifiant du plan de protection contre les programmes malveillants

Entrez les détails du compartiment S3

Suivez les étapes suivantes pour fournir les détails du compartiment Amazon S3 :

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez activer la protection contre les programmes malveillants pour S3.
3. Dans le volet de navigation, choisissez Malware Protection for S3.
4. Dans la section Compartiments protégés, choisissez Activer pour activer la protection contre les programmes malveillants pour S3 pour un compartiment S3 appartenant au vôtre. Compte AWS
5. Sous Entrez les détails du compartiment S3, entrez le nom du compartiment Amazon S3. Vous pouvez également choisir Browse S3 pour sélectionner un compartiment S3.

   Le Région AWS compartiment S3 et l' Compte AWS endroit où vous activez la protection contre les programmes malveillants pour S3 doivent être identiques. Par exemple, si votre compte appartient à la `us-east-1` région, la région de votre compartiment Amazon S3 doit également l'êtreus-east-1.
6. Sous Préfixe, vous pouvez sélectionner soit tous les objets du compartiment S3, soit les objets commençant par un préfixe spécifique.

   - Sélectionnez Tous les objets du compartiment S3 lorsque vous le souhaitez GuardDuty pour scanner tous les objets récemment téléchargés dans le compartiment sélectionné.
   - Sélectionnez Objets commençant par un préfixe spécifique lorsque vous souhaitez scanner les objets récemment chargés qui appartiennent à un préfixe spécifique. Cette option vous permet de concentrer l'analyse des programmes malveillants uniquement sur les préfixes d'objets sélectionnés. Pour plus d'informations sur l'utilisation des préfixes, consultez la section Organisation des objets dans la console Amazon S3 à l'aide de dossiers dans le guide de l'utilisateur Amazon S3.

     Choisissez Ajouter un préfixe et entrez le préfixe. Vous pouvez ajouter jusqu'à cinq préfixes.

Activer le balisage pour les objets numérisés

Il s'agit d'une étape facultative. Lorsque vous activez l'option de balisage avant qu'un objet ne soit chargé dans votre bucket, une fois l'analyse terminée, GuardDuty vous ajoutez une balise prédéfinie avec la clé as `GuardDutyMalwareScanStatus` et la valeur comme résultat de l'analyse. Pour utiliser Malware Protection for S3 de manière optimale, nous vous recommandons d'activer l'option permettant d'ajouter une balise aux objets S3 une fois l'analyse terminée. Le coût standard du balisage d'objets S3 s'applique. Pour de plus amples informations, veuillez consulter Tarification de la protection contre les programmes malveillants pour S3.

Pourquoi devriez-vous activer le balisage ?

- L'activation du balisage est l'un des moyens de connaître le résultat de l'analyse des logiciels malveillants. Pour plus d'informations sur le résultat d'une analyse des programmes malveillants S3, consultezSurveillance dans le cadre de la protection contre les programmes malveillants pour S3.
- Configurez une politique de contrôle d'accès basée sur des balises (TBAC) sur votre compartiment S3 contenant l'objet potentiellement malveillant. Pour plus d'informations sur les considérations à prendre en compte et sur la manière de mettre en œuvre le contrôle d'accès basé sur des balises (TBAC), consultezUtilisation du contrôle d'accès basé sur des balises (TBAC) avec Malware Protection pour S3.

Considérations relatives GuardDuty à l'ajout d'une balise à votre objet S3 :

- Par défaut, vous pouvez associer jusqu'à 10 balises à un objet. Pour plus d'informations, consultez la section Catégorisation de votre stockage à l'aide de balises dans le guide de l'utilisateur Amazon S3.

  Si les 10 balises sont déjà utilisées, GuardDuty vous ne pouvez pas ajouter la balise prédéfinie à l'objet numérisé. GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour de plus amples informations, veuillez consulter Surveillance avec Amazon EventBridge.
- Lorsque le IAM rôle sélectionné n'inclut pas l'autorisation de GuardDuty baliser l'objet S3, même si le balisage est activé pour votre compartiment protégé, vous ne GuardDuty pourrez pas ajouter de balise à cet objet S3 scanné. Pour plus d'informations sur l'autorisation de IAM rôle requise pour le balisage, consultezPrérequis : créer ou mettre à jour une politique de IAM rôle.

  GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour de plus amples informations, veuillez consulter Surveillance avec Amazon EventBridge.

Pour sélectionner une option sous Marquer les objets numérisés

- Lorsque vous souhaitez ajouter GuardDuty des balises à vos objets S3 numérisés, sélectionnez Étiqueter des objets.
- Si vous ne souhaitez pas ajouter GuardDuty de balises à vos objets S3 numérisés, sélectionnez Ne pas étiqueter les objets.

Autorisations

Suivez les étapes ci-dessous pour choisir un IAM rôle disposant des autorisations nécessaires pour effectuer des actions d'analyse des programmes malveillants en votre nom. Ces actions peuvent inclure l'analyse des objets S3 récemment téléchargés et (éventuellement) l'ajout de balises à ces objets.

Pour choisir un nom de IAM rôle

1. Si vous avez déjà effectué les étapes ci-dessousPrérequis : créer ou mettre à jour une politique de IAM rôle, procédez comme suit :

   - Dans la section Autorisations, pour le nom du IAM rôle, choisissez un nom de IAM rôle qui inclut les autorisations nécessaires.

2. Si vous n'avez pas encore effectué les étapes ci-dessousPrérequis : créer ou mettre à jour une politique de IAM rôle, procédez comme suit :

   a. Choisissez Afficher les autorisations.

   b. Sous Détails des autorisations, choisissez l'onglet Politique. Cela montre un modèle des IAM autorisations requises.

      Copiez ce modèle, puis choisissez Fermer à la fin de la fenêtre Détails des autorisations.

   c. Choisissez Attacher une politique qui ouvre la IAM console dans un nouvel onglet. Vous pouvez choisir de créer un nouveau IAM rôle ou de mettre à jour un IAM rôle existant avec les autorisations du modèle copié.

      Ce modèle inclut des valeurs d'espace réservé que vous devez remplacer par les valeurs appropriées associées à votre compartiment et Compte AWS.

   d. Retournez à l'onglet du navigateur avec la GuardDuty console. Choisissez à nouveau Afficher les autorisations.

   e. Sous Détails des autorisations, choisissez l'onglet Relation de confiance. Cela montre un modèle de politique de relation de confiance pour votre IAM rôle.

      Copiez ce modèle, puis choisissez Fermer à la fin de la fenêtre Détails des autorisations.

   f. Accédez à l'onglet du navigateur dans lequel la IAM console est ouverte. Ajoutez cette politique de relation de confiance à votre IAM rôle préféré.

3. Pour ajouter des balises à l'ID de votre plan de protection contre les programmes malveillants créé pour cette ressource protégée, passez à la section suivante ; sinon, choisissez Activer à la fin de cette page pour ajouter le compartiment S3 en tant que ressource protégée.

(Facultatif) Marquez l'identifiant du plan de protection contre les programmes malveillants

Il s'agit d'une étape facultative qui vous permet d'ajouter des balises à la ressource du plan de protection contre les programmes malveillants qui serait créée pour votre ressource de compartiment S3.

Chaque balise comporte deux parties : une clé de balise et une valeur de balise facultative. Pour plus d'informations sur le balisage et ses avantages, consultez la section Ressources relatives au balisage AWS.

Pour ajouter des balises à la ressource de votre plan de protection contre les programmes malveillants

1. Entrez la clé et une valeur facultative pour le tag. La clé de balise et la valeur de la balise distinguent les majuscules et minuscules. Pour plus d'informations sur les noms de clé de balise et de valeur de balise, voir Limites et exigences en matière de dénomination des balises.
2. Pour ajouter d'autres balises à la ressource de votre plan de protection contre les programmes malveillants, choisissez Ajouter une nouvelle balise et répétez l'étape précédente. Vous pouvez ajouter jusqu'à 50 balises à chaque ressource .
3. Sélectionnez Activer.

Étapes à suivre après avoir activé la protection contre les programmes malveillants pour S3

Après avoir activé la protection contre les programmes malveillants pour S3 pour un compartiment (ou des préfixes d'objets spécifiques), effectuez les étapes suivantes dans l'ordre indiqué :

1. Ajouter une politique de ressource de contrôle d'accès (TBAC) basée sur des balises : lorsque vous activez le balisage, assurez-vous d'ajouter la TBAC politique à la ressource de votre compartiment S3 avant qu'un objet ne soit chargé dans le compartiment sélectionné. Pour de plus amples informations, veuillez consulter Ajout TBAC d'une ressource de compartiment S3.

2. Surveiller l'état du plan de protection contre les programmes malveillants : surveillez la colonne État de chaque compartiment protégé. Pour plus d'informations sur les statuts potentiels et leur signification, consultezÉtat des ressources du plan de protection contre les logiciels malveillants.
3. Téléchargez un objet :
    1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
    2. Téléchargez un fichier dans le compartiment S3 ou dans le préfixe d'objet pour lequel vous avez activé cette fonctionnalité. Pour savoir comment charger un fichier, consultez la section Charger un objet dans votre compartiment dans le guide de l'utilisateur Amazon S3.
4. Surveiller l'état d'analyse de l'objet S3 : cette étape inclut des informations sur la façon de vérifier l'état de l'analyse des programmes malveillants de l'objet S3.

Activé à la fois GuardDuty et protection contre les logiciels malveillants pour S3	Protection contre les programmes malveillants activée pour S3 uniquement
• Lorsqu'il GuardDuty est activé, il peut générer le Protection contre les programmes malveillants pour le type de recherche S3 pour indiquer la présence d'un logiciel malveillant dans l'objet S3 scanné. • Vous pouvez éventuellement vérifier le résultat de l'analyse des objets S3 en utilisant une ou plusieurs options ci-dessousSurveillance dans le cadre de la protection contre les programmes malveillants pour S3. Il s'agit notamment de l'utilisation d'Amazon EventBridge, CloudWatch des métriques pour le plan de protection contre les logiciels malveillants et du marquage des objets numérisés.	Vous pouvez éventuellement vérifier le résultat de l'analyse des objets S3 en utilisant une ou plusieurs options ci-dessousSurveillance dans le cadre de la protection contre les programmes malveillants pour S3. Il s'agit notamment de l'utilisation d'Amazon EventBridge, CloudWatch des métriques pour le plan de protection contre les logiciels malveillants et du marquage des objets numérisés.

État des ressources du plan de protection contre les logiciels malveillants

Cette section décrit les différentes valeurs d'état de protection associées à la ressource de votre plan de protection contre les programmes malveillants.

État	Description
Actif	Votre compartiment S3 a été correctement configuré avec Malware Protection for S3.
Avertissement *	La protection contre les programmes malveillants pour S3 est conçue pour ne pas être affectée lorsqu'un avertissement apparaît. Lorsqu' GuardDuty il détecte un nouvel objet S3, il lance une analyse des logiciels malveillants. Une fois l'analyse lancée avec succès, la valeur de la colonne Status peut prendre quelques minutes pour passer à Active. Vous recevrez une EventBridge notification après la mise à jour de la valeur de la colonne État.
Erreur *	Votre seau n'est pas protégé. Aucune des analyses de programmes malveillants associées à ce compartiment S3 ne sera terminée. Il peut y avoir une ou plusieurs causes profondes potentielles.

* Pour plus d'informations sur les problèmes potentiels et les étapes correspondantes pour les résoudre, consultezRésolution des problèmes liés à l'état du plan de protection contre les.

Résolution des problèmes liés à l'état du plan de protection contre les

Pour tout compartiment protégé, GuardDuty affiche le statut en fonction du classement. Par exemple, si un bucket protégé présente des problèmes dans les catégories Erreur et Avertissement, GuardDuty il affichera d'abord le problème associé au statut d'erreur.

La liste suivante inclut les erreurs et l'avertissement concernant l'état du plan de protection contre les programmes malveillants.

Erreurs

- EventBridge la notification est désactivée pour ce compartiment S3
- EventBridge la règle gérée pour recevoir les événements du compartiment S3 est manquante
- Le compartiment S3 n'existe plus

Warning (Avertissement)

Impossible de mettre l'objet de test

EventBridge la notification est désactivée pour ce compartiment S3

Le code de motif du statut associé est`EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

Détail du statut

GuardDuty utilise EventBridge pour recevoir une notification lorsqu'un nouvel objet est chargé dans ce compartiment S3. Cette autorisation est absente de votre IAM rôle.

Étapes de résolution des problèmes

Option 1 : ajoutez la déclaration d'autorisation suivante à votre IAM rôle :

```
{
          "Sid": "AllowEnableS3EventBridgeEvents",
          "Effect": "Allow",
          "Action": [
             "s3:PutBucketNotification",
             "s3:GetBucketNotification"
             ],
          "Resource": [
             "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
}
```

Remplacez *amzn-s3-demo-bucket* avec le nom de votre compartiment Amazon S3.

Option 2 : activer les EventBridge notifications à l'aide de la console Amazon S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.

2. Sur la page Compartiments, sous l'onglet Compartiments à usage général, sélectionnez le nom du compartiment associé à cette erreur.
3. Sur cette page de bucket, choisissez l'onglet Propriétés.
4. Dans la EventBridge section Amazon, sélectionnez Modifier.
5. Sur la EventBridge page Modifier Amazon, pour Envoyer une notification à Amazon EventBridge pour tous les événements de ce compartiment, sélectionnez Activé.
6. Sélectionnez Enregistrer les modifications.

Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

EventBridge la règle gérée pour recevoir les événements du compartiment S3 est manquante

Le code de motif du statut associé est`EVENTBRIDGE_MANAGED_RULE_DISABLED`.

Détail du statut

Les autorisations des règles EventBridge gérées permettant de gérer la configuration des EventBridge règles sont manquantes.

Étapes de résolution des problèmes

Ajoutez la déclaration d'autorisation suivante à votre IAM rôle :

```
{
         "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
        "Effect": "Allow",
        "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
        "Resource": [
           "arn:aws:events:*:*:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
           ],
        "Condition": {
```

```
            "StringEquals": {
               "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
               }
            }
}
```

Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

Le compartiment S3 n'existe plus

Le code de motif du statut associé est`PROTECTED_RESOURCE_DELETED`.

Détail du statut

Ce compartiment S3 a été supprimé de votre compte et n'existe plus.

Étape de résolution des problèmes

Si la suppression du compartiment S3 n'était pas intentionnelle, vous pouvez en créer un nouveau à l'aide de la console Amazon S3.

Après avoir créé le compartiment avec succès, activez Malware Protection pour S3 en suivant les étapes décrites dans la Configuration de la protection contre les programmes malveillants pour S3 pour votre compartiment page.

Impossible de mettre l'objet de test

Le code de motif du statut associé est`INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

> **Note**
>
> L'autorisation d'ajouter un objet de test est facultative. L'absence de cette autorisation dans votre IAM rôle n'empêche pas Malware Protection for S3 de lancer une analyse des programmes malveillants sur un objet récemment chargé. Une fois l'analyse lancée avec succès, le passage de l'état du plan de protection contre les programmes malveillants de Avertissement à Actif peut prendre quelques minutes.
> Si le IAM rôle inclut déjà cette autorisation, cet avertissement indique une politique de compartiment Amazon S3 restrictive qui n'autorise pas le IAM rôle à inclure cette autorisation.

Détail du statut

Pour valider la configuration du bucket sélectionné, GuardDuty place un objet de test dans votre bucket.

Étapes de résolution des problèmes

Vous pouvez choisir de mettre à jour le IAM rôle pour inclure les autorisations manquantes. Au IAM rôle sélectionné, ajoutez les autorisations suivantes GuardDuty afin de placer l'objet de test sur la ressource sélectionnée :

```
{
         "Sid": "AllowPutValidationObject",
         "Effect": "Allow",
         "Action": [
           "s3:PutObject"
           ],
         "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-
object"
           ]
}
```

Remplacez *amzn-s3-demo-bucket* avec le nom de votre compartiment Amazon S3. Pour plus d'informations sur les autorisations des IAM rôles, consultezPrérequis : créer ou mettre à jour une politique de IAM rôle.

Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

Surveillance dans le cadre de la protection contre les programmes malveillants pour S3

Lorsque vous utilisez Malware Protection for S3 avec un identifiant de GuardDuty détecteur, si votre objet Amazon S3 est potentiellement malveillant, il GuardDuty sera généréProtection contre les programmes malveillants pour le type de recherche S3. À l'aide de la GuardDuty consoleAPIs, vous pouvez consulter les résultats générés. Pour plus d'informations sur la compréhension de ce type de recherche, consultezDétails d'un résultat.

Lorsque vous utilisez Malware Protection for S3 sans l'activer GuardDuty (aucun identifiant de détecteur), même si votre objet Amazon S3 scanné est potentiellement malveillant, GuardDuty vous ne pouvez générer aucun résultat.

La liste suivante fournit les valeurs d'état potentielles des résultats d'analyse d'objets S3 :

- `NO_THREATS_FOUND`— n'a GuardDuty détecté aucune menace potentielle associée à l'objet scanné.
- `THREATS_FOUND`— GuardDuty a détecté une menace potentielle associée à l'objet scanné.
- `UNSUPPORTED`— Il existe plusieurs raisons pour lesquelles Malware Protection for S3 ignore une analyse. Les raisons potentielles incluent un fichier protégé par mot de passe, la protection contre les programmes malveillants pour les quotas S3 et certaines fonctionnalités d'Amazon S3. Pour de plus amples informations, veuillez consulter Fonctionnalités de protection contre les malwares pour S3.
- `ACCESS_DENIED`— GuardDuty Impossible d'accéder à cet objet pour le scanner. Vérifiez les autorisations de IAM rôle associées à ce compartiment. Pour de plus amples informations, veuillez consulter Prérequis : créer ou mettre à jour une politique de IAM rôle.
- `FAILED`— GuardDuty impossible d'effectuer une analyse des programmes malveillants sur cet objet en raison d'une erreur interne.

La liste suivante fournit les valeurs d'état potentielles de l'analyse des objets S3 et leur mappage avec le résultat de l'analyse des objets S3 :

- Terminé — L'analyse s'est terminée avec succès et indique si l'objet S3 contient un logiciel malveillant. Dans ce cas, la valeur potentielle du résultat de l'analyse d'un objet S3 peut être l'une `THREATS_FOUND` ou l'autre`NO_THREATS_FOUND`.
- Ignorée : GuardDuty ignore une analyse des programmes malveillants lorsque les détails de l'objet S3 ne sont pas alignés sur le Quotas dans la protection contre les malwares pour S3 compartiment sélectionné ou si vous GuardDuty n'avez pas accès à l'objet S3 chargé dans le compartiment sélectionné.

  Dans ce cas, la valeur potentielle du résultat de l'analyse d'un objet S3 peut être l'une `UNSUPPORTED` ou l'autre`ACCESS_DENIED`.
- Échec : similaire à la valeur du résultat de l'analyse de l'objet S3`FAILED`, cet état d'analyse signifie qu'il n' GuardDuty a pas été possible d'effectuer une analyse des programmes malveillants sur l'objet S3 en raison d'une erreur interne.

Rubriques

Surveillance avec 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. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications oftware-as-a S-Service (SaaS) et AWS services et achemine ces données vers des cibles telles que Lambda. Cela vous permet de surveiller les événements qui se produisent dans les services et de créer des architectures basées sur les événements. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

En tant que compte propriétaire d'un compartiment S3 protégé par Malware Protection for S3, il GuardDuty publie EventBridge des notifications sur le bus d'événements par défaut dans les scénarios suivants :

- La protection contre les programmes malveillants planifie les modifications de l'état des ressources pour tous vos compartiments protégés. Pour plus d'informations sur les différents statuts, consultezÉtat des ressources du plan de protection contre les logiciels malveillants.
- Un événement de balise a échoué pour les raisons suivantes :
  - Votre IAM rôle ne dispose pas des autorisations nécessaires pour étiqueter l'objet.

    Le Ajouter des autorisations IAM liées aux politiques modèle inclut l'autorisation de GuardDuty baliser un objet.
  - La ressource ou l'objet du bucket spécifié dans le IAM rôle n'existe plus.
  - L'objet S3 associé a déjà atteint la limite maximale de balises. Pour plus d'informations sur la limite de balises, consultez la section Catégorisation de votre stockage à l'aide de balises dans le guide de l'utilisateur Amazon S3.
- Le résultat de l'analyse des objets S3 est publié sur votre bus d' EventBridge événements par défaut.

Configurer des EventBridge règles

Vous pouvez configurer des EventBridge règles dans votre compte pour envoyer soit l'état des ressources, soit les événements d'échec des balises après le scan, soit le résultat de l'analyse des objets S3 à une autre AWS service personne. En tant que compte GuardDuty administrateur délégué, vous recevrez la notification de l'état des ressources du plan de protection contre les programmes malveillants en cas de modification du statut.

La EventBridge tarification standard s'appliquera. Pour plus d'informations, consultez les EventBridge tarifs Amazon.

Toutes les valeurs qui apparaissent dans *red* sont des espaces réservés pour l'exemple. Ces valeurs changeront en fonction des valeurs de votre compte et de la détection ou non d'un logiciel malveillant.

État des ressources du plan de protection contre les logiciels malveillants

Vous pouvez créer un modèle d' EventBridge événement basé sur les scénarios suivants :

`detail-type`Valeurs potentielles

- `"GuardDuty Malware Protection Resource Status Active"`
- `"GuardDuty Malware Protection Resource Status Warning"`
- `"GuardDuty Malware Protection Resource Status Error"`

Schéma d'événement

```
{
      "detail-type": ["potential detail-type"],
      "source": ["aws.guardduty"]
}
```

Exemple de schéma de notification pour **`GuardDuty Malware Protection Resource Status Active`** :

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status Active",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
```

```
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ACTIVE"
    }
}
```

Exemple de schéma de notification pour **`GuardDuty Malware Protection Resource Status Warning`** :

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status warning",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "WARNING",
        "statusReasons": [
         {
            "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
         }
        ]
    }
}
```

Exemple de schéma de notification pour **`GuardDuty Malware Protection Resource Status Error`** :

```
{
    "version": "0",
    "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
    "detail-type": "GuardDuty Malware Protection Resource Status Error",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ERROR",
        "statusReasons": [
        {
            "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
        }
       ]
    }
}
```

En fonction de la raison `resourceStatus`ERROR, la `statusReasons` valeur sera renseignée.

Pour plus d'informations sur les étapes de résolution des problèmes liés aux avertissements et erreurs suivants, consultezRésolution des problèmes liés à l'état du plan de protection contre les.

Résultat de l'analyse d'objets S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Exemple de schéma de notification pour **`NO_THREATS_FOUND`** :

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
```

```
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "threats": null
        }
    }
}
```

Exemple de schéma de notification pour **THREATS_FOUND** :

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
```

```
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "threats": [
                {
                    "name": "EICAR-Test-File (not a virus)"
                }
            ]
        }
    }
}
```

Exemple de schéma de notification pour l'état des résultats du scan **UNSUPPORTED** (ignoré) :

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "UNSUPPORTED",
            "threats": null
        }
    }
}
```

Exemple de schéma de notification pour l'état des résultats du scan **ACCESS_DENIED** (ignoré) :

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "ACCESS_DENIED",
            "threats": null
        }
    }
}
```

Exemple de schéma de notification pour l'état des résultats du scan **FAILED** :

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
```

```
        "scanStatus": "FAILED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "FAILED",
            "threats": null
        }
    }
}
```

Événements de défaillance des balises après la numérisation

Schéma de l'événement :

```
{
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
 }
```

Exemple de schéma de notification pour **`ACCESS_DENIED`** :

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
```

```
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "status": "FAILED",
            "failureReason": "ACCESS_DENIED"
        }]
    }
}
```

Exemple de schéma de notification pour **`MAX_TAG_LIMIT_EXCEEDED`** :

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "status": "FAILED",
            "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
        }]
    }
}
```

Pour résoudre ces causes de défaillance, voirRésolution des défaillances des balises après numérisation des objets S3.

Surveillance des statistiques relatives à l'état du scan à l'aide d'Amazon CloudWatch

Vous pouvez surveiller GuardDuty l'utilisation CloudWatch, qui collecte les données brutes et les transforme en indicateurs lisibles en temps quasi réel. Ces statistiques sont conservées pendant 15 mois, afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de Malware Protection for S3. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Les CloudWatch métriques relatives à Malware Protection for S3 sont disponibles au niveau des ressources. Vous pouvez interroger ces métriques séparément pour chaque ressource protégée. Les métriques sont signalées dans l'espace de `AWS/GuardDuty/MalwareProtection` noms. Vous pouvez configurer des alarmes sur des ressources spécifiques afin de surveiller le niveau de sécurité.

Mesures d'état de l'analyse des programmes malveillants

Métrique	Description
`CompletedScanCount`	Nombre d'analyses de programmes malveillants sur des objets S3 effectuées dans un laps de temps donné. Dimensions valides : • `Malware Protection Plan Id` `Resource Name` Unités : nombre
`FailedScanCount`	Nombre d'analyses de programmes malveillants sur des objets S3 effectuées dans un laps de temps donné. Dimensions valides : • `Malware Protection Plan Id`

	`Resource Name` Unités : nombre

`SkippedScanCount`	Nombre d'analyses de programmes malveillants sur des objets S3 qui ont été ignorées au cours d'une période donnée.
	
	Dimensions valides :
	
	• `Malware Protection Plan Id`
	
	`Resource Name`
	
	`Skipped Reason`
	
	Valeurs potentielles
	
	• `UnSupported`
	• `MissingPermissions`
	
	Unités : nombre

Mesures des résultats de l'analyse des logiciels malveillants	
`InfectedScanCount`	Nombre d'analyses de programmes malveillants sur des objets S3 qui ont détecté un objet potentiellement malveillant au cours d'une période donnée. Dimensions valides : • `Malware Protection Plan Id` `Resource Name` Unités : nombre

`CompletedScanBytes`	Le nombre d'octets d'objets S3 analysés au cours d'une période donnée. Dimensions valides : • `Malware Protection Plan Id` `Resource Name` Unités : nombre

> **Note**
>
> Par défaut, les statistiques des CloudWatch métriques sontAVG.

Les dimensions suivantes sont prises en charge pour les métriques de protection contre les programmes malveillants pour S3.

Dimension	Description
`Malware Protection Plan Id`	Identifiant unique associé à la ressource du plan de protection contre les programme s malveillants GuardDuty créée pour votre ressource protégée.
`Resource Name`	Le nom de la ressource protégée.
`Skipped Reason`	La raison pour laquelle une analyse des malwares liés à un objet S3 a été ignorée. Valeurs potentielles • `UnSupported` • `MissingPermissions`

Pour plus d'informations sur l'accès à ces statistiques et leur interrogation, consultez la section Utiliser CloudWatch les métriques Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations sur la configuration des alarmes, consultez la section Utilisation des CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

Surveillance à l'aide de balises d'objets S3

Utilisez l'option d'activation du balisage afin d' GuardDuty ajouter des balises à votre objet Amazon S3 une fois l'analyse des logiciels malveillants terminée.

Considérations relatives à l'activation du balisage

- Il y a un coût d'utilisation associé lorsque vous GuardDuty balisez vos objets S3. Pour de plus amples informations, veuillez consulter Tarification de la protection contre les programmes malveillants pour S3.
- Vous devez conserver les autorisations de balisage requises pour votre IAM rôle préféré associé à ce compartiment ; sinon, GuardDuty vous ne pourrez pas ajouter de balises à vos objets numérisés. Le IAM rôle inclut déjà les autorisations permettant d'ajouter des balises aux objets S3 scannés. Pour de plus amples informations, veuillez consulter Prérequis : créer ou mettre à jour une politique de IAM rôle.
- Par défaut, vous pouvez associer jusqu'à 10 balises à un objet S3. Pour de plus amples informations, veuillez consulter Utilisation du contrôle d'accès basé sur des balises () TBAC.

Une fois que vous avez activé le balisage pour un compartiment S3 ou pour des préfixes spécifiques, tout objet récemment chargé qui est scanné sera associé à une balise au format de paire clé-valeur suivant :

`GuardDutyMalwareScanStatus:`*`Scan-Status`*

Pour plus d'informations sur les valeurs de balise potentielles, consultezUtilisation du contrôle d'accès basé sur des balises () TBAC.

Résolution des défaillances des balises après le scan des objets S3 dans Malware Protection for S3

Cette section ne s'applique à vous que si vous êtes Activer le balisage pour les objets numérisés dans votre compartiment protégé.

Lorsque GuardDuty vous tentez d'ajouter une balise à votre objet S3 numérisé, l'action de balisage peut entraîner un échec. Les raisons potentielles pour lesquelles cela peut arriver à votre compartiment sont `ACCESS_DENIED` et`MAX_TAG_LIMIT_EXCEEDED`. Consultez les rubriques suivantes pour comprendre les causes potentielles de ces défaillances des balises après le scan et pour les résoudre.

ACCESS_DENIED

La liste suivante fournit les raisons potentielles pouvant être à l'origine de ce problème :

- L'AllowPostScanTagautorisation n'est pas requise pour le IAM rôle utilisé pour ce compartiment S3 protégé. Vérifiez que le IAM rôle associé utilise cette politique de compartiment. Pour de plus amples informations, veuillez consulter Prérequis : créer ou mettre à jour une politique de IAM rôle.
- La politique de compartiment S3 protégé n'autorise pas GuardDuty l'ajout de balises à cet objet.
- L'objet S3 scanné n'existe plus.

MAX_TAG_LIMIT_EXCEEDED

Par défaut, vous pouvez associer jusqu'à 10 balises à un objet S3. Pour plus d'informations, consultez la section Considérations relatives GuardDuty à l'ajout d'une balise à votre objet S3 sousActiver le balisage pour les objets numérisés.

Utilisation du contrôle d'accès basé sur des balises (TBAC) avec Malware Protection pour S3

Lorsque vous activez Malware Protection for S3 pour votre compartiment, vous pouvez éventuellement choisir d'activer le balisage. Après avoir tenté de scanner un objet S3 récemment chargé dans le compartiment sélectionné, GuardDuty ajoute une balise à l'objet scanné pour indiquer l'état de l'analyse des programmes malveillants. Un coût d'utilisation direct est associé à l'activation du balisage. Pour de plus amples informations, veuillez consulter Tarification de la protection contre les programmes malveillants pour S3.

GuardDuty utilise une balise prédéfinie avec la clé as `GuardDutyMalwareScanStatus` et la valeur comme l'un des statuts d'analyse des programmes malveillants. Pour plus d'informations sur ces valeurs, consultezS3 object potential scan result values.

Considérations relatives GuardDuty à l'ajout d'une balise à votre objet S3 :

- Par défaut, vous pouvez associer jusqu'à 10 balises à un objet. Pour plus d'informations, consultez la section Catégorisation de votre stockage à l'aide de balises dans le guide de l'utilisateur Amazon S3.

  Si les 10 balises sont déjà utilisées, GuardDuty vous ne pouvez pas ajouter la balise prédéfinie à l'objet numérisé. GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour de plus amples informations, veuillez consulter Surveillance avec Amazon EventBridge.
- Lorsque le IAM rôle sélectionné n'inclut pas l'autorisation de GuardDuty baliser l'objet S3, même si le balisage est activé pour votre compartiment protégé, vous ne GuardDuty pourrez pas ajouter de balise à cet objet S3 scanné. Pour plus d'informations sur l'autorisation de IAM rôle requise pour le balisage, consultezPrérequis : créer ou mettre à jour une politique de IAM rôle.

  GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour de plus amples informations, veuillez consulter Surveillance avec Amazon EventBridge.

Ajout TBAC d'une ressource de compartiment S3

Vous pouvez utiliser les politiques de ressources du compartiment S3 pour gérer le contrôle d'accès basé sur des balises (TBAC) pour vos objets S3. Vous pouvez autoriser des utilisateurs spécifiques à accéder à l'objet S3 et à le lire. Si votre organisation a été créée en utilisant AWS Organizations, vous devez faire en sorte que personne ne puisse modifier les balises ajoutées par GuardDuty. Pour plus d'informations, consultez la section Empêcher la modification des balises, sauf par des personnes autorisées, dans le Guide de l'AWS Organizations utilisateur. L'exemple utilisé dans le sujet lié mentionne`ec2`. Lorsque vous utilisez cet exemple, remplacez *`ec2`* avec `s3`.

La liste suivante explique ce que vous pouvez faire en utilisant TBAC :

- Empêchez tous les utilisateurs, à l'exception du principal de service Malware Protection for S3, de lire les objets S3 qui ne sont pas encore balisés avec la paire clé-valeur de balise suivante :

  `GuardDutyMalwareScanStatus:`*`Potential key value`*
- GuardDuty Autoriser uniquement l'ajout de la clé de balise `GuardDutyMalwareScanStatus` avec une valeur comme résultat de numérisation, à un objet S3 scanné. Le modèle de politique suivant peut permettre à des utilisateurs spécifiques qui y ont accès de potentiellement remplacer la paire clé-valeur du tag.

Exemple de politique de ressources du compartiment S3 :

Remplacez *IAM-role-name* avec le IAM rôle que vous avez utilisé pour configurer Malware Protection pour S3 dans votre compartiment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "NoReadExceptForClean",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:iam::555555555555:root",
                    "arn:aws:iam::555555555555:role/IAM-role-name",
                    "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
 "NO_THREATS_FOUND"
                }
            }
        },
        {
            "Sid": "OnlyGuardDutyCanTag",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:iam::555555555555:root",
                    "arn:aws:iam::555555555555:role/IAM-role-name",
                    "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
                ]
```

```
            },
            "Action": "s3:PutObjectTagging",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

Pour plus d'informations sur le balisage de votre ressource S3, les politiques de balisage et de contrôle d'accès.

Modification de la protection contre les programmes malveillants pour S3 pour un compartiment protégé

Procédez comme suit pour modifier la configuration existante de votre compartiment S3 protégé :

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Malware Protection for S3.
3. Sous Compartiments protégés, sélectionnez le compartiment pour lequel vous souhaitez modifier la configuration existante.
4. Choisissez Modifier.
5. Mettez à jour la configuration et les paramètres existants de votre compartiment et confirmez les modifications. Pour plus d'informations sur la description et les étapes de chaque section, consultezActivez la protection contre les programmes malveillants pour S3 pour votre compartiment.

   Surveillez la colonne État de ce compartiment protégé. S'il apparaît sous la forme d'un avertissement ou d'une erreur, consultezRésolution des problèmes liés à l'état du plan de protection contre les.

Affichage de l'utilisation et du coût de Malware Protection for S3

Votre compte commence à être soumis à des frais d'utilisation lorsque vous utilisez Malware Protection for S3 au-delà de la limite spécifiée dans le plan Free Tier ou lorsque le plan Free

Tier de 12 mois de votre compte prend fin. Pour plus d'informations sur le plan Free Tier, consultezTarification de la protection contre les programmes malveillants pour S3.

Pour consulter le coût d'utilisation, accédez à Cost Explorer dans la console https://console.aws.amazon.com/billing/. Pour plus d'informations sur Compte AWS la facturation, consultez le guide de AWS Billing l'utilisateur.

Désactiver la protection contre les programmes malveillants pour S3 pour un compartiment protégé

Lorsque vous désactivez la protection contre les programmes malveillants pour S3 pour un compartiment protégé, l'ID du GuardDuty plan de protection contre les programmes malveillants associé à ce compartiment est supprimé. GuardDuty ne lancera plus d'analyse des programmes malveillants lorsqu'un nouvel objet est chargé dans ce compartiment ou dans l'un des préfixes d'objets sélectionnés.

Si vous avez activé GuardDuty et souhaitez maintenant le suspendre ou le désactiver GuardDuty, consultezSuspension ou désactivation GuardDuty. Comme il n'existe aucun concept d'identifiant de détecteur dans Malware Protection for S3, la désactivation ou la suspension GuardDuty n'a aucune incidence sur le statut d'un compartiment protégé dans votre compte. Vous pouvez continuer à utiliser la fonctionnalité Malware Protection for S3 indépendamment avec le tarif standard associé. Pour plus d’informations, consultez Affichage de l'utilisation et du coût de Malware Protection for S3. Pour arrêter d'utiliser Malware Protection for S3, vous devez la désactiver pour tous les compartiments protégés de votre compte. Si vous souhaitez continuer à utiliser GuardDuty et désactiver uniquement Malware Protection for S3 pour un bucket, les étapes suivantes n'auront aucune incidence sur la configuration du GuardDuty service ni sur les autres plans de protection que vous avez peut-être activés.

Pour désactiver la protection contre les programmes malveillants pour S3 pour un compartiment protégé

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Malware Protection for S3.
3. Sous Compartiments protégés, sélectionnez le compartiment pour lequel vous souhaitez désactiver la protection contre les programmes malveillants pour S3.

Vous ne pouvez sélectionner qu'un seul compartiment protégé à la fois. Pour désactiver la protection contre les programmes malveillants pour S3 pour plusieurs compartiments, suivez à nouveau ces étapes pour un autre compartiment S3.

4. Choisissez Désactiver.
5. Choisissez Désactiver pour confirmer la sélection.

Supportabilité des fonctionnalités d'Amazon S3

Le tableau suivant indique si Malware Protection for S3 prend en charge les fonctionnalités Amazon S3 répertoriées.

Le support est-il disponible ?	Description
Oui	Les objets S3 peuvent être récupérés sans restauration asynchrone.

Le support est-il disponible ?	Description

Le support est-il disponible ?	Description
Conditionnel	• La prise en charge de la hiérarchisation intelligente est disponible pour les objets S3 dans les niveaux Frequent, Infrequent et Archive Instance Access. • Les niveaux opt-in Archive et Deep Archive ne sont pas pris en charge. • La hiérarchisation intelligente crée toujours un nouvel objet dans le niveau Accès fréquent. Par conséquent, le scan d'objets lors de la création est pris en charge. • Les futures fonctionnalités de hiérarchisation intellige nte pourraient démarrer les objets dans Archive. Par conséquent, cela n'est pas pris en charge.
Non	GuardDuty ne prend en charge que les compartiments à usage général pour la protection contre les logiciels malveillants pour S3.

Le support est-il disponible ?	Description
Non	Les objets S3 doivent être restaurés avant d'être accessibles.
Non	La protection contre les programmes malveillants pour S3 n'est pas prise en charge sur Outposts.

Le support est-il disponible ?	Description
Oui	Tous les objets S3 chargés sont analysés pour détecter la présence de malwares. Si vous avez chargé un objet avec la version de fichier v1 et que vous avez immédiate ment téléchargé une autre version, remplacez par v2, les versions v1 et v2 du fichier objet GuardDuty seront analysées à la fois. Cependant, il se peut que l'heure de début de l'analyse ne soit pas dans le même ordre.
Oui	Si le compartiment de destination est une ressource protégée, il GuardDuty scannera tous les objets S3 et les répliquera vers les préfixes protégés et surveillés.
Non	Vous ne pouvez pas définir de règle de réplication en fonction de la balise de résultat du scan. Amazon S3 ne prend pas en charge la réplication pour les balises, sauf lors de la création.

Le support est-il disponible ?	Description
Oui	GuardDuty prend en charge les analyses de programme s malveillants pour les objets S3 chiffrés à l'aide de clés gérées et gérées par le client. Assurez-vous que le IAM rôle inclut l'autorisation d'utiliser la clé. Pour de plus amples informations, veuillez consulter Ajouter des autorisations IAM liées aux politiques.

Le support est-il disponible ?	Description
Non	Malware Protection for S3 ne prend pas en charge l'analyse des objets S3 chiffrés avec des clés inaccessibles.
Non	Lorsque vos objets S3 sont chiffrés à l'aide du client de chiffrement Amazon S3, ils ne sont exposés à aucun tiers, y compris AWS. Pour plus d'informations sur les raisons pour lesquelles cela n'est pas pris en charge, consultez la section Protection des données à l'aide du chiffrement côté client dans le guide de l'utilisateur Amazon S3.

Le support est-il disponible ?	Description
Oui	Les objets S3 verrouillés sont verrouillés selon le WORM principe « Write Once Read Many ». Malware Protection for S3 peut accéder aux objets et les scanner.
Oui	Malware Protection for S3 peut scanner les buckets configurés avec Requester Pays. Le demandeur paiera les appels S3. Pour plus d'informations, consultez Utilisation des compartiments de type Paiement par le demandeur pour les transferts et l'utilisation du stockage dans le Guide de l'utilisateur Amazon S3.
Oui	Vous pouvez définir des politiques de cycle de vie en fonction de la balise de résultat du scan. Supprimez automatiquement les objets malveillants, par exemple. Pour plus d'informations sur la configuration du cycle de vie, consultez Gérer le cycle de vie de votre stockage dans le guide de l'utilisateur Amazon S3.

Le support est-il disponible ?	Description
Oui	Vous pouvez définir des politiques de ressources de compartiment en fonction de votre balise de résultat d'analyse d'objets S3. Par exemple, empêchez l'accès aux objets S3 qui ne sont pas encore scannés ou aux menaces GuardDuty détectées. Pour de plus amples informations, veuillez consulter Utilisation du contrôle d'accès basé sur des balises (TBAC) avec Malware Protection pour S3.

Quotas dans la protection contre les malwares pour S3

Cette section fournit des quotas par défaut, souvent appelés limites. Sauf indication contraire, chaque quota est spécifique à une région. Pour consulter les quotas par défaut spécifiques à l'utilisation du GuardDuty service de base (ou principal), consultez GuardDuty Quotas Amazon.

Les tableaux suivants décrivent les multiples quotas qui s'appliqueront à votre Compte AWS.

AWS valeur de quota par défaut	Est-il ajustable ?	Description
5 Go	Non	Taille maximale de l'objet S3 qui GuardDuty tentera de détecter les logiciels malveillants.

AWS valeur de quota par défaut	Est-il ajustable ?	Description
5 Go	Non	Quantité maximale de données (en Go) GuardDuty pouvant être extraites et analysées à partir d'un fichier d'archive . Même si un fichier d'archive contient plus de 5 Go, le contenu au-delà de cette valeur GuardDuty sera ignoré.
1 000	Non	Nombre maximal de fichiers GuardDuty pouvant être extraits et analysés dans un fichier d'archive. Si le fichier contient plus de 1 000 fichiers, vous GuardDuty devrez ignorer le fichier archivé.
5	Non	Les niveaux maximaux d'archives imbriquées GuardDuty pouvant être extraites. Si l'archive inclut des fichiers imbriqués au-delà de cette valeur, ces fichiers imbriqués GuardDuty seront ignorés.
25	Non	Nombre maximal de compartiments S3 pour lesquels vous pouvez activer la protection contre les programmes malveillants pour S3. Cette limite de quota est fixée par compte dans chaque région.

AWS valeur de quota par défaut	Est-il ajustable ?	Description
25	Au niveau de la région	Le nombre maximum d'opérations du plan de contrôle pouvant être initiées par seconde dans chaque région. Les API opérations incluent la création, la lecture, la mise à jour et la suppression de ressources. Cette valeur de quota s'applique au niveau de la région.

GuardDuty RDSProtection

RDSLa protection d'Amazon GuardDuty analyse et établit le profil des activités de RDS connexion pour détecter les menaces d'accès potentielles à vos bases de données Amazon Aurora (Amazon Aurora My SQL -Compatible Edition et Aurora Postgre SQL -Compatible Edition) et à Amazon RDS pour Postgre. SQL Cette fonctionnalité vous permet d'identifier les comportements de connexion potentiellement suspects. RDSLa protection ne nécessite aucune infrastructure supplémentaire ; elle est conçue de manière à ne pas affecter les performances de vos instances de base de données.

Lorsque RDS la Protection détecte une tentative de connexion potentiellement suspecte ou anormale indiquant une menace pour votre base de données, GuardDuty génère un nouveau résultat contenant des informations détaillées sur la base de données potentiellement compromise.

Vous pouvez activer ou désactiver la fonctionnalité de RDS protection pour n'importe quel compte, Région AWS partout où cette fonctionnalité est disponible sur Amazon GuardDuty, à tout moment. Un GuardDuty compte existant peut activer RDS Protection avec une période d'essai de 30 jours. Pour un nouveau GuardDuty compte, RDS la protection est déjà activée et incluse dans la période d'essai gratuite de 30 jours. Pour de plus amples informations, veuillez consulter Estimation du coût.

> **Note**
>
> Lorsque la fonction de RDS protection n'est pas activée, elle GuardDuty ne collecte pas votre activité de RDS connexion et ne détecte aucun comportement de connexion anormal ou suspect.

Pour plus d'informations sur Régions AWS Where qui GuardDuty ne prend pas encore en charge RDS la protection, consultezDisponibilité des fonctionnalités propres à la région.

RDSBases de données Amazon Aurora et Amazon prises en charge

Le tableau suivant indique les versions de base de RDS données Aurora et Amazon prises en charge.

Amazon Aurora et moteur de base de RDS données Amazon	Versions de moteur prises en charge
Aurora My SQL	• Versions 2.10.2 ou ultérieures • Versions 3.02.1 ou ultérieures
Poster Aurora SQL	• Versions 10.17 ou ultérieures • Versions 11.12 ou ultérieures • Versions 12.7 ou ultérieures • Versions 13.3 ou ultérieures • Versions 14.3 ou ultérieures • 15.2 ou version ultérieure • 16.1 ou version ultérieure
RDSpour Postgre SQL	• 14.5 ou version ultérieure • 13.8 ou version ultérieure • 12.12 ou version ultérieure • 11.17 ou version ultérieure • 10.22 ou version ultérieure • RDSpour Postgre SQL version 15 • RDSpour Postgre SQL version 16

Comment RDS Protection utilise la surveillance RDS de l'activité de connexion

RDSLa protection d'Amazon vous GuardDuty aide à protéger les SQL bases de données Amazon Aurora (Aurora) prises en RDS charge et Postgre dans votre compte. Après avoir activé la fonction de RDS protection, commence GuardDuty immédiatement à surveiller l'activité de RDS connexion à partir des bases de données Aurora et d'Amazon sur RDS votre compte. GuardDuty surveille et profile en permanence les activités de RDS connexion pour détecter toute activité suspecte, par exemple un accès non autorisé à la base de données Aurora depuis votre compte, par un acteur externe invisible auparavant. Lorsque vous activez la RDS protection pour la première fois ou que vous avez une instance de base de données nouvellement créée, une période d'apprentissage

est nécessaire pour définir un comportement normal. Pour cette raison, il est possible que les instances de base de données nouvellement activées ou créées n'aient aucun résultat de connexion anormale pendant jusqu'à deux semaines. Pour de plus amples informations, veuillez consulter RDSsurveillance de l'activité de connexion.

Lorsque RDS Protection détecte une menace potentielle, telle qu'un schéma inhabituel issu d'une série de tentatives de connexion réussies, échouées ou incomplètes, GuardDuty génère un nouveau résultat contenant des informations détaillées sur l'instance de base de données potentiellement compromise. Pour de plus amples informations, veuillez consulter Types de résultat de la protection RDS. Si vous désactivez RDS la protection, la surveillance de l'activité de RDS connexion s'arrête GuardDuty immédiatement et vous ne pouvez détecter aucune menace potentielle pour vos instances de base de données prises en charge.

> **Note**
>
> GuardDuty ne gère pas votre activité Bases de données prises en charge ou votre activité de RDS connexion, et ne met pas l'activité de RDS connexion à votre disposition.

Fonctionnalité de RDS la protection

RDSsurveillance de l'activité de connexion

RDSl'activité de connexion capture les tentatives de connexion réussies et infructueuses effectuées RDSBases de données Amazon Aurora et Amazon prises en charge dans votre AWS environnement. Pour vous aider à protéger vos bases de données, GuardDuty RDS Protection surveille en permanence l'activité de connexion afin de détecter toute tentative de connexion potentiellement suspecte. Par exemple, un adversaire peut tenter d'accéder par force brute à une base de données Amazon Aurora en devinant le mot de passe de la base de données.

Lorsque vous activez la fonction de RDS protection, elle commence GuardDuty automatiquement à surveiller l'activité de RDS connexion à vos bases de données directement depuis les RDS services Aurora et Amazon. En cas d'indication d'un comportement de connexion anormal, GuardDuty génère un résultat contenant des informations détaillées sur la base de données potentiellement compromise. Lorsque vous activez la RDS protection pour la première fois ou que vous avez une instance de base de données nouvellement créée, une période d'apprentissage est nécessaire pour définir un comportement normal. Pour cette raison, il est possible que les instances de base de

données nouvellement activées ou créées n'aient aucun résultat de connexion anormale pendant jusqu'à deux semaines.

La fonctionnalité de RDS protection ne nécessite aucune configuration supplémentaire ; elle n'affecte aucune de vos bases de données Amazon Aurora ou RDS configurations Amazon existantes. GuardDuty ne gère pas vos bases de données prises en charge ni votre activité de RDS connexion, et ne met pas l'activité de RDS connexion à votre disposition.

Si vous choisissez d'activer automatiquement la fonctionnalité de RDS protection pour les nouveaux comptes membres lorsqu'ils rejoignent votre organisation, cette action active GuardDuty automatiquement ces nouveaux comptes membres. Pour plus d'informations sur la configuration de la surveillance de l'activité de RDS connexion en tant que fonctionnalité, consultezGuardDuty RDSProtection.

Configuration de RDS la protection pour un compte autonome

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez RDSProtection.
3. La page RDSProtection indique l'état actuel de votre compte. Vous pouvez activer ou désactiver la fonctionnalité à tout moment en sélectionnant Activer ou Désactiver. Confirmez votre sélection.

API/CLI

Exécutez l'updateDetectorAPIopération en utilisant votre propre identifiant de détecteur régional et en passant l'`features`objet au `name` `status` fur `RDS_LOGIN_EVENTS` `ENABLED` et à mesure`DISABLED`.

Vous pouvez également activer ou désactiver RDS la protection en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser votre propre code valide *`detector ID`*.

> **Note**
>
> L'exemple de code suivant active RDS la protection. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

Configuration de RDS la protection dans les environnements à comptes multiples

Dans un environnement à comptes multiples, seul le compte d' GuardDuty administrateur délégué a la possibilité d'activer ou de désactiver la fonctionnalité de RDS protection pour les comptes des membres de son organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration depuis leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes de ses membres à l'aide de AWS Organizations. Ce compte d' GuardDuty administrateur délégué peut choisir d'activer automatiquement le suivi des activités de RDS connexion pour tous les nouveaux comptes lorsqu'ils rejoignent l'organisation. Pour plus d'informations sur les environnements à comptes multiples, consultez Gérer plusieurs comptes sur Amazon. GuardDuty

Configuration de RDS la protection pour le compte GuardDuty d'administrateur délégué

Choisissez votre méthode d'accès préférée pour configurer la surveillance de l'activité de RDS connexion pour le compte GuardDuty d'administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte de gestion.
2. Dans le volet de navigation, choisissez RDSProtection.
3. Sur la page RDSProtection, choisissez Modifier.
4. Effectuez l’une des actions suivantes :

Utilisation d'Activer pour tous les comptes

- Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
- Choisissez Save (Enregistrer).

Utilisation de Configurer les comptes manuellement

- Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
- Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
- Choisissez Save (Enregistrer).

API/CLI

Exécutez l'updateDetectorAPIopération en utilisant votre propre identifiant de détecteur régional et en passant l'`features`objet au `name` `status` fur `RDS_LOGIN_EVENTS` `ENABLED` et à mesure`DISABLED`.

Vous pouvez activer ou désactiver RDS la protection en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser un compte GuardDuty d'administrateur délégué valide *`detector ID`*.

> **Note**
>
> L'exemple de code suivant active RDS la protection. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

Activer automatiquement RDS la protection pour tous les comptes des membres

Choisissez votre méthode d'accès préférée pour activer la fonction de RDS protection pour tous les comptes membres. Cela inclut les comptes membres existants et les nouveaux comptes qui rejoignent l'organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.
2. Effectuez l’une des actions suivantes :

   Utilisation de la page RDSProtection

   1. Dans le volet de navigation, choisissez RDSProtection.
   2. Choisissez Activer pour tous les comptes. Cette action active automatiquement RDS la protection des comptes existants et nouveaux de l'organisation.
   3. Choisissez Save (Enregistrer).

   > **Note**
   >
   > La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

   Utilisation de la page Comptes

   1. Dans le panneau de navigation, choisissez Accounts (Comptes).
   2. Sur la page Comptes, choisissez les préférences d'activation automatique avant Ajouter des comptes par invitation.
   3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes sous Surveillance de l'activité de RDS connexion.
   4. Choisissez Save (Enregistrer).

   Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes, veuillez consulter Activer ou désactiver de manière sélective RDS la protection pour les comptes des membres.

API/CLI

- Pour activer ou désactiver de manière sélective RDS la protection de vos comptes de membre, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer RDS la protection pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer RDS la protection pour tous les comptes de membres actifs existants

Choisissez votre méthode d'accès préférée pour activer RDS la protection de tous les comptes de membres actifs existants de votre organisation.

Console

Pour configurer RDS la protection pour tous les comptes de membres actifs existants

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le volet de navigation, choisissez RDSProtection.

3. Sur la page RDSProtection, vous pouvez consulter l'état actuel de la configuration. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Choisissez Confirmer.

API/CLI

- Pour activer ou désactiver de manière sélective RDS la protection de vos comptes de membre, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer RDS la protection pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer automatiquement RDS la protection pour les nouveaux comptes de membres

Choisissez votre méthode d'accès préférée pour activer les activités de RDS connexion pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte d' GuardDuty administrateur délégué peut activer de nouveaux comptes membres dans une organisation via la console, en utilisant la page RDSProtection ou la page Comptes.

Pour activer automatiquement RDS la protection pour les nouveaux comptes de membres

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l’une des actions suivantes :
   - À l'aide de RDSla page Protection :
     1. Dans le volet de navigation, choisissez RDSProtection.
     2. Sur la page RDSProtection, choisissez Modifier.
     3. Choisissez Configurer les comptes manuellement.
     4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, RDS la protection sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
     5. Choisissez Save (Enregistrer).
   - Utilisation de la page Comptes :
     1. Dans le panneau de navigation, choisissez Accounts (Comptes).
     2. Sur la page Comptes, choisissez les préférences d'activation automatique.
     3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous Surveillance des activités de RDS connexion.
     4. Choisissez Save (Enregistrer).

API/CLI

- Pour activer ou désactiver de manière sélective RDS la protection de vos comptes de membre, lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer RDS la protection pour un seul compte membre. Pour la désactiver, veuillez consulter Activer ou désactiver de manière sélective RDS la

protection pour les comptes des membres. Si vous ne souhaitez pas l'activer pour tous les nouveaux comptes qui rejoignent l'organisation, définissez `autoEnable` sur `NONE`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer ou désactiver de manière sélective RDS la protection pour les comptes des membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver de manière sélective la surveillance de l'activité de RDS connexion pour les comptes des membres.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

   Sur la page Comptes, consultez la colonne des activités de RDS connexion pour connaître l'état de votre compte de membre.

3. Pour activer ou désactiver de manière sélective l'activité RDS de connexion

   Sélectionnez le compte pour lequel vous souhaitez configurer RDS la protection. Vous pouvez sélectionner plusieurs comptes à la fois. Dans le menu déroulant Modifier les plans de protection, sélectionnez Activité de RDS connexion, puis choisissez l'option appropriée.

API/CLI

Pour activer ou désactiver de manière sélective RDS la protection de vos comptes de membre, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.

L'exemple suivant montre comment activer RDS la protection pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

> **Note**
>
> Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

GuardDuty Protection Lambda

La protection Lambda vous aide à identifier les menaces de sécurité potentielles lorsqu'une fonction AWS Lambda est invoquée dans votre environnement AWS . Lorsque vous activez la protection Lambda, GuardDuty commence à surveiller les journaux d'activité du réseau Lambda, en commençant par Journaux de flux VPC toutes les fonctions Lambda du compte, y compris les journaux qui n'utilisent pas le VPC réseau, et sont générés lorsque la fonction Lambda est invoquée. S'il GuardDuty identifie un trafic réseau suspect indiquant la présence d'un code potentiellement malveillant dans votre fonction Lambda, il GuardDuty générera un résultat.

> **Note**
>
> La surveillance de l'activité du réseau Lambda n'inclut pas les journaux des fonctions Lambda@Edge.

Vous pouvez configurer la protection Lambda pour n'importe quel compte ou être disponible Régions AWSà tout moment. Par défaut, un GuardDuty compte existant peut activer Lambda Protection avec une période d'essai de 30 jours. Pour un nouveau GuardDuty compte, la protection Lambda est déjà activée et incluse dans la période d'essai de 30 jours. Pour de plus amples informations sur l'utilisation des statistiques, veuillez consulter Estimation du coût.

GuardDuty surveille les journaux d'activité réseau générés en invoquant les fonctions Lambda. À l'heure actuelle, la surveillance de l'activité réseau Lambda inclut les journaux de VPC flux Amazon relatifs à toutes les fonctions Lambda de votre compte, y compris les journaux qui n'utilisent pas le VPC réseau, et sont susceptibles d'être modifiés, notamment en cas d'extension à d'autres activités réseau, telles que les données de DNS requête générées par l'appel des fonctions Lambda. L'extension à d'autres formes de surveillance de l'activité réseau augmentera le volume de données à traiter pour la protection Lambda. GuardDuty Cela aura un impact direct sur le coût d'utilisation de la protection Lambda. Chaque fois que vous GuardDuty commencez à surveiller un journal d'activité réseau supplémentaire, il fournit une notification aux comptes qui ont activé la protection Lambda, au moins 30 jours avant la publication.

Fonctionnalité de la protection Lambda

Surveillance de l'activité du réseau Lambda

Lorsque vous activez la protection Lambda, surveille les journaux d'activité du réseau GuardDuty Lambda générés lorsqu'une fonction Lambda associée à votre compte est invoquée. Cela vous permet de détecter les menaces de sécurité potentielles qui pèsent sur la fonction Lambda. GuardDuty surveille les journaux de VPC flux de toutes vos fonctions Lambda, y compris celles qui n'utilisent VPC pas le réseau. Pour les fonctions Lambda configurées pour utiliser le VPC réseau, il n'est pas nécessaire d'activer les journaux de VPC flux pour les interfaces réseau élastiques (ENI) créées par Lambda pour. GuardDuty GuardDuty ne facture que le montant des données des journaux d'activité du réseau Lambda traitées (en Go) pour générer un résultat. GuardDuty optimise les coûts en appliquant des filtres intelligents et en analysant un sous-ensemble de journaux d'activité du réseau Lambda pertinents pour la détection des menaces. Pour plus d'informations sur les tarifs, consultez GuardDuty les tarifs Amazon.

GuardDuty ne gère pas les journaux d'activité de votre réseau Lambda (y compris VPC les journaux non liés aux VPC flux) et ne les rend pas accessibles dans votre compte.

Configuration de la protection Lambda

Configuration de la protection Lambda pour un compte autonome

Pour les comptes associés à AWS Organizations, vous pouvez automatiser ce processus via une GuardDuty console ou API des instructions, comme décrit dans la section suivante.

Choisissez votre méthode d'accès préférée pour activer ou désactiver la protection Lambda pour un compte autonome.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, sous Paramètres, choisissez Protection Lambda.
3. La page Protection Lambda indique l'état actuel de votre compte. Vous pouvez activer ou désactiver la fonctionnalité à tout moment en sélectionnant Activer ou Désactiver.
4. Choisissez Save (Enregistrer).

API/CLI

Exécutez l'updateDetectorAPIopération en utilisant votre propre identifiant de détecteur régional et en passant l'`features`objet au `name` `status` fur `LAMBDA_NETWORK_LOGS` `ENABLED` et à mesure`DISABLED`.

Vous pouvez également activer ou désactiver la surveillance de l'activité réseau Lambda en exécutant la commande suivante AWS CLI . Assurez-vous d'utiliser votre propre code valide *`detector ID`*.

> **Note**
>
> L'exemple de code suivant active la surveillance de l'activité du réseau Lambda. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

Configuration de la protection Lambda dans des environnements à comptes multiples

Dans un environnement multi-comptes, seul le compte d' GuardDuty administrateur délégué a la possibilité d'activer ou de désactiver la protection Lambda pour les comptes des membres de son organisation. Les comptes GuardDuty membres ne peuvent pas modifier cette configuration depuis leurs comptes. Le compte d' GuardDuty administrateur délégué gère les comptes des membres à l'aide de AWS Organizations. Le compte GuardDuty administrateur délégué peut choisir d'activer automatiquement la surveillance de l'activité réseau Lambda pour tous les nouveaux comptes lorsqu'ils rejoignent l'organisation. Pour plus d'informations sur les environnements multi-comptes, consultez Gérer plusieurs comptes sur Amazon GuardDuty.

Configuration de la protection Lambda pour un compte d'administrateur délégué GuardDuty

Choisissez votre méthode d'accès préférée pour activer ou désactiver la surveillance de l'activité réseau Lambda pour le compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte de gestion.
2. Dans le volet de navigation, sous Paramètres, choisissez Protection Lambda.
3. Sur la page Protection Lambda, choisissez Modifier.
4. Effectuez l’une des actions suivantes :

   Utilisation d'Activer pour tous les comptes

   - Choisissez Activer pour tous les comptes. Cela activera le plan de protection pour tous les GuardDuty comptes actifs de votre AWS organisation, y compris les nouveaux comptes qui rejoignent l'organisation.
   - Choisissez Save (Enregistrer).

   Utilisation de Configurer les comptes manuellement

   - Pour activer le plan de protection uniquement pour le compte GuardDuty administrateur délégué, choisissez Configurer les comptes manuellement.
   - Choisissez Activer dans la section compte GuardDuty administrateur délégué (ce compte).
   - Choisissez Save (Enregistrer).

API/CLI

Exécutez l'updateDetectorAPIopération en utilisant votre propre identifiant de détecteur régional et en passant l'`features`objet au `name` `status` fur `LAMBDA_NETWORK_LOGS` `ENABLED` et à mesure`DISABLED`.

Vous pouvez activer ou désactiver la surveillance de l'activité réseau Lambda en exécutant la commande suivante AWS CLI . Assurez-vous d'utiliser un compte GuardDuty d'administrateur délégué valide *`detector ID`*.

> **Note**
>
> L'exemple de code suivant active la surveillance de l'activité du réseau Lambda. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-detector --detector-
id 12abc34d567e8fa901bc2d34e56789f0 555555555555 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Activer automatiquement la surveillance de l'activité du réseau Lambda pour tous les comptes membres

Choisissez votre méthode d'accès préférée pour activer la fonctionnalité Surveillance de l'activité du réseau Lambda pour tous les comptes membres. Cela inclut les comptes membres existants et les nouveaux comptes qui rejoignent l'organisation.

Console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l’une des actions suivantes :

   Utilisation de la page Protection Lambda

   1. Dans le panneau de navigation, choisissez Protection Lambda.
   2. Choisissez Activer pour tous les comptes. Cette action active automatiquement la surveillance de l'activité du réseau Lambda pour les comptes existants et nouveaux de l'organisation.
   3. Choisissez Save (Enregistrer).

> **Note**
>
> La mise à jour de la configuration des comptes membres peut prendre jusqu'à 24 heures.

Utilisation de la page Comptes

1. Dans le panneau de navigation, choisissez Accounts (Comptes).
2. Sur la page Comptes, choisissez les préférences d'activation automatique avant Ajouter des comptes par invitation.
3. Dans la fenêtre Gérer les préférences d'activation automatique, choisissez Activer pour tous les comptes sous Surveillance de l'activité du réseau Lambda.

   > **Note**
   >
   > Par défaut, cette action active automatiquement l'option Activation automatique GuardDuty pour les nouveaux comptes membres.

4. Choisissez Save (Enregistrer).

Si vous ne pouvez pas utiliser l'option Activer pour tous les comptes, veuillez consulter Activer ou désactiver de manière sélective la surveillance de l'activité du réseau Lambda pour les comptes membres.

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance de l'activité réseau Lambda pour vos comptes membres, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer la surveillance de l'activité du réseau Lambda pour un seul compte membre. Pour désactiver un compte membre, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer la surveillance de l'activité du réseau Lambda pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée pour activer la surveillance de l'activité du réseau Lambda pour tous les comptes membres actifs existants de l'organisation.

Console

Pour configurer la surveillance de l'activité du réseau Lambda pour tous les comptes membres actifs existants

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.

   Connectez-vous à l'aide des informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le panneau de navigation, choisissez Protection Lambda.
3. Sur la page Protection Lambda, vous pouvez afficher l'état actuel de la configuration. Dans la section Comptes membres actifs, choisissez Actions.
4. Dans le menu déroulant Actions, choisissez Activer pour tous les comptes membres actifs existants.
5. Choisissez Confirmer.

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance de l'activité réseau Lambda pour vos comptes membres, lancez l'updateMemberDetectorsAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer la surveillance de l'activité du réseau Lambda pour un seul compte membre. Pour désactiver un compte membre, remplacez `ENABLED` par `DISABLED`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.
- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer automatiquement la surveillance de l'activité du réseau Lambda pour les nouveaux comptes membres

Choisissez votre méthode d'accès préférée pour activer la surveillance de l'activité du réseau Lambda pour les nouveaux comptes qui rejoignent votre organisation.

Console

Le compte d' GuardDuty administrateur délégué peut activer la surveillance de l'activité réseau Lambda pour les nouveaux comptes membres d'une organisation, à l'aide de la page Lambda Protection ou des comptes.

Pour activer automatiquement la surveillance de l'activité du réseau Lambda pour les nouveaux comptes membres

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.

2. Effectuez l’une des actions suivantes :
   - Utilisation de la page Protection Lambda :
     1. Dans le panneau de navigation, choisissez Protection Lambda.
     2. Sur la page Protection Lambda, choisissez Modifier.
     3. Choisissez Configurer les comptes manuellement.
     4. Sélectionnez Activer automatiquement pour les nouveaux comptes membres. Cette étape garantit que chaque fois qu'un nouveau compte rejoint votre organisation, la protection Lambda sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
     5. Choisissez Save (Enregistrer).
   - Utilisation de la page Comptes :
     1. Dans le panneau de navigation, choisissez Accounts (Comptes).
     2. Sur la page Comptes, choisissez les préférences d'activation automatique.
     3. Dans la fenêtre Gérer les préférences d'activation automatique, sélectionnez Activer pour les nouveaux comptes sous Surveillance de l'activité du réseau Lambda.
     4. Choisissez Save (Enregistrer).

API/CLI

- Pour activer ou désactiver la surveillance de l'activité réseau Lambda pour les nouveaux comptes membres, lancez l'UpdateOrganizationConfigurationAPIopération en utilisant votre propre *`detector ID`*.
- L'exemple suivant montre comment activer la surveillance de l'activité du réseau Lambda pour un seul compte membre. Pour la désactiver, veuillez consulter Activer ou désactiver de manière sélective la surveillance de l'activité du réseau Lambda pour les comptes membres. Si vous ne souhaitez pas l'activer pour tous les nouveaux comptes qui rejoignent l'organisation, définissez `AutoEnable` sur `NONE`.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

- Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Activer ou désactiver de manière sélective la surveillance de l'activité du réseau Lambda pour les comptes membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver de manière sélective la surveillance de l'activité du réseau Lambda pour les comptes membres.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser les informations d'identification du compte GuardDuty administrateur délégué.
2. Dans le volet de navigation, sous Settings, choisissez Accounts.

   Sur la page Comptes, examinez la colonne Surveillance de l'activité du réseau Lambda. Elle indique si la surveillance de l'activité du réseau Lambda est activée ou non.
3. Sélectionnez le compte pour lequel vous souhaitez configurer la protection Lambda. Vous pouvez choisir plusieurs comptes à la fois.
4. Dans le menu déroulant Modifier les plans de protection, choisissez Surveillance de l'activité du réseau Lambda, puis choisissez une action appropriée.

API/CLI

Invoquez le updateMemberDetectorsAPIen utilisant le vôtre *`detector ID`*.

L'exemple suivant montre comment activer la surveillance de l'activité du réseau Lambda pour un seul compte membre. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Vous pouvez également transmettre une liste de comptes IDs séparés par un espace.

Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts`. En cas de problème lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.

Protéger les charges de travail liées à l'IA avec GuardDuty

La détection GuardDuty des menaces de base d'Amazon et la protection Lambda vous aident à mieux sécuriser et à détecter les menaces qui pèsent sur les charges de travail basées sur l'IA. AWS

La détection des GuardDuty menaces de base surveille les événements de AWS CloudTrail gestion afin de détecter les activités suspectes et malveillantes dans les charges de travail d'IA génératives créées à l'aide de AWS services tels qu'Amazon Bedrock et Amazon. SageMaker Par exemple, GuardDuty peut identifier des activités telles que :

- Suppression inhabituelle des rambardes de sécurité Amazon Bedrock
- Modification de la source de données d'entraînement du modèle susceptible de provoquer une attaque d'empoisonnement des données
- Invocation suspecte du modèle Amazon Bedrock
- Instance inhabituelle de bloc-notes ou création d'emplois de formation dans SageMaker
- Informations d'identification Amazon Elastic Compute Cloud exfiltrées qui peuvent avoir été utilisées pour appeler APIs Amazon Bedrock, Amazon SageMaker ou des charges de travail d'IA autogérées sur des EC2 instances, EKS des clusters ou des tâches. ECS

GuardDuty Lambda Protection peut aider à détecter les menaces potentielles liées aux agents Amazon Bedrock. Cela peut inclure des activités réseau suspectes, telles que le minage de cryptomonnaies, et la communication avec des serveurs de commande et de contrôle malveillants, qui peuvent être causées par une attaque de la chaîne d'approvisionnement ou par des demandes complexes.

La vidéo suivante montre à quoi ressembleraient les résultats associés.

La vidéo suivante montre à quoi ressembleraient les résultats associés. Utiliser Amazon GuardDuty pour surveiller et sécuriser vos charges de travail basées sur l'IA AWS

Gestion de plusieurs comptes sur Amazon GuardDuty

Lorsque votre AWS environnement comporte plusieurs comptes, vous pouvez les gérer en désignant un Compte AWS comme compte administrateur. Vous pouvez ensuite associer le multiple Comptes AWS à ce compte administrateur en tant que comptes de membre. Grâce à cette configuration, un compte GuardDuty administrateur désigné peut évaluer et surveiller la sécurité globale de votre organisation. Le compte administrateur peut également effectuer des tâches de gestion du compte, telles que l'examen de tous les résultats générés et la configuration des plans de protection qu'il contient GuardDuty.

Dans GuardDuty, une organisation se compose d'un compte d' GuardDuty administrateur délégué et d'un ou de plusieurs comptes de membres associés. Vous pouvez associer les comptes de deux manières : en les intégrant à AWS Organizations la console ou en utilisant une ancienne méthode d'envoi et d'acceptation des invitations d'adhésion dans la GuardDuty console. GuardDuty vous recommande de l'intégrer à AWS Organizations.

AWS Organizations est un service mondial de gestion de comptes qui permet aux AWS administrateurs de consolider et de gérer de manière centralisée plusieurs comptes Comptes AWS. Il fournit des fonctionnalités de gestion des comptes et de facturation consolidée conçues pour répondre aux besoins budgétaires, de sécurité et de conformité. Il est proposé sans frais supplémentaires et s'intègre à plusieurs AWS services applications, notamment Macie et Amazon GuardDuty. AWS Security Hub Pour plus d’informations, consultez le AWS Organizations Guide de l’utilisateur .

Table des matières

Comprendre la relation entre le compte GuardDuty administrateur et les comptes membres

Lorsque vous l'utilisez GuardDuty dans un environnement à comptes multiples, le compte administrateur peut gérer certains aspects des comptes membres pour GuardDuty le compte des membres. Un compte administrateur peut exécuter les principales fonctions suivantes :

- Ajouter et supprimer des comptes membres associés. Le processus par lequel un compte administrateur peut effectuer cette opération varie en fonction de la façon dont vous gérez les comptes, par le biais d'organisations ou sur invitation.
- Activation GuardDuty du compte administrateur délégué GuardDuty dans le compte de gestion

  Si le compte AWS Organizations de gestion est désactivé GuardDuty, le compte d' GuardDuty administrateur délégué peut l'activer GuardDuty dans le compte de gestion. Cependant, il est nécessaire que le compte de gestion n'ait pas explicitement supprimé leAutorisations de rôle liées à un service pour GuardDuty.
- Gérez le statut des comptes GuardDuty membres associés, notamment en les activant et en les suspendant GuardDuty.

  > **Note**
  >
  > Comptes d'administrateur délégué gérés avec activation AWS Organizations automatique GuardDuty dans les comptes ajoutés en tant que membres.
- Personnalisez les résultats au sein du GuardDuty réseau en créant et en gérant des règles de suppression, des listes d'adresses IP fiables et des listes de menaces. Dans un environnement à comptes multiples, la configuration de ces fonctionnalités n'est disponible que pour un compte d' GuardDuty administrateur délégué. Un compte membre ne peut pas mettre à jour cette configuration.

Le tableau suivant détaille la relation entre le compte GuardDuty d'administrateur et les comptes de membre.

Dans ce tableau :

- Auto-utilisateur : un compte ne peut effectuer l'action répertoriée que pour son propre compte.
- N'importe lequel : un compte peut exécuter l'action répertoriée pour n'importe quel compte associé.
- Tout — Un compte peut effectuer l'action répertoriée et elle s'applique à tous les comptes associés. Généralement, le compte effectuant cette action est un compte GuardDuty administrateur désigné

Les cellules du tableau marquées d'un tiret (—) indiquent que le compte ne peut pas effectuer l'action répertoriée.

Action	À travers AWS Organizations		Sur invitation	
	Compte GuardDuty d'administrateur délégué	Compte de membre associé	Compte GuardDuty d'administrateur délégué	Compte de membre associé
Activer GuardDuty	N'importe quel compte	–	Auto-utilisateur	Auto-utilisateur
GuardDuty Activation automatique pour l'ensemble de l'organisation (`ALL`,`NEW`,`NONE`)	Tous	–	–	–
Afficher les comptes de tous les membres des Organisations, quel que soit leur GuardDuty statut	N'importe quel compte	–	–	–
Générer des exemples de résultats	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Afficher tous les GuardDuty résultats	N'importe quel compte	Auto-utilisateur	N'importe quel compte	Auto-utilisateur
GuardDuty Conclusions des archives	N'importe quel compte	–	N'importe quel compte	–

Appliquer des règles de suppression	Tous	–	Tous	–
Créez une liste d'adresses IP fiables ou des listes de menaces	Tous	–	Tous	–
Mettre à jour la liste d'adresses IP fiables ou les listes de menaces	Tous	–	Tous	–
Supprimer la liste d'adresses IP fiables ou les listes de menaces	Tous	–	Tous	–
Définissez la fréquence des EventBridge notifications	Tous	–	Tous	Auto-utilisateur
Définir l'emplacement Amazon S3 pour l'exportation des résultats	Tous	–	Tous	Auto-utilisateur

Activez un ou plusieurs plans de protection facultatifs pour l'ensemble de l'entreprise (`ALL`,`NEW`,`NONE`) Cela n'inclut pas la protection contre les programmes malveillants pour S3.	Tous	–	–	–
Activez n'importe quel plan de GuardDuty protection pour les comptes individuels Cela n'inclut pas la protection contre les programmes malveillants ni EC2 la protection contre les programmes malveillants pour S3.	N’importe quel compte	–	N’importe quel compte	–
Protection contre les logiciels malveillants pour EC2	N’importe quel compte	–	Auto-utilisateur	Auto-utilisateur

Protection contre les logiciels malveillants pour S3	–	Auto-utilisateur	–	Auto-utilisateur
Dissocier un compte membre	N'importe quel compte	–	N'importe quel compte	–
Dissocier d'un compte administrateur	–	Soi [+]	–	Auto-utilisateur
Supprimer un compte de membre dissocié	N'importe quel compte	–	N'importe quel compte	–
Suspendre GuardDuty	N'importe lequel [*]	–	N'importe lequel [*]	–
Désactiver GuardDuty	N'importe lequel [*]	–	N'importe lequel [*]	–

[+] Indique que le compte ne peut effectuer cette action que si le compte GuardDuty administrateur délégué n'a pas configuré la préférence d'activation automatique pour `ALL` les membres de l'organisation.

[*] Indique qu'un compte d' GuardDuty administrateur délégué ne peut pas être désactivé directement GuardDuty dans un compte de membre. Le compte GuardDuty d'administrateur délégué doit d'abord dissocier le compte du membre, puis le supprimer. Ensuite, chaque compte membre peut être désactivé GuardDuty dans son propre compte. Pour plus d'informations sur l'exécution de ces tâches dans votre organisation, consultezMaintien de votre organisation au sein GuardDuty.

Gérer des GuardDuty comptes avec AWS Organizations

Dans une AWS organisation, le compte de gestion peut désigner n'importe quel compte au sein de cette organisation comme compte d' GuardDuty administrateur délégué. Pour ce compte administrateur, GuardDuty il est activé automatiquement uniquement dans le cas actuel Région AWS. Par défaut, le compte administrateur peut activer et gérer tous GuardDuty les comptes membres

de l'organisation au sein de cette région. Le compte administrateur peut consulter et ajouter des membres à cette AWS organisation.

Les sections suivantes vous expliqueront les différentes tâches que vous pouvez effectuer en tant que compte d' GuardDuty administrateur délégué.

Considérations et recommandations d'utilisation GuardDuty avec AWS Organizations

Les considérations et recommandations suivantes peuvent vous aider à comprendre le fonctionnement d'un compte d' GuardDuty administrateur délégué dans GuardDuty :

Un compte d' GuardDuty administrateur délégué peut gérer un maximum de 50 000 membres.

Il y a une limite de 50 000 comptes membres par compte GuardDuty d'administrateur délégué. Cela inclut les comptes de membres ajoutés par le biais du compte GuardDuty administrateur AWS Organizations ou ceux qui ont accepté l'invitation du compte administrateur à rejoindre leur organisation. Toutefois, votre AWS organisation peut compter plus de 50 000 comptes.

Si vous dépassez la limite de 50 000 comptes membres, vous recevrez une notification et un e-mail du compte d' GuardDuty administrateur délégué désigné. CloudWatch AWS Health Dashboard

Un compte GuardDuty d'administrateur délégué est régional.

Contrairement à AWS Organizations, GuardDuty il s'agit d'un service régional. Les comptes d' GuardDuty administrateur délégué et leurs comptes de membre doivent être ajoutés AWS Organizations dans chaque région souhaitée dans laquelle vous avez GuardDuty activé votre compte. Si le compte de gestion de l'organisation désigne un compte d' GuardDuty administrateur délégué uniquement dans l'est des États-Unis (Virginie du Nord), le compte d' GuardDuty administrateur délégué gérera uniquement les comptes des membres ajoutés à l'organisation dans cette région. Pour plus d'informations sur la parité des fonctionnalités dans les régions où GuardDuty elle est disponible, consultezRégions et points de terminaison.

Cas particuliers pour les régions optionnelles

- Lorsqu'un compte d' GuardDuty administrateur délégué se retire d'une région optionnelle, même si la configuration d' GuardDuty activation automatique de votre organisation est définie sur les nouveaux comptes membres uniquement (`NEW`) ou sur tous les comptes membres (`ALL`), il GuardDuty ne peut être activé pour aucun compte de membre de l'organisation actuellement désactivé. GuardDuty Pour plus d'informations sur la configuration de vos

comptes membres, ouvrez Comptes dans le volet de navigation de la GuardDuty console ou utilisez le ListMembersAPI.

- Lorsque vous travaillez avec la configuration GuardDuty d'activation automatique définie surNEW, assurez-vous que la séquence suivante est respectée :

  1. Les comptes membres optent pour une région optionnelle.
  2. Ajoutez les comptes des membres à votre organisation dans AWS Organizations.

  Si vous modifiez l'ordre de ces étapes, le paramètre d' GuardDuty activation automatique ne **NEW** fonctionnera pas dans la région d'inscription spécifique, car le compte du membre n'est plus nouveau pour l'organisation. GuardDuty propose deux solutions alternatives :

  - Définissez la configuration GuardDuty d'activation automatique surALL, qui inclut les comptes de membres nouveaux et existants. Dans ce cas, l'ordre de ces étapes n'est pas pertinent.
  - Si un compte membre fait déjà partie de votre organisation, gérez la GuardDuty configuration de ce compte individuellement dans la région d'adhésion spécifique à l'aide de la GuardDuty console ou duAPI.

Nécessaire pour qu'une AWS organisation dispose du même compte GuardDuty d'administrateur délégué pour tous les Régions AWS.

Vous devez désigner un compte membre comme compte d' GuardDuty administrateur délégué pour tous les comptes Régions AWS GuardDuty Where activé. Par exemple, si vous désignez un compte de membre *111122223333* dans *Europe (Ireland)*, vous ne pouvez pas désigner un autre compte membre *555555555555* dans *Canada (Central)*. Vous devez utiliser le même compte que le compte d' GuardDuty administrateur délégué dans toutes les autres régions.

Vous pouvez désigner un nouveau compte GuardDuty d'administrateur délégué à tout moment. Pour plus d'informations sur la suppression du compte GuardDuty administrateur délégué existant, consultezModification du compte GuardDuty d'administrateur délégué.

Il n'est pas recommandé de définir le compte de gestion de votre organisation comme compte GuardDuty d'administrateur délégué.

Le compte de gestion de votre organisation peut être le compte GuardDuty d'administrateur délégué. Cependant, les bonnes pratiques de sécurité AWS suivent le principe du moindre privilège et ne recommandent pas cette configuration.

La modification d'un compte d' GuardDuty administrateur délégué n'est pas désactivée GuardDuty pour les comptes des membres.

> Si vous supprimez un compte d' GuardDuty administrateur délégué, GuardDuty tous les comptes de membre associés à ce compte d' GuardDuty administrateur délégué sont supprimés. GuardDuty reste activé pour tous ces comptes de membres.

Autorisations requises pour désigner un compte d' GuardDuty administrateur délégué

Pour commencer à utiliser Amazon GuardDuty avec AWS Organizations, le compte AWS Organizations de gestion de l'organisation désigne un compte en tant que compte d' GuardDuty administrateur délégué. Cela permet GuardDuty en tant que service fiable de AWS Organizations. Il active également le compte GuardDuty d' GuardDuty administrateur délégué et permet également au compte d'administrateur délégué d'activer et de gérer GuardDuty d'autres comptes de l'organisation dans la région actuelle. Pour plus d'informations sur la manière dont ces autorisations sont accordées, voir Utilisation AWS Organizations avec d'autres AWS services.

En tant que compte de AWS Organizations gestion, avant de désigner le compte d' GuardDuty administrateur délégué pour votre organisation, vérifiez que vous pouvez effectuer l' GuardDuty action suivante : `guardduty:EnableOrganizationAdminAccount` Cette action vous permet de désigner le compte d' GuardDuty administrateur délégué pour votre organisation en utilisant GuardDuty. Vous devez également vous assurer que vous êtes autorisé à effectuer les AWS Organizations actions qui vous aident à récupérer des informations sur votre organisation.

Pour accorder ces autorisations, incluez la déclaration suivante dans une politique AWS Identity and Access Management (IAM) pour votre compte :

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Si vous souhaitez désigner votre compte AWS Organizations de gestion comme compte d' GuardDuty administrateur délégué, votre compte aura également besoin de l'IAMaction :`CreateServiceLinkedRole`. Cette action vous permet d'initialiser le compte GuardDuty de gestion. Cependant, vérifiez Considérations et recommandations d'utilisation GuardDuty avec AWS Organizations avant de procéder à l'ajout des autorisations.

Pour continuer à désigner le compte de gestion comme compte d' GuardDuty administrateur délégué, ajoutez l'énoncé suivant à la IAM politique et remplacez *111122223333* avec l' Compte AWS identifiant du compte de gestion de votre organisation :

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Désignation d'un compte d'administrateur délégué GuardDuty

Choisissez une méthode d'accès préférée pour désigner un compte d' GuardDuty administrateur délégué pour votre organisation. Seul un compte de gestion peut effectuer cette étape.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

Pour vous connecter, utilisez les informations d'identification du compte de gestion de votre AWS Organizations organisation.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désigner le compte d' GuardDuty administrateur délégué pour votre organisation.
3. Procédez de l'une des manières suivantes, selon que votre compte de gestion GuardDuty est activé ou non dans la région actuelle :

   - Si cette option GuardDuty est activée, sélectionnez Amazon GuardDuty - toutes les fonctionnalités, puis choisissez Get started. Cette action vous redirigera vers la GuardDuty page de bienvenue.
   - Si cette option GuardDuty est activée, choisissez Paramètres dans le volet de navigation.
4. Sous Administrateur délégué, entrez l' Compte AWS ID à 12 chiffres du compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué pour l'organisation.

   Assurez-vous d'activer le compte GuardDuty d' GuardDuty administrateur délégué que vous venez de désigner, sinon il ne pourra effectuer aucune action.
5. Choisisssez Delegate (Déléguer).
6. (Recommandé) Répétez les étapes précédentes pour désigner le compte d' GuardDuty administrateur délégué dans chaque Région AWS endroit où vous avez GuardDuty activé le compte.

API/CLI

1. enableOrganizationAdminAccountExécuté en utilisant les informations d'identification Compte AWS du compte de gestion de l'organisation.
   - Vous pouvez également utiliser AWS Command Line Interface pour cela. La AWS CLI commande suivante désigne un compte d' GuardDuty administrateur délégué pour votre région actuelle uniquement. Exécutez la AWS CLI commande suivante et assurez-vous de remplacer *111111111111* avec l' Compte AWS ID du compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué :

     ```
     aws guardduty enable-organization-admin-account --admin-account-
     id 111111111111
     ```

Pour désigner le compte d' GuardDuty administrateur délégué pour les autres régions, spécifiez la région dans la AWS CLI commande. L'exemple suivant montre comment activer un compte d' GuardDuty administrateur délégué dans l'ouest des États-Unis (Oregon). Assurez-vous de remplacer *us-west-2* avec la région à laquelle vous souhaitez attribuer le compte d' GuardDuty administrateur délégué.

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111 --region us-west-2
```

Pour plus d'informations sur l' Régions AWS endroit où GuardDuty est disponible, consultezRégions et points de terminaison.

S' GuardDuty il n'est pas activé pour votre compte d' GuardDuty administrateur délégué, il ne pourra effectuer aucune action. Si ce n'est pas déjà fait, assurez-vous GuardDuty d'activer le compte d' GuardDuty administrateur délégué nouvellement désigné.

2. (Recommandé) Répétez les étapes précédentes pour désigner le compte d' GuardDuty administrateur délégué dans chaque Région AWS cas où vous l'avez GuardDuty activé.

Mettre à jour les préférences d'activation automatique de l'organisation

La fonctionnalité d'activation automatique de l'organisation vous GuardDuty permet de définir le même statut GuardDuty et le statut des plans de protection pour `ALL` les comptes existants ou `NEW` membres de votre organisation, en une seule étape. De même, vous pouvez également spécifier à quel moment vous ne souhaitez effectuer aucune action sur les comptes des membres, en choisissant`NEW`. Les étapes suivantes expliquent ces paramètres et indiquent également quand vous souhaitez utiliser un paramètre spécifique.

Choisissez une méthode d'accès préférée pour mettre à jour les préférences d'activation automatique pour l'organisation.

Console

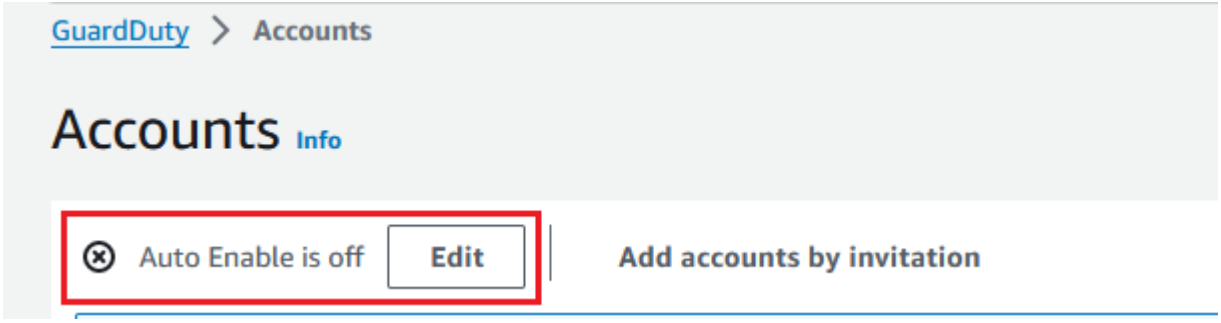
1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Pour vous connecter, utilisez les informations d'identification du compte GuardDuty administrateur.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

La page Comptes fournit des options de configuration pour le compte GuardDuty administrateur à activer automatiquement GuardDuty et les plans de protection facultatifs pour le compte des comptes membres appartenant à l'organisation.

3. Pour mettre à jour les paramètres d'activation automatique existants, choisissez Modifier.



Ce support est disponible pour configurer GuardDuty et tous les plans de protection optionnels pris en charge dans votre Région AWS. Vous pouvez sélectionner l'une des options de configuration suivantes pour GuardDuty le compte de vos comptes membres :

- Activer pour tous les comptes (**`ALL`**) : sélectionnez cette option pour activer l'option correspondante pour tous les comptes d'une organisation. Cela inclut les nouveaux comptes qui rejoignent l'organisation et ceux qui peuvent avoir été suspendus ou supprimés de l'organisation. Cela inclut également le compte GuardDuty d'administrateur délégué.

  > **Note**
  >
  > La mise à jour de la configuration de tous les comptes membres peut prendre jusqu'à 24 heures.

- Activation automatique pour les nouveaux comptes (**`NEW`**) : sélectionnez cette option pour activer automatiquement les plans de protection GuardDuty ou les plans de protection facultatifs pour les nouveaux comptes uniquement lorsqu'ils rejoignent votre organisation.
- Ne pas activer (**`NONE`**) : sélectionnez cette option pour empêcher l'activation de l'option correspondante pour les nouveaux comptes de votre organisation. Dans ce cas, le compte GuardDuty administrateur gérera chaque compte individuellement.

  Lorsque vous mettez à jour le paramètre d'activation automatique depuis `ALL` ou `NEW` vers`NONE`, cette action ne désactive pas l'option correspondante pour vos comptes existants. Cette configuration s'appliquera aux nouveaux comptes qui rejoignent

l'organisation. Après avoir mis à jour les paramètres d'activation automatique, l'option correspondante ne sera activée pour aucun nouveau compte.

> **Note**
>
> Lorsqu'un compte d' GuardDuty administrateur délégué se retire d'une région optionnelle, même si la configuration d' GuardDuty activation automatique de votre organisation est définie sur les nouveaux comptes membres uniquement (`NEW`) ou sur tous les comptes membres (`ALL`), il GuardDuty ne peut être activé pour aucun compte de membre de l'organisation actuellement désactivé. GuardDuty Pour plus d'informations sur la configuration de vos comptes membres, ouvrez Comptes dans le volet de navigation de la GuardDuty console ou utilisez le ListMembersAPI.

4. Sélectionnez Enregistrer les modifications.
5. (Facultatif) Si vous souhaitez utiliser les mêmes préférences dans chaque région, mettez à jour vos préférences séparément dans chacune des régions prises en charge.

   Certains des plans de protection optionnels peuvent ne pas être disponibles partout Régions AWS où ils GuardDuty sont disponibles. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.

API/CLI

1. Exécutez-le en UpdateOrganizationConfigurationutilisant les informations d'identification du compte d' GuardDuty administrateur délégué, afin de configurer GuardDuty automatiquement des plans de protection facultatifs dans cette région pour votre organisation. Pour plus d'informations sur les différentes configurations d'activation automatique, consultez la section autoEnableOrganizationMembres.

   Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

   Pour définir les préférences d'activation automatique pour l'un des plans de protection facultatifs pris en charge dans votre région, suivez les étapes indiquées dans les sections de documentation correspondantes de chaque plan de protection.

2. Vous pouvez valider les préférences de votre organisation dans la région actuelle. Exécutez describeOrganizationConfiguration. Assurez-vous de spécifier l'ID du détecteur du compte GuardDuty administrateur délégué.

   > **Note**
   >
   > La mise à jour de la configuration de tous les comptes membres peut prendre jusqu'à 24 heures.

1. Vous pouvez également exécuter la AWS CLI commande suivante pour définir les préférences afin d'activer ou de désactiver automatiquement GuardDuty dans cette région les nouveaux comptes (`NEW`) qui rejoignent l'organisation, tous les comptes (`ALL`) ou aucun des comptes (`NONE`) de l'organisation. Pour plus d'informations, consultez la section autoEnableOrganizationMembres. Selon vos préférences, vous devrez peut-être remplacer `NEW` par `ALL` ou `NONE`. Si vous configurez le plan de protection avec`ALL`, le plan de protection sera également activé pour le compte d' GuardDuty administrateur délégué. Assurez-vous de spécifier l'ID du détecteur du compte d' GuardDuty administrateur délégué qui gère la configuration de l'organisation.

   Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

   ```
   aws guardduty update-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
   ```

2. Vous pouvez valider les préférences de votre organisation dans la région actuelle. Exécutez la AWS CLI commande suivante en utilisant l'ID du détecteur du compte GuardDuty administrateur délégué.

   ```
   aws guardduty describe-organization-configuration --detector-
   id 12abc34d567e8fa901bc2d34e56789f0
   ```

(Recommandé) Répétez les étapes précédentes dans chaque région en utilisant l'identifiant du détecteur de compte GuardDuty administrateur délégué.

> **Note**
>
> Lorsqu'un compte d' GuardDuty administrateur délégué se retire d'une région optionnelle, même si la configuration d' GuardDuty activation automatique de votre organisation est définie sur les nouveaux comptes membres uniquement (`NEW`) ou sur tous les comptes membres (`ALL`), il GuardDuty ne peut être activé pour aucun compte de membre de l'organisation actuellement désactivé. GuardDuty Pour plus d'informations sur la configuration de vos comptes membres, ouvrez Comptes dans le volet de navigation de la GuardDuty console ou utilisez le ListMembersAPI.

Ajouter des membres à l'organisation

Choisissez une méthode d'accès préférée pour ajouter des membres à votre organisation.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Pour vous connecter, utilisez les informations d'identification du compte GuardDuty administrateur délégué.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).

   Le tableau des comptes affiche tous les comptes ajoutés, soit Via les organisations (AWS Organizations) ou Par invitation. Si un compte de membre n'est pas associé au compte GuardDuty administrateur de l'organisation, le statut de ce compte de membre est Non membre.

3. Sélectionnez un ou plusieurs comptes IDs que vous souhaitez ajouter en tant que membres. Ces comptes IDs doivent être de type Via Organizations.

   Les comptes ajoutés par invitation ne font pas partie de votre organisation. Vous pouvez gérer ces comptes individuellement. Pour de plus amples informations, veuillez consulter Gestion des comptes par invitation.

4. Choisissez Actions, puis Ajouter un membre. Après avoir ajouté ce compte en tant que membre, la GuardDuty configuration d'activation automatique s'applique. Selon les paramètres définis dansMettre à jour les préférences d'activation automatique de l'organisation, la GuardDuty configuration de ces comptes peut changer.

5. Vous pouvez sélectionner la flèche vers le bas de la colonne État pour trier les comptes selon le statut Non membre, puis choisir chaque compte qui n'est pas GuardDuty activé dans la région actuelle.

   Si aucun des comptes répertoriés dans le tableau des comptes n'a encore été ajouté en tant que membre, vous pouvez activer tous les comptes de l'organisation GuardDuty dans la région actuelle. Dans la bannière en haut de la page, choisissez Activer. Cette action active automatiquement la GuardDuty configuration d'activation automatique afin qu' GuardDuty elle soit activée pour tout nouveau compte qui rejoint l'organisation.

6. Choisissez Confirmer pour ajouter les comptes en tant que membres. Cette action active GuardDuty également tous les comptes sélectionnés. La valeur Statut des comptes invités devient Activé.

7. (Recommandé) Répétez ces étapes pour chacune d'entre elles Région AWS. Cela garantit que le compte d' GuardDuty administrateur délégué peut gérer les résultats et les autres configurations des comptes membres dans toutes les régions où vous l'avez GuardDuty activé.

   La fonction d'activation automatique est accessible GuardDuty à tous les futurs membres de votre organisation. Cela permet à votre compte d' GuardDuty administrateur délégué de gérer tous les nouveaux membres créés au sein de l'organisation ou ajoutés à celle-ci. Lorsque le nombre de comptes de membres atteint la limite de 50 000, la fonction d'activation automatique est automatiquement désactivée. Si vous supprimez un compte de membre et que le nombre total de membres tombe à moins de 50 000, la fonction d'activation automatique est réactivée.

API/CLI

- Exécutez en CreateMembersutilisant les informations d'identification du compte GuardDuty d'administrateur délégué désigné à l'étape précédente.

  Vous devez spécifier l'ID de détecteur régional du compte d' GuardDuty administrateur délégué et les détails du compte (Compte AWS IDset les adresses e-mail correspondantes) des comptes que vous souhaitez ajouter en tant que GuardDuty membres. Vous pouvez créer un ou plusieurs membres à l'aide de cette API opération.

  Lorsque vous gérez CreateMembers au sein de votre organisation, les préférences d'activation automatique pour les nouveaux membres s'appliquent à mesure que de

nouveaux comptes membres rejoignent votre organisation. Lorsque vous utilisez CreateMembers un compte membre existant, la configuration de l'organisation s'applique également aux membres existants. Cela peut modifier la configuration actuelle des comptes de membres existants.

Exécutez ListAccountsdans la AWS Organizations APIréférence pour afficher tous les comptes de l' AWS organisation.

> **Important**
>
> Lorsque vous ajoutez un compte en tant que GuardDuty membre, il sera automatiquement GuardDuty activé dans cette région. Il existe une exception au compte de gestion de l'organisation. Avant que le compte de gestion ne soit ajouté en tant que GuardDuty membre, il doit être GuardDuty activé.

- Vous pouvez également utiliser AWS Command Line Interface. Exécutez la commande AWS CLI suivante et assurez-vous d'utiliser votre propre ID de détecteur valide, votre ID Compte AWS et l'adresse e-mail associée à l'ID de compte.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
   --account-details AccountId=111122223333,Email=guardduty-member-
  name@amazon.com
  ```

  Vous pouvez consulter la liste de tous les membres de l'organisation en exécutant la AWS CLI commande suivante :

  ```
  aws organizations list-accounts
  ```

Après avoir ajouté ce compte en tant que membre, la GuardDuty configuration d'activation automatique s'applique.

(Facultatif) Activez les plans de protection pour les comptes de membres existants

La procédure suivante inclut les étapes permettant d'activer les plans de protection pour les comptes de membres existants à l'aide de la page Comptes. Pour savoir comment procéder en utilisant API ou AWS CLI, consultez les documents relatifs au plan de protection spécifique.

Vous pouvez activer les plans de protection pour des comptes individuels via la page Comptes.

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Utilisez les informations d'identification GuardDuty du compte administrateur délégué.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sélectionnez un ou plusieurs comptes pour lesquels vous souhaitez configurer un plan de protection. Répétez les étapes suivantes pour chaque plan de protection que vous souhaitez configurer :

   a. Choisissez Modifier les plans de protection.

   b. Dans la liste des plans de protection, choisissez celui que vous souhaitez configurer.

   c. Choisissez l'une des actions que vous souhaitez effectuer pour ce plan de protection, puis cliquez sur Confirmer.

   d. Pour le compte sélectionné, la colonne correspondant au plan de protection configuré affichera la configuration mise à jour en tant que Activée ou Non activée.

Maintien de votre organisation au sein GuardDuty

En tant que compte d' GuardDuty administrateur délégué, vous êtes chargé de gérer la configuration GuardDuty et les plans de protection facultatifs de tous les comptes pris en charge au sein de votre organisation Région AWS. Les sections suivantes présentent les options relatives au maintien de l'état de configuration de GuardDuty ou de l'un de ses plans de protection facultatifs :

Pour maintenir l'état de configuration de l'ensemble de votre organisation dans chaque région

- Définissez les préférences d'activation automatique pour l'ensemble de l'organisation à l'aide de la GuardDuty console : vous pouvez les activer GuardDuty automatiquement pour tous (`ALL`) les membres de l'organisation ou pour les nouveaux (`NEW`) membres qui rejoignent l'organisation, ou choisir de ne pas (`NONE`) l'activer automatiquement pour aucun des membres de l'organisation.

Vous pouvez également configurer des paramètres identiques ou différents pour tous les plans de protection inclus GuardDuty.

La mise à jour de la configuration de tous les comptes membres de l'organisation peut prendre jusqu'à 24 heures.

- Mettez à jour les préférences d'activation automatique en utilisant API — Exécuter UpdateOrganizationConfigurationpour configurer automatiquement GuardDuty et ses plans de protection facultatifs pour l'organisation. Lorsque vous lancez CreateMemberspour ajouter de nouveaux comptes membres dans votre organisation, les paramètres configurés s'appliquent automatiquement. Lorsque vous utilisez CreateMembers un compte de membre existant, la configuration de l'organisation s'applique également aux membres existants. Cela peut modifier la configuration actuelle des comptes de membres existants.

  Pour consulter tous les comptes de votre organisation, lancez-vous ListAccountsdans la AWS Organizations APIréférence.

Pour maintenir l'état de configuration des comptes membres individuellement dans chaque région

- Pour consulter tous les comptes de votre organisation, lancez-vous ListAccountsdans la AWS Organizations APIréférence.
- Si vous souhaitez que les comptes de membres sélectionnés aient un statut de configuration différent, UpdateMemberDetectorsexécutez-les individuellement pour chaque compte membre.

  Vous pouvez utiliser GuardDuty la console pour effectuer la même tâche en accédant à la page Comptes de la GuardDuty console.

  Pour plus d'informations sur l'activation des plans de protection pour des comptes individuels à l'aide de l'une ou l'autre des consolesAPI, consultez la page de configuration du plan de protection correspondant.

Modification du compte GuardDuty d'administrateur délégué

Vous pouvez modifier le compte d' GuardDuty administrateur délégué de votre organisation dans chaque région, puis déléguer un nouvel administrateur dans chaque région. Pour garantir la sécurité des comptes des membres de votre organisation dans une région, vous devez disposer d'un compte d' GuardDuty administrateur délégué dans cette région.

Supprimer un compte d' GuardDuty administrateur délégué existant

Étape 1 - Pour supprimer le compte d' GuardDuty administrateur délégué existant dans chaque région

1. En tant que compte d' GuardDuty administrateur délégué existant, listez tous les comptes de membre associés à votre compte d'administrateur. Courez ListMembersavec`OnlyAssociated=false`.
2. Si la préférence d'activation automatique pour GuardDuty ou l'un des plans de protection facultatifs est définie sur`ALL`, exécutez pour mettre à jour la configuration UpdateOrganizationConfigurationde l'organisation vers l'un `NEW` ou `NONE` l'autre. Cette action empêchera une erreur lorsque vous dissocierez tous les comptes des membres à l'étape suivante.
3. Exécutez DisassociateMemberspour dissocier tous les comptes membres associés au compte administrateur.
4. Exécutez DeleteMemberspour supprimer les associations entre le compte administrateur et les comptes membres.
5. En tant que compte de gestion de l'organisation, exécutez la procédure DisableOrganizationAdminAccountpour supprimer le compte GuardDuty administrateur délégué existant.
6. Répétez ces étapes dans chaque Région AWS cas où vous possédez ce compte GuardDuty d'administrateur délégué.

Étape 2 - Pour désenregistrer le compte GuardDuty administrateur délégué existant dans AWS Organizations (Action globale unique)

- Exécutez DeregisterDelegatedAdministratordans la AWS Organizations APIréférence, pour désenregistrer le compte GuardDuty administrateur délégué existant dans AWS Organizations.

  Vous pouvez également exécuter la AWS CLI commande suivante :

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Assurez-vous de remplacer *111122223333* avec le compte d' GuardDuty administrateur délégué existant.

Après avoir désenregistré l'ancien compte d' GuardDuty administrateur délégué, vous pouvez l'ajouter en tant que compte de membre au nouveau compte d' GuardDuty administrateur délégué.

Désignation d'un nouveau compte d' GuardDuty administrateur délégué dans chaque région

1. Désignez un nouveau compte d' GuardDuty administrateur délégué dans chaque région en utilisant votre méthode d'accès préférée : GuardDuty console ou API ou AWS CLI. Pour de plus amples informations, veuillez consulter Désignation d'un compte d'administrateur délégué GuardDuty .
2. Exécutez DescribeOrganizationConfigurationpour afficher la configuration d'activation automatique actuelle de votre organisation.

> **Important**
>
> Avant d'ajouter des membres au nouveau compte d' GuardDuty administrateur délégué, vous devez vérifier la configuration d'activation automatique pour votre organisation. Cette configuration est spécifique au nouveau compte d' GuardDuty administrateur délégué et à la région sélectionnée, et n'est pas liée à AWS Organizations. Lorsque vous ajoutez un compte de membre de l'organisation (nouveau ou existant) sous le nouveau compte d' GuardDuty administrateur délégué, la configuration d'activation automatique du nouveau compte d' GuardDuty administrateur délégué s'applique au moment de l'activation GuardDuty ou de l'un de ses plans de protection facultatifs.

Modifiez la configuration de l'organisation pour le nouveau compte d' GuardDuty administrateur délégué en utilisant votre méthode d'accès préférée : GuardDuty console ou API ou AWS CLI. Pour de plus amples informations, veuillez consulter Mettre à jour les préférences d'activation automatique de l'organisation.

Gestion GuardDuty des comptes sur invitation

Pour gérer des comptes en dehors de votre organisation, vous pouvez utiliser la méthode d'invitation héritée. Lorsque vous utilisez cette méthode, votre compte est désigné comme compte administrateur lorsqu'un autre compte accepte votre invitation à devenir un compte membre.

Si votre compte n'est pas un compte administrateur, vous pouvez accepter une invitation provenant d'un autre compte. Lorsque vous acceptez, votre compte devient un compte membre. Un AWS compte ne peut pas être à la fois un compte GuardDuty administrateur et un compte membre.

Lorsque vous acceptez l'invitation d'un compte, vous ne pouvez pas accepter l'invitation d'un autre compte. Pour accepter une invitation provenant d'un autre compte, vous devez d'abord dissocier votre compte du compte administrateur existant. Le compte administrateur peut également dissocier votre compte de son organisation et le supprimer.

Les comptes associés par invitation ont la même account-to-member relation d'administrateur globale que les comptes associés par AWS Organizations, comme décrit dansComprendre la relation entre le compte GuardDuty administrateur et les comptes membres. Toutefois, les utilisateurs du compte administrateur des invitations ne peuvent pas GuardDuty activer au nom des comptes membres associés ni consulter d'autres comptes non membres au sein de leur AWS Organizations organisation.

> **Important**
>
> Un transfert de données interrégional peut avoir lieu lors de la GuardDuty création de comptes membres à l'aide de cette méthode. Afin de vérifier les adresses e-mail des comptes des membres, GuardDuty utilise un service de vérification des e-mails qui fonctionne uniquement dans la région de l'est des États-Unis (Virginie du Nord).

Ajout et gestion des comptes par invitation

Choisissez l'une des méthodes d'accès pour ajouter et inviter des comptes à devenir des comptes GuardDuty membres en tant que compte GuardDuty administrateur.

Console

Étape 1 : ajouter un compte

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Choisissez Ajouter des comptes par invitation dans le panneau supérieur.
4. Sur la page Ajouter des comptes membres, sous Entrez les détails du compte, entrez l' Compte AWS identifiant et l'adresse e-mail associés au compte que vous souhaitez ajouter.
5. Pour ajouter une autre ligne afin de saisir les détails du compte un par un, choisissez Ajouter un autre compte. Vous pouvez également choisir Charger un fichier .csv avec les détails du compte pour ajouter des comptes en bloc.

   > **Important**
   >
   > La première ligne de votre fichier csv doit contenir l'en-tête, comme illustré dans l'exemple ci-dessous : `Account ID,Email`. Chaque ligne suivante doit contenir un seul Compte AWS identifiant valide et l'adresse e-mail associée. Le format d'une ligne est valide si elle ne contient qu'un seul Compte AWS identifiant et l'adresse e-mail associée séparés par une virgule.
   >
   > ```
   > Account ID,Email
   > 555555555555,user@example.com
   > ```

6. Après avoir ajouté tous les détails des comptes, choisissez Suivant. Vous pouvez consulter les comptes récemment ajoutés dans le tableau Comptes. L'état de ces comptes sera Invitation non envoyée. Pour plus d'informations sur l'envoi d'une invitation à un ou plusieurs comptes ajoutés, veuillez consulter Step 2 - Invite an account.

Étape 2 : inviter un compte

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Accounts (Comptes).
3. Sélectionnez un ou plusieurs comptes que vous souhaitez inviter sur Amazon GuardDuty.
4. Choisissez le menu déroulant Actions, puis choisissez Inviter.
5. Dans la GuardDuty boîte de dialogue Invitation à, entrez un message d'invitation (facultatif).

   Si le compte invité n'a pas accès aux e-mails, sélectionnez Envoyer également une notification par e-mail à l'utilisateur root sur le Compte AWS de l'invité et générer une alerte dans le AWS Health Dashboard de l'invité.

6. Choisissez Send invitation (Envoyer une invitation). Si les invités ont accès à l'adresse e-mail spécifiée, ils peuvent consulter l'invitation en ouvrant la GuardDuty console à l'adresse. https://console.aws.amazon.com/guardduty/
7. Lorsqu'un invité accepte l'invitation, la valeur de la colonne Statut devient Invité. Pour plus d'informations sur l'acceptation d'une invitation, veuillez consulter Step 3 - Accept an invitation.

Étape 3 : accepter une invitation

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   > **Important**
   >
   > Vous devez l'activer GuardDuty avant de pouvoir consulter ou accepter une invitation d'adhésion.

2. Procédez comme suit uniquement si vous ne l'avez pas GuardDuty encore activé ; sinon, vous pouvez ignorer cette étape et passer à l'étape suivante.

   Si vous ne l'avez pas encore activé GuardDuty, choisissez Get Started sur la GuardDuty page Amazon.

   Sur la GuardDuty page Bienvenue, sélectionnez Activer GuardDuty.
3. Après avoir activé GuardDuty votre compte, procédez comme suit pour accepter l'invitation d'adhésion :

   a. Dans le panneau de navigation, sélectionnez Settings (Paramètres).

   b. Choisissez Accounts.

   c. Sur les comptes, assurez-vous de vérifier le propriétaire du compte à partir duquel vous acceptez l'invitation. Activez Accepter pour accepter l'invitation d'adhésion.
4. Une fois que vous avez accepté l'invitation, votre compte devient un compte GuardDuty membre. Le compte dont le propriétaire a envoyé l'invitation devient le compte GuardDuty administrateur. Le compte administrateur saura que vous avez accepté l'invitation. Le tableau des comptes de leur GuardDuty compte sera mis à jour. La valeur de la colonne État correspondant à votre identifiant de compte de membre deviendra Activé. Le titulaire du compte administrateur peut désormais consulter GuardDuty et gérer les configurations du

plan de protection pour le compte de votre compte. Le compte administrateur peut également consulter et gérer les GuardDuty résultats générés pour votre compte membre.

API/CLI

Vous pouvez désigner un compte GuardDuty administrateur et créer ou ajouter des comptes GuardDuty membres sur invitation via les API opérations. Exécutez les GuardDuty API opérations suivantes afin de désigner le compte administrateur et les comptes membres dans GuardDuty.

Effectuez la procédure suivante en utilisant les informations d'identification du compte Compte AWS que vous souhaitez désigner comme compte GuardDuty administrateur.

Création ou ajout de comptes membres

1. Exécutez l'CreateMembersAPIopération en utilisant les informations d'identification du AWS compte GuardDuty activé. Il s'agit du compte que vous souhaitez utiliser comme GuardDuty compte administrateur.

   Vous devez spécifier l'identifiant du détecteur du AWS compte actuel ainsi que l'identifiant du compte et l'adresse e-mail des comptes dont vous souhaitez devenir GuardDuty membres. Vous pouvez créer un ou plusieurs membres à l'aide de cette API opération.

   Vous pouvez également utiliser les outils de ligne de AWS commande pour désigner un compte administrateur en exécutant la CLI commande suivante. Assurez-vous d'utiliser vos propres ID de détecteur, ID de compte et adresse e-mail valides.

   Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Exécutez InviteMembersen utilisant les informations d'identification du AWS compte GuardDuty activé. Il s'agit du compte que vous souhaitez utiliser comme GuardDuty compte administrateur.

   Vous devez spécifier l'identifiant du détecteur du AWS compte courant et le compte IDs des comptes dont vous souhaitez devenir GuardDuty membres. Vous pouvez inviter un ou plusieurs membres avec cette API opération.

> **Note**
>
> Vous pouvez également spécifier un message d'invitation en option à l'aide du paramètre de requête `message`.

Vous pouvez également l'utiliser AWS Command Line Interface pour désigner des comptes membres en exécutant la commande suivante. Assurez-vous d'utiliser votre propre identifiant de détecteur valide et votre propre compte valide IDs pour les comptes que vous souhaitez inviter.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Acceptation d'invitations

Effectuez la procédure suivante en utilisant les informations d'identification de chaque AWS compte que vous souhaitez désigner comme compte GuardDuty membre.

1. Exécutez l'CreateDetectorAPIopération pour chaque AWS compte qui a été invité à devenir un compte GuardDuty membre et pour lequel vous souhaitez accepter une invitation.

   Vous devez spécifier si la ressource du détecteur doit être activée à l'aide du GuardDuty service. Un détecteur doit être créé et activé GuardDuty pour être opérationnel. Vous devez d'abord l'activer GuardDuty avant d'accepter une invitation.

   Vous pouvez également le faire en utilisant les outils de ligne de AWS commande à l'aide de la CLI commande suivante.

   ```
   aws guardduty create-detector --enable
   ```

2. Exécutez l'AcceptAdministratorInvitationAPIopération pour chaque AWS compte pour lequel vous souhaitez accepter l'invitation d'adhésion, en utilisant les informations d'identification de ce compte.

Vous devez spécifier l'ID de détecteur de ce AWS compte pour le compte membre, l'ID de compte du compte administrateur qui a envoyé l'invitation et l'ID d'invitation de l'invitation que vous acceptez. Vous pouvez trouver l'identifiant du compte administrateur dans l'e-mail d'invitation ou en ListInvitationsutilisant leAPI.

Vous pouvez également accepter une invitation à l'aide des outils de ligne de AWS commande en exécutant la CLI commande suivante. Assurez-vous d'utiliser un ID de détecteur, un ID de compte administrateur et un ID d'invitation valides.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

Consolidation des comptes d' GuardDuty administrateur sous un seul compte d' GuardDuty administrateur délégué de l'organisation

GuardDuty recommande d'utiliser le service d'association AWS Organizations pour gérer les comptes des membres sous un compte d' GuardDuty administrateur délégué. Vous pouvez utiliser l'exemple de processus décrit ci-dessous pour consolider le compte administrateur et le membre associé sur invitation dans une organisation sous un seul compte d' GuardDuty administrateur GuardDuty délégué.

> **Note**
>
> Les comptes déjà gérés par un compte d' GuardDuty administrateur délégué ou les comptes de membres actifs associés à un compte d' GuardDuty administrateur délégué ne peuvent pas être ajoutés à un autre compte d' GuardDuty administrateur délégué. Chaque organisation ne peut avoir qu'un seul compte d' GuardDuty administrateur délégué par région, et chaque compte de membre ne peut avoir qu'un seul compte d' GuardDuty administrateur délégué.

Choisissez l'une des méthodes d'accès pour consolider les comptes d' GuardDuty administrateur sous un seul compte d' GuardDuty administrateur délégué.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Pour vous connecter, utilisez les informations d'identification du compte de gestion de l'organisation.
2. Tous les comptes que vous souhaitez gérer GuardDuty doivent faire partie de votre organisation. Pour plus d'informations sur l'ajout d'un compte à votre organisation, voir Inviter un Compte AWS homme à rejoindre votre organisation.
3. Assurez-vous que tous les comptes de membre sont associés au compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué unique. Dissociez tout compte membre toujours associé aux comptes administrateur préexistants.

   Les étapes suivantes vous aideront à dissocier les comptes membres du compte administrateur préexistant :

   a. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   b. Pour vous connecter, utilisez les informations d'identification du compte administrateur préexistant.

   c. Dans le panneau de navigation, choisissez Accounts (Comptes).

   d. Sur la page Comptes, sélectionnez un ou plusieurs comptes que vous souhaitez dissocier du compte administrateur.

   e. Choisissez Actions, puis Dissocier le compte.

   f. Choisissez Confirmer pour finaliser l'étape.
4. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Pour vous connecter, utilisez les informations d'identification du compte de gestion .
5. Dans le panneau de navigation, sélectionnez Settings (Paramètres). Sur la page Paramètres, désignez le compte GuardDuty d'administrateur délégué pour l'organisation.
6. Connectez-vous au compte d' GuardDuty administrateur délégué désigné.
7. Ajoutez des membres de l'organisation. Pour plus d’informations, consultez Gérer des GuardDuty comptes avec AWS Organizations.

API/CLI

1. Tous les comptes que vous souhaitez gérer GuardDuty doivent faire partie de votre organisation. Pour plus d'informations sur l'ajout d'un compte à votre organisation, voir Inviter un Compte AWS homme à rejoindre votre organisation.
2. Assurez-vous que tous les comptes de membre sont associés au compte que vous souhaitez désigner comme compte d' GuardDuty administrateur délégué unique.

   a. Exécutez DisassociateMemberspour dissocier tout compte de membre toujours associé aux comptes d'administrateur préexistants.

   b. Vous pouvez également AWS Command Line Interface exécuter la commande suivante et remplacer *777777777777* avec l'identifiant du détecteur du compte administrateur préexistant dont vous souhaitez dissocier le compte membre. Remplacez *666666666666* avec l' Compte AWS identifiant du compte membre que vous souhaitez dissocier.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
   ```

3. Exécutez EnableOrganizationAdminAccountpour déléguer un compte Compte AWS en tant GuardDuty qu'administrateur délégué.

   Vous pouvez également exécuter la commande suivante AWS Command Line Interface pour déléguer un compte d' GuardDuty administrateur délégué :

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. Ajoutez des membres de l'organisation. Pour plus d’informations, consultez Create or add member member accounts using API.

> **Important**
>
> Pour optimiser l'efficacité d' GuardDutyun service régional, nous vous recommandons de désigner votre compte d' GuardDuty administrateur délégué et d'ajouter tous vos comptes de membre dans chaque région.

GuardDuty Activation simultanée sur plusieurs comptes

Utilisez la méthode suivante pour l'activer GuardDuty dans plusieurs comptes en même temps.

Utilisez des scripts Python pour activer GuardDuty simultanément plusieurs comptes

Vous pouvez automatiser l'activation ou la désactivation de plusieurs comptes à l'aide des scripts du référentiel d'exemples GuardDuty sur Amazon GuardDuty Multiaccount Scripts. Utilisez le processus décrit dans cette section GuardDuty pour activer la liste des comptes de membres utilisant AmazonEC2. Pour plus d'informations sur l'utilisation du script de désactivation ou sur sa configuration locale, reportez-vous aux instructions figurant dans le lien partagé.

Le `enableguardduty.py` script active GuardDuty, envoie des invitations depuis le compte administrateur et accepte les invitations dans tous les comptes membres. Le résultat est un GuardDuty compte administrateur qui contient tous les résultats de sécurité pour tous les comptes membres. Étant donné qu' GuardDuty il est isolé par région, les résultats pour chaque compte membre sont répercutés sur la région correspondante dans le compte administrateur. Par exemple, la région us-east-1 de GuardDuty votre compte administrateur contient les résultats de sécurité relatifs à tous les résultats us-east-1 provenant de tous les comptes membres associés.

Ces scripts dépendent d'un IAM rôle partagé avec la politique gérée —AWS politique gérée : AmazonGuardDutyFullAccess. Cette politique permet aux entités d'accéder au compte administrateur GuardDuty et doit être présente sur celui-ci et dans chaque compte pour lequel vous souhaitez l'activer GuardDuty.

Le processus suivant est activé par défaut GuardDuty dans toutes les régions disponibles. Vous pouvez l'activer GuardDuty dans les régions spécifiées uniquement en utilisant l'`--enabled_regions`argument facultatif et en fournissant une liste de régions séparées par des virgules. Vous pouvez également personnaliser le message d'invitation envoyé aux comptes membres en ouvrant `enableguardduty.py` et en modifiant la chaîne `gd_invite_message`.

1. Créez un IAM rôle dans le compte GuardDuty administrateur et associez la AWS politique gérée : AmazonGuardDutyFullAccess politique à activer GuardDuty.
2. Créez un IAM rôle dans chaque compte de membre que vous souhaitez voir gérer par votre compte GuardDuty d'administrateur. Ce rôle doit porter le même nom que le rôle créé à l'étape 1, il doit autoriser le compte administrateur en tant qu'entité de confiance et il doit avoir la même politique AmazonGuardDutyFullAccess gérée décrite précédemment.
3. Lancez une nouvelle instance Amazon Linux avec un rôle attaché ayant la relation d'approbation suivante, qui permet à l'instance d'assumer un rôle de service.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Connectez-vous à la nouvelle instance et exécutez les commandes suivantes pour la configurer.

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. Créez un CSV fichier contenant la liste des comptes IDs et des e-mails des comptes de membres auxquels vous avez ajouté un rôle à l'étape 2. Chaque compte doit figurer sur une ligne distincte, et l'ID de compte et l'adresse e-mail doivent être séparés par une virgule, comme illustré dans l'exemple suivant.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> Le CSV fichier doit se trouver au même emplacement que votre `enableguardduty.py` script. Vous pouvez copier un CSV fichier existant depuis Amazon S3 vers votre répertoire actuel à l'aide de la méthode suivante.
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Exécutez le script python. Assurez-vous de fournir votre identifiant de compte GuardDuty administrateur, le nom du rôle créé lors des premières étapes et le nom de votre CSV fichier comme arguments.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Comprendre les GuardDuty résultats d'Amazon

Une GuardDuty découverte représente un problème de sécurité potentiel détecté au sein de votre réseau. GuardDutygénère un résultat chaque fois qu'il détecte une activité inattendue et potentiellement malveillante dans votre AWS environnement.

Vous pouvez consulter et gérer vos GuardDuty résultats sur la page Résultats de la GuardDuty console ou à l'aide API des opérations AWS CLI or. Pour un aperçu des façons dont vous pouvez gérer les résultats, veuillez consulter Gérer les GuardDuty résultats d'Amazon.

Rubriques :

Format de résultat GuardDuty

Comprenez le format des types de GuardDuty recherche et les différents objectifs des menaces suivis par GuardDuty.

Exemples de résultats

Essayez de générer des échantillons de résultats pour tester et comprendre GuardDuty les résultats et les détails associés. Ces résultats sont marqués d'un préfixe [SAMPLE].

GuardDuty Résultats des tests dans des comptes dédiés

Exécutez un `guardduty-tester` script dans une non-production dédiée Compte AWS pour générer des GuardDuty résultats sélectionnés dans votre AWS environnement.

Détails d’un résultat

Découvrez les détails associés aux GuardDuty résultats générés dans votre compte.

Types de résultats

Affichez et recherchez toutes les recherches GuardDuty disponibles par type. Chaque entrée de type de résultat comprend une explication de ce dernier, ainsi que des conseils et des suggestions de mesure corrective.

Format de résultat GuardDuty

Quand GuardDuty détecte un comportement suspect ou inattendu dans votre environnement AWS, il génère un résultat. Un résultat est une notification qui contient les détails sur un problème de sécurité potentiel découvert par GuardDuty. Les détails du résultat incluent des informations sur ce qui s'est

passé, les ressources AWS impliquées dans l'activité suspecte, le moment où cette activité a eu lieu et d'autres informations.

Le type de résultat est l'une des informations les plus utiles. Le type de résultat vise à fournir une description brève mais intelligible du problème de sécurité potentiel. Par exemple, le type de résultat Recon:EC2/PortProbeUnprotectedPort de GuardDuty vous informe rapidement qu'un port non protégé d'une instance EC2 de votre environnement AWS est en train d'être analysé par un pirate potentiel.

GuardDuty utilise le format de dénomination suivant pour les différents types de résultat qu'il génère :

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

Chaque partie de ce format représente un aspect d'un type de résultat. Ces aspects sont expliqués comme suit :

- ThreatPurpose : décrit l'objectif principal d'une menace, d'un type d'attaque ou d'une étape d'une attaque potentielle. Consultez la section suivante pour obtenir une liste complète des objectifs de GuardDuty en matière de menaces.
- ResourceTypeAffected : décrit le type de ressource AWS identifié en tant que cible potentielle d'un adversaire dans ce résultat. Actuellement, GuardDuty peut générer des résultats pour les ressources EC2, S3, IAM et EKS.
- ThreatFamilyName : décrit la menace ou l'activité malveillante potentielle globale détectée par GuardDuty. Par exemple, la valeur NetworkPortUnusual indique qu'une instance EC2 identifiée dans le résultat de GuardDuty n'a aucun historique de communication avec un port distant également identifié dans ce résultat.
- DetectionMechanism : décrit la méthode par laquelle GuardDuty a détecté le résultat. Cela peut être utilisé pour indiquer une variation par rapport à un type de résultat courant ou un résultat que GuardDuty a utilisé pour détecter un mécanisme spécifique. Par exemple, Backdoor:EC2/DenialOfService.Tcp indique qu'un déni de service (DoS) a été détecté via TCP. La variante UDP est Backdoor:EC2/DenialOfService.Udp.

  La valeur .Personnalisé indique que GuardDuty a détecté le résultat sur la base de vos listes de menaces personnalisées, tandis que Réputation indique que GuardDuty a détecté le résultat à l'aide d'un modèle de score de réputation de domaine.
- Artefact : décrit une ressource spécifique appartenant à un outil utilisé pour l'activité malveillante. Par exemple, DNS dans le type de résultat CryptoCurrency:EC2/BitcoinTool.B!DNS indique qu'une instance EC2 communique avec un domaine connu lié au bitcoin.

Buts de la menace

Dans GuardDuty, un but de la menace décrit l'objectif principal d'une menace, un type d'attaque ou le stade d'une attaque potentielle. Par exemple, certaines menaces, telles que Backdoor, indiquent un type d'attaque. Cependant, certains buts de la menace, tels que Impact, s'alignent sur les tactiques MITRE ATT&CK. Les tactiques MITRE ATT&CK indiquent les différentes phases du cycle d'attaque d'un adversaire. Dans la version actuelle de GuardDuty, ThreatPurpose peut avoir les valeurs suivantes :

Backdoor

Cette valeur indique que l'attaque a compromis une ressource AWS et l'a modifiée afin d'être à même de contacter son serveur de contrôle et de commande (C&C) pour recevoir des instructions supplémentaires à des fins malveillantes.

Comportement

Cette valeur indique que GuardDuty a détecté une activité ou des modèles d'activité différents de la référence établie pour les ressources AWS impliquées.

CredentialAccess

Cette valeur indique que GuardDuty a détecté des modèles d'activité qu'un adversaire pourrait utiliser pour voler des informations d'identification, telles que des ID de compte ou des mots de passe, dans votre environnement. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Cryptomonnaie

Cette valeur indique que GuardDuty a détecté qu'une ressource AWS de votre environnement héberge un logiciel associé à des cryptomonnaies (par exemple, le Bitcoin).

DefenseEvasion

Cette valeur indique que GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire peut utiliser pour éviter d'être détecté lorsqu'il infiltre votre environnement. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Découverte

Cette valeur indique que GuardDuty a détecté des activités ou des modèles d'activité qu'un adversaire pourrait utiliser pour approfondir ses connaissances de vos systèmes et de vos réseaux internes. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Exécution

Cette valeur indique que GuardDuty a détecté qu'un adversaire pourrait essayer d'exécuter un code malveillant pour explorer le réseau ou voler des données. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Exfiltration

Cette valeur indique que GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire pourrait utiliser lorsqu'il tente de voler des données sur votre réseau. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Impact

Cette valeur indique que GuardDuty a détecté une activité ou des modèles d'activité qui suggèrent qu'un adversaire tente de manipuler, d'interrompre ou de détruire vos systèmes et vos données. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

InitialAccess

Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Pentest

Parfois, les propriétaires de ressources AWS ou leurs représentants autorisés exécutent intentionnellement des tests sur des applications AWS pour identifier leurs vulnérabilités (groupes de sécurité ouverts, clés d'accès trop permissives). Ces tests d'intrusion sont réalisés pour tenter d'identifier et de verrouiller les ressources vulnérables avant qu'elles ne soient découvertes par des adversaires. Toutefois, certains des outils utilisés par les testeurs autorisés sont disponibles gratuitement et peuvent donc être utilisés par des utilisateurs non autorisés ou des adversaires à des fins d'analyse. Bien que GuardDuty ne puisse pas identifier le véritable objectif de cette activité, la valeur Pentest indique que GuardDuty détecte une telle activité, qu'elle est similaire à l'activité générée par des outils de test d'intrusion connus, et qu'elle pourrait indiquer un sondage malveillant de votre réseau.

Persistance

Cette valeur indique que GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire peut utiliser pour tenter de conserver l'accès à vos systèmes, même si sa voie d'accès initiale est coupée. Par exemple, cela peut inclure la création d'un utilisateur IAM après avoir obtenu l'accès via les informations d'identification compromises d'un utilisateur existant. Lorsque les informations d'identification de l'utilisateur existant sont supprimées, l'adversaire retient l'accès

au nouvel utilisateur qui n'a pas été détecté lors de l'événement d'origine. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Stratégie

Cette valeur indique que votre Compte AWS présente un comportement qui va à l'encontre des bonnes pratiques en matière de sécurité.

PrivilegeEscalation

Cette valeur vous indique que le principal impliqué dans votre environnement AWS présente un comportement susceptible d'être utilisé par un adversaire pour obtenir des autorisations de niveau supérieur sur votre réseau. Ce but de la menace est basé sur les tactiques MITRE ATT&CK.

Recon

Cette valeur indique que GuardDuty a détecté une activité ou des modèles d'activité qu'un adversaire peut utiliser lors de la reconnaissance de votre réseau afin de déterminer comment il peut élargir son accès ou utiliser vos ressources. Par exemple, cette activité peut inclure l'identification des vulnérabilités de votre environnement AWS en analysant les ports, en répertoriant les utilisateurs, les tables de base de données, etc.

Stealth

Cette valeur indique qu'un adversaire essaie activement de masquer ses actions. Par exemple, il peut utiliser un serveur proxy anonyme, ce qui rend extrêmement difficile l'évaluation de la véritable nature de l'activité.

Trojan

Cette valeur indique qu'une attaque utilise des chevaux de Troie pour mener une action malveillante en silence. Parfois, ce logiciel prend l'aspect d'un programme légitime. Parfois, les utilisateurs l'exécutent accidentellement. Ou bien le logiciel peut s'exécuter automatiquement en exploitant une vulnérabilité.

UnauthorizedAccess

Cette valeur indique que GuardDuty a détecté une activité suspecte ou un modèle d'activité suspecte de la part d'un individu non autorisé.

GuardDuty moteur d'analyse pour la détection des malwares

Amazon GuardDuty dispose d'un moteur de scan conçu et géré en interne et d'un fournisseur tiers. Les deux utilisent des indicateurs de compromission (IoCs) provenant de différents flux internes

qui permettent de visualiser les différents types de malwares susceptibles de les cibler AWS. GuardDuty propose également des définitions de détection basées sur des YARA règles ajoutées par nos ingénieurs en sécurité, ainsi que des détections basées sur des modèles heuristiques et d'apprentissage automatique (ML). La détection basée sur les signatures inclut non seulement la mise en correspondance d'octets, mais également un extrait de code potentiellement complexe, et le scanner peut analyser le contenu et prendre des décisions.

Le moteur d'analyse des programmes malveillants n'effectue pas d'analyse comportementale en temps réel, dans le cadre de laquelle la détonation du logiciel malveillant surveille l'échantillon lorsqu'il s'exécute dans un système réel. La GuardDuty solution consiste principalement en une détection basée sur des fichiers. Pour détecter les malwares sans fichier, GuardDuty fournit une solution basée sur un agent, comme pour Surveillance d'exécution Amazon, Amazon EC2 et EKS Amazon ECS (y compris). AWS Fargate

Sans aucune restriction quant aux formats de fichiers permettant de détecter les malwares, les moteurs d'analyse qu'il utilise peuvent détecter différents types de malwares, tels que les cryptomineurs, les ransomwares et les webshells. GuardDuty Le moteur d' GuardDuty analyse entièrement géré met à jour en permanence la liste des signatures de logiciels malveillants toutes les 15 minutes.

Le moteur d'analyse fait partie d'un système de renseignement sur les GuardDuty menaces qui utilise un composant interne de détonation de logiciels malveillants. Cela génère de nouvelles informations sur les menaces en collectant indépendamment des malwares et des échantillons bénins provenant de sources multiples. Le type de hachage de fichier IoC du système de renseignement sur les menaces alimente également le moteur d'analyse des logiciels malveillants afin de détecter les logiciels malveillants sur la base de hachages de fichiers défectueux connus.

Génération d'échantillons de résultats dans GuardDuty

Vous pouvez générer des exemples de résultats avec Amazon GuardDuty pour vous aider à visualiser et à comprendre les différents types de résultats qui GuardDuty peuvent être générés. Lorsque vous générez des résultats d'échantillonnage GuardDuty, votre liste de résultats actuelle contient un échantillon de résultats pour chaque type de résultat pris en charge.

Les exemples générés sont des approximations renseignées avec des valeurs d'espace réservé. Ces exemples peuvent sembler différents des résultats réels pour votre environnement, mais vous pouvez les utiliser pour tester différentes configurations GuardDuty, telles que vos EventBridge événements ou vos filtres. Pour une liste des valeurs disponibles pour rechercher des types, voir le Types de résultats tableau.

Génération d'échantillons de résultats via la GuardDuty console ou API

Choisissez votre méthode d'accès préférée pour générer des exemples de résultats.

> **Note**
>
> La méthode de la console génère un résultat de chaque type. Les résultats d'un échantillon unique ne peuvent être générés que par le biais duAPI.

Console

Utilisez la procédure suivante pour générer des exemples de résultats. Ce processus génère un échantillon de recherche pour chaque type de GuardDuty recherche.

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Settings, sous Sample findings, choisissez Generate sample findings.
4. Dans le volet de navigation, choisissez Conclusions. Les exemples de résultats sont affichés sur la page Résultats actuels avec le préfixe [SAMPLE].

API/CLI

Vous pouvez générer un échantillon de recherche unique correspondant à n'importe quel type de GuardDuty recherche grâce au tableau. Les valeurs disponibles pour les types de recherche sont répertoriées dans le Types de résultats tableau. CreateSampleFindingsAPI

Cela est utile pour tester les règles relatives aux CloudWatch événements ou pour automatiser les événements en fonction des résultats. L'exemple suivant montre comment générer un exemple de résultat unique du type `Backdoor:EC2/DenialOfService.Tcp` à l'aide de l' AWS CLI.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Le titre des échantillons de résultats générés par ces méthodes commence toujours par [SAMPLE] dans la console. Les résultats des échantillons ont une valeur de `"sample": true` dans la additionalInfosection des JSON détails des résultats.

Pour générer des résultats communs basés sur une activité simulée dans un environnement dédié et isolé Compte AWS , voir GuardDuty Résultats des tests dans des comptes dédiés.

GuardDuty Résultats des tests dans des comptes dédiés

Utilisez ce document pour exécuter un script de test qui génère des GuardDuty résultats dans un script Compte AWS que vous utilisez spécifiquement à cette fin. Vous pouvez effectuer ces étapes pour comprendre et découvrir certains types de GuardDuty recherche. Cette expérience est différente de la générationExemples de résultats. Pour plus d'informations sur l'expérience des GuardDuty résultats des tests, consultezConsidérations.

Table des matières

Considérations

Avant de poursuivre, tenez compte des considérations suivantes :

- GuardDuty recommande de déployer le script du testeur dans un environnement de non-production dédié Compte AWS ou isolé. En exécutant le script du testeur, certaines AWS ressources GuardDuty seront déployées dans ce compte. Cela vous aidera également à identifier ces résultats simulés.
- Le script du testeur génère plus de 100 GuardDuty résultats avec différentes combinaisons de AWS ressources. Actuellement, cela n'inclut pas tous lesTypes de résultats. Pour obtenir la liste des types de recherche que vous pouvez générer avec ce script de test, consultezGuardDuty résultats que le script de testeur peut générer.

- Le script du testeur valide l'état GuardDuty de la configuration dans votre compte dédié. Si ce compte n' GuardDuty est pas activé, le script vous demandera de l'activer lors de votre performanceÉtape 3 - Exécuter des scripts de test. Le script du testeur vous demandera l'autorisation d'activer certains plans de protection nécessaires pour générer les résultats.

  Activation GuardDuty pour la première fois

  Lorsqu' GuardDuty il est activé sur votre compte dédié pour la première fois dans une région spécifique, votre compte sera automatiquement inscrit à un essai gratuit de 30 jours.

  GuardDuty propose des plans de protection optionnels. Au moment de l'activation GuardDuty, certains plans de protection sont également activés et sont inclus dans l'essai gratuit de GuardDuty 30 jours. Pour de plus amples informations, veuillez consulter Utilisation de l' GuardDuty essai gratuit de 30 jours.

  GuardDuty est déjà activé dans votre compte avant l'exécution du script de test

  Lorsque cette option GuardDuty est déjà activée, le script du testeur vérifie l'état de configuration de certains plans de protection et d'autres paramètres au niveau du compte requis pour générer les résultats en fonction des paramètres.

  En exécutant ce script de test, certains plans de protection peuvent être activés pour la première fois sur votre compte dédié dans une région. Cela lancera l'essai gratuit de 30 jours pour ce plan de protection. Pour plus d'informations sur l'essai gratuit associé à chaque plan de protection, consultezUtilisation de l' GuardDuty essai gratuit de 30 jours.
- Une fois le script de test terminé, la configuration et les paramètres du plan de protection d'origine de votre compte dédié seront restaurés.

GuardDuty résultats que le script de testeur peut générer

Actuellement, le script du testeur génère les types de résultats suivants liés à AmazonEC2, AmazonEKS, Amazon S3 et aux journaux EKS d'audit : IAM

- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Udp
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation

- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- PenTest:IAMUser/KaliLinux
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- PrivilegeEscalation:Kubernetes/PrivilegedContainer

- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- PenTest:S3/KaliLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

Étape 1 - Prérequis

Pour préparer votre environnement de test, vous aurez besoin des éléments suivants :

- Git — Installez l'outil de ligne de commande git en fonction du système d'exploitation que vous utilisez. Cela est nécessaire pour cloner le `amazon-guardduty-tester`dépôt.
- AWS Command Line Interface— Un outil open source avec lequel vous pouvez interagir à l'aide AWS services de commandes dans votre interface de ligne de commande. Pour plus d'informations, voir Commencer AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.
- AWS Systems Manager— Pour lancer des sessions de gestionnaire de session avec vos nœuds gérés en utilisant, AWS CLI vous devez installer le plug-in Session Manager sur votre machine locale. Pour plus d'informations, voir Installer le plug-in Session Manager AWS CLI dans le guide de AWS Systems Manager l'utilisateur.
- Node Package Manager (NPM) : installez NPM pour installer toutes les dépendances.
- Docker — Docker doit être installé. Pour obtenir les instructions d'installation, consultez le site web Docker.

  Pour vérifier que Docker a été installé, exécutez la commande suivante et vérifiez qu'il existe un résultat similaire au résultat suivant :

  ```
  $ docker --version
  Docker version 19.03.1
  ```

- Abonnez-vous à l'image Kali Linux dans le AWS Marketplace.

Étape 2 - Déployer AWS les ressources

Cette section fournit une liste des concepts clés et les étapes à suivre pour déployer certaines AWS ressources dans votre compte dédié.

Concepts

La liste suivante fournit les concepts clés liés aux commandes qui vous aident à déployer les ressources :

- AWS Cloud Development Kit (AWS CDK)— CDK est un framework de développement de logiciels open source permettant de définir l'infrastructure cloud dans le code et de la provisionner via ce dernier. AWS CloudFormation CDKprend en charge deux langages de programmation pour définir des composants cloud réutilisables appelés constructions. Vous pouvez les composer ensemble en piles et en applications. Vous pouvez ensuite déployer vos CDK applications pour AWS CloudFormation approvisionner ou mettre à jour vos ressources. Pour plus d'informations,

voir Qu'est-ce que le AWS CDK ? dans le Guide AWS Cloud Development Kit (AWS CDK) du développeur.

- Bootstrapping — Il s'agit du processus de préparation de votre AWS environnement pour une utilisation avec. AWS CDK Avant de déployer une CDK pile dans un AWS environnement, celui-ci doit d'abord être amorcé. Ce processus de mise en service de AWS ressources spécifiques dans votre environnement qui sont utilisées par AWS CDK fait partie des étapes que vous allez effectuer dans la section suivante -Étapes de déploiement AWS des ressources.

  Pour plus d'informations sur le fonctionnement du bootstrapping, voir Bootstrapping dans le manuel du développeur.AWS Cloud Development Kit (AWS CDK)

Étapes de déploiement AWS des ressources

Procédez comme suit pour commencer à déployer les ressources :

1. Configurez votre compte et votre région AWS CLI par défaut, sauf si les variables de région du compte dédié sont définies manuellement dans le `bin/cdk-gd-tester.ts` fichier. Pour plus d'informations, consultez la section Environnements du guide du AWS Cloud Development Kit (AWS CDK) développeur.
2. Exécutez les commandes suivantes pour déployer les ressources :

   ```
   git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-tester
   npm install
   cdk bootstrap
   cdk deploy
   ```

   La dernière commande (`cdk deploy`) crée une AWS CloudFormation pile en votre nom. Le nom de cette pile est GuardDutyTesterStack.

   Dans le cadre de ce script, GuardDuty crée de nouvelles ressources pour générer des GuardDuty résultats dans votre compte. Il ajoute également la paire de balises clé:valeur suivante aux instances Amazon EC2 :

   `CreatedBy:GuardDuty Test Script`

   Les EC2 instances Amazon incluent également les EC2 instances qui hébergent EKS des nœuds et des ECS clusters.

> **Types d'instances**
>
> GuardDuty crée `t3.micro` pour toutes les ressources à l'exception du groupe de EKS nœuds Amazon. Comme EKS il nécessite au moins 2 cœurs, le EKS nœud possède un type d'`t3.medium`instance. Pour plus d'informations sur les types d'instances, consultez la section Tailles disponibles dans le guide EC2 des types d'instances Amazon.

Étape 3 - Exécuter des scripts de test

Il s'agit d'un processus en deux étapes dans lequel vous devez d'abord démarrer une session avec le pilote de test, puis exécuter des scripts pour générer des GuardDuty résultats avec des combinaisons de ressources spécifiques.

Partie A - Démarrer une session avec le pilote d'essai

1. Une fois vos ressources déployées, enregistrez le code de région dans une variable dans votre session de terminal en cours. Utilisez la commande suivante et remplacez *us-east-1* avec le code de région dans lequel vous avez déployé les ressources :

```
$ REGION=us-east-1
```

2. Le script du testeur est uniquement disponible via AWS Systems Manager (SSM). Pour démarrer un shell interactif sur l'instance hôte du testeur, interrogez l'hôte InstanceId.
3. Utilisez la commande suivante pour démarrer votre session pour le script du testeur :

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

Partie B - Générer des résultats

Le script testeur est un programme basé sur Python qui crée dynamiquement un script bash pour générer des résultats en fonction de vos entrées. Vous disposez de la flexibilité nécessaire pour générer des résultats basés sur un ou plusieurs types de AWS ressources, plans de GuardDuty protectionSource de données de base, Buts de la menace (tactiques) outhe section called "GuardDuty résultats que le script de testeur peut générer".

Utilisez les exemples de commandes suivants comme référence et exécutez une ou plusieurs commandes pour générer les résultats que vous souhaitez explorer :

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Pour plus d'informations sur les paramètres valides, vous pouvez exécuter la commande d'aide suivante :

```
python3 guardduty_tester.py --help
```

Partie C - Conclusions générées par l'examen

Choisissez une méthode préférée pour afficher les résultats générés dans votre compte.

GuardDuty console

1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Dans le tableau des résultats, sélectionnez un résultat dont vous souhaitez consulter les détails. Cela ouvrira le panneau des détails de la recherche. Pour plus d'informations, veuillez consulter Comprendre les GuardDuty résultats d'Amazon.
4. Si vous souhaitez filtrer ces résultats, utilisez la clé et la valeur de la balise de ressource. Par exemple, pour filtrer les résultats générés pour les EC2 instances Amazon, utilisez

`CreatedBy` : `GuardDuty Test Script` tag key:value pair pour la clé de balise d'instance et la clé de balise d'instance.

API

- Exécutez ListFindingspour afficher les résultats d'un identifiant de détecteur spécifique. Vous pouvez définir des paramètres pour filtrer les résultats.

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

AWS CLI

- Exécutez la AWS CLI commande suivante pour afficher les résultats générés et remplacez *us-east-1* and *12abc34d567e8fa901bc2d34EXAMPLE* avec des valeurs appropriées :

  ```
  aws guardduty list-findings --region us-east-1 --detector-
  id 12abc34d567e8fa901bc2d34EXAMPLE
  ```

  Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

  Pour plus d'informations sur les paramètres que vous pouvez utiliser pour filtrer les résultats, consultez list-findings dans la référence des AWS CLI commandes.

Étape 4 - Nettoyer les ressources AWS de test

Les paramètres au niveau du compte et les autres mises à jour de l'état de configuration effectuées lors du Étape 3 - Exécuter des scripts de test retour à l'état d'origine à la fin du script du testeur.

Après avoir exécuté le script du testeur, vous pouvez choisir de nettoyer les ressources de AWS test. Vous pouvez choisir de le faire en utilisant l'une des méthodes suivantes :

- Exécutez la commande suivante :

  ```
  cdk destroy
  ```

- Supprimez la AWS CloudFormation pile portant le nom GuardDutyTesterStack. Pour plus d'informations sur les étapes, voir Supprimer une pile sur la AWS CloudFormation console.

Résolution des problèmes courants

GuardDuty a identifié les problèmes courants et recommande les étapes de résolution des problèmes :

- `Cloud assembly schema version mismatch`— Passez AWS CDK CLI à une version compatible avec la version d'assemblage cloud requise ou à la dernière version disponible. Pour plus d'informations, consultez la section AWS CDK CLICompatibilité.
- `Docker permission denied`— Ajoutez l'utilisateur du compte dédié aux docker-users afin que le compte dédié puisse exécuter les commandes. Pour plus d'informations sur les étapes à suivre, consultez la section Accès Docker refusé.
- `Your requested instance type is not supported in your requested Availability Zone`— Certaines zones de disponibilité ne prennent pas en charge certains types d'instances. Pour identifier les zones de disponibilité compatibles avec votre type d'instance préféré et réessayer de déployer AWS des ressources, effectuez les opérations suivantes :

  1. Choisissez une méthode préférée pour déterminer les zones de disponibilité compatibles avec votre type d'instance :

     Console

     Pour identifier les zones de disponibilité qui prennent en charge le type d'instance préféré

     1. Connectez-vous à la EC2 console Amazon AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
     2. À l'aide du sélecteur de AWS région situé dans le coin supérieur droit de la page, choisissez la région dans laquelle vous souhaitez lancer l'instance.
     3. Dans le volet de navigation, sous Instances, sélectionnez Types d'instances.
     4. Dans le tableau Types d'instances, choisissez un type d'instance préféré.
     5. Sous Mise en réseau, consultez les régions répertoriées sous Zones de disponibilité.

        Sur la base de ces informations, vous devrez peut-être choisir une nouvelle région dans laquelle vous pourrez déployer les ressources.

AWS CLI

Exécutez la commande suivante pour afficher la liste des zones de disponibilité. Assurez-vous de spécifier le type d'instance que vous préférez et la région (*us-east-1*).

```
aws ec2 describe-instance-type-offerings --location-type availability-zone  --
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
output table
```

Pour plus d'informations sur cette commande, consultez describe-instance-type-offeringsla référence des AWS CLI commandes.

Lorsque vous exécutez cette commande, si vous recevez un message d'erreur, assurez-vous que vous utilisez la dernière version de AWS CLI. Pour plus d'informations, consultez Résolution des problèmes dans le Guide de l'utilisateur AWS Command Line Interface .

2. Réessayez de déployer les AWS ressources et spécifiez une zone de disponibilité qui prend en charge votre type d'instance préféré.

   Pour réessayer de déployer des ressources AWS

   1. Configurez la région par défaut dans le `bin/cdk-gd-tester.ts` fichier.
   2. Pour définir la zone de disponibilité, ouvrez le `amazon-guardduty-tester/lib/common/network/vpc.ts` fichier.
   3. Dans ce fichier, remplacez `maxAzs: 2,` par l'`availabilityZones: ['us-east-1a', 'us-east-1c'],`endroit où vous devez spécifier les zones de disponibilité pour votre type d'instance.
   4. Continuez avec les étapes restantes ci-dessousÉtapes de déploiement AWS des ressources.

Niveaux de gravité des GuardDuty résultats

Chaque GuardDuty découverte est associée à un niveau de gravité et à une valeur qui reflètent le risque potentiel que cette découverte pourrait présenter pour votre réseau, tel que déterminé par nos ingénieurs en sécurité. La valeur de la gravité peut être comprise entre 1.0 et 8.9. Plus la valeur est élevée, plus le risque en matière de sécurité est important. Pour vous aider à déterminer la réponse

à apporter à un problème de sécurité potentiel mis en évidence par une constatation, GuardDuty divisez cette plage en niveaux de gravité élevé, moyen et faible.

> **Note**
>
> Les valeurs 0 et de 9.0 à 10.0 sont réservées pour un usage futur.

Voici les niveaux de gravité et les valeurs actuellement définis pour les GuardDuty résultats, ainsi que les recommandations générales pour chacun d'entre eux :

Niveau de gravité	Plage de valeurs
Élevée	7,0 - 8,9
Un niveau de gravité élevé indique que la ressource en question (une EC2 instance ou un ensemble d'informations de connexion IAM utilisateur) est compromise et est activement utilisée à des fins non autorisées. Nous vous recommandons de traiter en priorité tout problème de sécurité lié à un résultat de gravité Élevée et de prendre des mesures de correction immédiates pour empêcher toute utilisati on non autorisée de vos ressources. Par exemple, nettoyez votre EC2 instance, mettez-la hors service ou modifiez les IAM informations d'identification. Pour de plus amples informations, veuillez consulter Étapes de correction.	
Moyenne	4,0 - 6,9
Un niveau de gravité Moyenne indique une activité suspecte qui s'écarte du comportement normalement observé et, selon votre cas d'utilisation, peut indiquer une compromission des ressources. Nous vous recommandons d'examiner la ressource impliquée dans un délai raisonnable. Les étapes de correction varient selon la ressource et la famille du résultat mais en général, il est conseillé de chercher à confirmer que l'activité est autorisée et conforme à votre cas d'utilisation. Si vous ne pouvez pas identifier la cause ou confirmer que l'activité a été autorisée, vous devez considérer la ressource comme compromise et suivre les étapes de correction de manière à sécuriser la ressource.	

Niveau de gravité	Plage de valeurs
Voici quelques éléments à prendre en compte lors de l'examen d'un résultat de niveau de gravité moyen : • Vérifiez si un utilisateur autorisé a installé un nouveau logiciel qui a changé le comportement d'une ressource (par exemple, trafic plus élevé que le trafic normal autorisé ou communication activée sur un nouveau port). • Vérifiez si un utilisateur autorisé a modifié les paramètres du panneau de configuration : par exemple, un paramètre de groupe de sécurité. • Exécutez une analyse antivirus sur les ressources impliquées pour détecter les logiciels non autorisés. • Vérifiez les autorisations associées au IAM rôle, à l'utilisateur, au groupe ou à l'ensemble d'informations d'identification concerné. Celles-ci peuvent avoir été modifiées ou fait l'objet d'une rotation.	
Faible	1,0 - 3,9
Un niveau de gravité faible indique une tentative d'activité suspecte qui n'a pas compromis votre réseau, par exemple une analyse de port ou une tentative d'intrusion qui a échoué. Il n'y a pas d'action immédiate recommandée, mais il est recommandé de prendre note de cette information car elle peut indiquer que quelqu'un recherche des points faibles dans votre réseau.	

Examen des GuardDuty résultats

Suivez la procédure suivante pour examiner et comprendre vos GuardDuty conclusions.

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Choisissez Résultats, puis sélectionnez un résultat spécifique pour afficher ses détails.

   Les détails de chaque résultat varient selon le type de résultat, les ressources concernées et la nature de l'activité. Pour de plus amples informations sur les champs de résultat disponibles, veuillez consulter Détails d'un résultat.
3. (Facultatif) Si vous souhaitez archiver un résultat, sélectionnez-le dans la liste de vos résultats, puis choisissez le menu Actions. Choisissez ensuite Archivage.

Les résultats archivés peuvent être consultés en choisissant Archivé dans la liste déroulante Actuels.

Actuellement, les GuardDuty utilisateurs de comptes GuardDuty membres ne peuvent pas archiver les résultats.

> **Important**
>
> Si vous archivez un résultat manuellement en suivant la procédure qui précède, toutes les occurrences suivantes de ce résultat (générées après l'archivage) sont ajoutées à la liste de vos résultats actuels. Pour ne plus jamais voir ce résultat dans votre liste actuelle, vous pouvez l'archiver automatiquement. Pour de plus amples informations, veuillez consulter Règles de suppression.

4. (Facultatif) Pour télécharger un résultat, sélectionnez-le dans la liste de vos résultats, puis choisissez le menu Actions. Choisissez ensuite Export (Exportation). Lorsque vous exportez un résultat, vous pouvez voir son JSON document complet.

> **Note**
>
> Dans certains cas, GuardDuty prend conscience que certains résultats sont des faux positifs une fois qu'ils ont été générés. GuardDuty fournit un champ de confiance dans le JSON résultat et définit sa valeur à zéro. De cette façon GuardDuty , vous savez que vous pouvez ignorer ces résultats en toute sécurité.

Détails d'un résultat

Dans la GuardDuty console Amazon, vous pouvez consulter les détails des recherches dans la section récapitulative des recherches. Les détails des résultats varient en fonction du type de résultat.

Deux détails principaux permettent de déterminer les types d'information disponibles pour tout résultat. Le premier est le type de ressource, qui peut être `Instance` `AccessKey` `S3Bucket`, `S3` `Object` `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance`, ou `Lambda`. Le deuxième détail qui détermine les informations d'un résultat est le rôle de la ressource. Le rôle de la ressource peut être `Target` pour les clés d'accès, ce qui signifie que la ressource a été la cible d'une activité suspecte. Pour les résultats du type d'instance, le rôle de la ressource peut également

être `Actor`, ce qui signifie que votre ressource était l'acteur à l'origine de l'activité suspecte. Cette rubrique décrit certains des détails les plus fréquemment disponibles en matière de résultats.

Présentation des résultats

La section Présentation d'un résultat contient les fonctionnalités d'identification les plus élémentaires du résultat, notamment les informations suivantes :

- ID du compte : identifiant du AWS compte sur lequel s'est déroulée l'activité qui a incité GuardDuty à générer ce résultat.
- Nombre : nombre de fois qu'une activité correspondant à ce modèle GuardDuty a été agrégée à cet identifiant de recherche.
- Créé à : heure et date de création de ce résultat. Si cette valeur diffère de la valeur Mise à jour à, cela indique que l'activité s'est produite plusieurs fois et qu'il s'agit d'un problème continu.

> **Note**
>
> Les horodatages des résultats dans la GuardDuty console apparaissent dans votre fuseau horaire local, tandis que les JSON exportations et les CLI sorties affichent les horodatages. UTC

- ID de résultat : identifiant unique pour ce type de résultat et ensemble de paramètres. Les nouvelles occurrences d'activité correspondant à ce modèle seront regroupées sous le même ID.
- Type de résultat : chaîne formatée représentant le type d'activité qui a déclenché le résultat. Pour de plus amples informations, veuillez consulter Format de résultat GuardDuty.
- Région : AWS région dans laquelle le résultat a été généré. Pour de plus amples informations sur les régions prises en charge, veuillez consulter Régions et points de terminaison.
- ID de ressource : ID de la AWS ressource par rapport à laquelle a eu lieu l'activité qui a incité GuardDuty à générer ce résultat.
- ID de scan : applicable aux résultats lorsque la protection contre les GuardDuty programmes malveillants EC2 est activée, il s'agit d'un identifiant de l'analyse des programmes malveillants exécutée sur les EBS volumes attachés à l'EC2instance ou à la charge de travail du conteneur potentiellement compromise. Pour de plus amples informations, veuillez consulter Protection contre les logiciels malveillants pour la EC2 recherche de détails.
- Gravité : niveau de gravité attribué à un résultat : Élevée, Moyenne ou Faible. Pour de plus amples informations, veuillez consulter Niveaux de gravité des GuardDuty résultats.

- Mis à jour à — La dernière fois que ce résultat a été mis à jour avec une nouvelle activité correspondant au modèle qui a incité GuardDuty à générer ce résultat.

Ressource

La ressource affectée fournit des détails sur la AWS ressource ciblée par l'activité initiatrice. Les informations disponibles varient selon le type de ressource et le type d'action.

Rôle de ressource : rôle de la AWS ressource à l'origine de la recherche. Cette valeur peut être TARGETou ACTOR, et indique si votre ressource a été la cible de l'activité suspecte ou l'acteur qui a effectué l'activité suspecte.

Type de ressource : type de la ressource affectée. Si plusieurs ressources étaient impliquées, un résultat peut inclure plusieurs types de ressource. Les types de ressources sont Instance AccessKey, S3Bucket, S3Object,, KubernetesClusterECSCluster, RDSDBInstanceContainer et Lambda. Selon le type de ressource, différents détails de résultats sont disponibles. Sélectionnez un onglet d'option de ressource pour en savoir plus sur les détails disponibles pour cette ressource.

Instance

Détails de l'instance :

> **Note**
>
> Certains détails de l'instance peuvent être manquants si l'instance a déjà été arrêtée ou si l'APIappel sous-jacent provient d'une EC2 instance d'une autre région lors d'un appel interrégionalAPI.

- ID d'instance : ID de l'EC2instance impliquée dans l'activité qui a incité GuardDuty à générer le résultat.
- Type d'instance : type de l'EC2instance impliquée dans la recherche.
- Heure de lancement : date et heure auxquelles l'instance a été lancée.
- Outpost ARN — Le nom de la ressource Amazon (ARN) de AWS Outposts. Applicable uniquement aux AWS Outposts instances. Pour plus d'informations, consultez Qu'est-ce que AWS Outposts ?
- Nom du groupe de sécurité : nom du groupe de sécurité attaché à l'instance concernée.
- ID du groupe de sécurité : ID du groupe de sécurité attaché à l'instance concernée.

- État de l'instance : état actuel de l'instance ciblée.
- Zone de disponibilité : zone de disponibilité de la Région AWS dans laquelle se trouve l'instance concernée.
- ID de l'image : ID de l'Amazon Machine Image utilisée pour créer l'instance impliquée dans l'activité.
- Description de l'image : description de l'ID de l'Amazon Machine Image utilisée pour créer l'instance impliquée dans l'activité.
- Balises : liste des balises attachées à cette ressource, répertoriées au format `key:value`.

AccessKey

Détails de la clé d'accès :

- ID de clé d'accès : ID de clé d'accès de l'utilisateur impliqué dans l'activité GuardDuty à l'origine de la recherche.
- ID principal : identifiant principal de l'utilisateur impliqué dans l'activité GuardDuty à l'origine de la recherche.
- Type d'utilisateur : type d'utilisateur impliqué dans l'activité qui a incité GuardDuty à générer le résultat. Pour plus d'informations, voir CloudTrail userIdentity élément.
- Nom d'utilisateur : nom de l'utilisateur impliqué dans l'activité GuardDuty à l'origine de la recherche.

S3Bucket

Détails du compartiment Amazon S3 :

- Nom : nom du compartiment impliqué dans le résultat.
- ARN— Le ARN compartiment impliqué dans la découverte.
- Propriétaire : ID utilisateur canonique de l'utilisateur propriétaire du compartiment impliqué dans le résultat. Pour plus d'informations sur les utilisateurs canoniques, IDs voir les identifiants de AWS compte.
- Type : le type de résultat de compartiment peut être Destination ou Source.
- Détails du chiffrement côté serveur par défaut : détails du chiffrement pour le compartiment.
- Balises de compartiment : liste des balises attachées à cette ressource, répertoriées au format `key:value`.

- Autorisations effectives : évaluation de toutes les autorisations et stratégies effectives sur le compartiment qui indique si le compartiment impliqué est exposé publiquement. Les valeurs peuvent être Publique ou Non publique.

S3Object

- Détails de l'objet S3 : inclut les informations suivantes sur l'objet S3 scanné :
  - ARN— Amazon Resource Name (ARN) de l'objet S3 scanné.
  - Clé : nom attribué au fichier lors de sa création dans le compartiment S3.
  - ID de version : lorsque vous avez activé le contrôle de version des compartiments, ce champ indique l'identifiant de version associé à la dernière version de l'objet S3 scanné. Pour plus d'informations, consultez la section Utilisation du versionnement dans les compartiments S3 dans le guide de l'utilisateur Amazon S3.
  - eTag— Représente la version spécifique de l'objet S3 scanné.
  - Hachage : hachage de la menace détectée dans cette constatation.
- Détails du compartiment S3 : inclut les informations suivantes sur le compartiment Amazon S3 associé à l'objet S3 scanné :
  - Nom — Indique le nom du compartiment S3 qui contient l'objet.
  - ARN— Amazon Resource Name (ARN) du compartiment S3.
- Propriétaire : identifiant canonique du propriétaire du compartiment S3.

EKSCluster

Détails du cluster Kubernetes :

- Nom : nom du cluster Kubernetes.
- ARN— Celui ARN qui identifie le cluster.
- Créé à : heure et date de création de ce cluster.

> **Note**
>
> Les horodatages des résultats dans la GuardDuty console apparaissent dans votre fuseau horaire local, tandis que les JSON exportations et les CLI sorties affichent les horodatages. UTC

- VPCID — L'ID du VPC qui est associé à votre cluster.
- État : extrait l'état actuel du cluster.
- Balises : métadonnées que vous appliquez au cluster pour faciliter le classement et l'organisation. Chaque balise est constituée d'une clé et d'une valeur facultative, répertoriées au format `key:value`. Vous pouvez définir à la fois la clé et la valeur.

  Les balises de cluster ne sont pas propagées vers les autres ressources associées au cluster.

Détails de la charge de travail Kubernetes :

- Type : type de charge de travail Kubernetes, tel que le pod, le déploiement et la tâche.
- Nom : nom de la charge de travail Kubernetes.
- Uid : identifiant unique de la charge de travail Kubernetes.
- Créé à : heure et date de création de cette charge de travail.
- Étiquettes : paires clé-valeur attachées à la charge de travail Kubernetes.
- Conteneurs : détails du conteneur exécuté dans le cadre de la charge de travail de Kubernetes.
- Espace de noms : la charge de travail appartient à cet espace de noms Kubernetes.
- Volumes : volumes utilisés par la charge de travail Kubernetes.
  - Chemin d'accès de l'hôte : représente un fichier ou un répertoire préexistant sur la machine hôte vers lequel le volume est mappé.
  - Nom : nom du volume.
- Contexte de sécurité du pod : définit les paramètres de contrôle des privilèges et des accès pour tous les conteneurs d'un pod.
- Réseau hôte : définissez sur `true` si les pods sont inclus dans la charge de travail Kubernetes.

Informations utilisateur Kubernetes :

- Groupes : groupes Kubernetes RBAC (contrôle basé sur l'accès aux rôles) de l'utilisateur impliqué dans l'activité qui a généré le résultat.
- ID : ID unique de l'utilisateur Kubernetes.
- Nom d'utilisateur : nom de l'utilisateur Kubernetes qui participe à l'activité à l'origine du résultat.
- Nom de session : entité qui a assumé le IAM rôle avec les autorisations KubernetesRBAC.

ECSCluster

ECSdétails du cluster :

- ARN— Celui ARN qui identifie le cluster.
- Nom : nom du cluster.
- État : extrait l'état actuel du cluster.
- Nombre de services actifs : nombre de services exécutés sur le cluster à l'état `ACTIVE`. Vous pouvez consulter ces services avec ListServices
- Nombre d'instances de conteneur enregistrées : nombre d'instances de conteneur enregistrées dans le cluster. Cela inclut les instances de conteneur à la fois à l'état `ACTIVE` et `DRAINING`.
- Nombre de tâches en cours : nombre de tâches du cluster qui sont à l'état `RUNNING`.
- Balises : métadonnées que vous appliquez au cluster pour faciliter le classement et l'organisation. Chaque balise est constituée d'une clé et d'une valeur facultative, répertoriées au format `key:value`. Vous pouvez définir à la fois la clé et la valeur.
- Conteneurs : détails sur le conteneur associé à la tâche :
  - Nom de conteneur : nom du conteneur.
  - Image de conteneur : image du conteneur.
- Détails de la tâche : détails d'une tâche dans un cluster.
  - ARN— Le nom de la ressource Amazon (ARN) de la tâche.
  - Définition ARN : nom de ressource Amazon (ARN) de la définition de tâche qui crée la tâche.
  - Version : compteur de version de la tâche.
  - Tâche créée à : horodatage Unix lors de la création de la tâche.
  - Tâche démarrée à : horodatage Unix lors du démarrage d'une tâche.
  - Tâche démarrée par : balise spécifiée lors du démarrage d'une tâche.

Container

Détails du conteneur :

- Exécution du conteneur : exécution du conteneur (comme `docker` ou `containerd`) utilisé pour exécuter le conteneur.
- ID — L'ID de l'instance de conteneur ou ARN les entrées complètes de l'instance de conteneur.
- Nom : nom du conteneur.

Lorsqu'il est disponible, ce champ affiche la valeur de l'étiquette `io.kubenetes.container.name`.

- Image : image de l'instance de conteneur.
- Montages de volume : liste des montages de volume de conteneurs. Un conteneur peut monter un volume sous son système de fichiers.
- Contexte de sécurité : le contexte de sécurité du conteneur définit les paramètres de contrôle de privilèges et d'accès pour un conteneur.
- Détails du processus : décrit les détails du processus associé au résultat.

RDSDBInstance

RDSDBInstancedétails :

> **Note**
>
> Cette ressource est disponible dans les résultats de RDS protection relatifs à l'instance de base de données.

- ID de l'instance de base de données : identifiant associé à l'instance de base de données impliquée dans la GuardDuty recherche.
- Moteur : nom du moteur de base de données de l'instance de base de données impliquée dans le résultat. Les valeurs possibles sont Aurora My SQL -Compatible ou Aurora Postgre SQL - Compatible.
- Version du moteur : version du moteur de base de données impliquée dans la GuardDuty recherche.
- ID du cluster de base de données : identifiant du cluster de base de données qui contient l'identifiant de l'instance de base de données impliquée dans la GuardDuty recherche.
- Instance de base de données ARN : ARN qui identifie l'instance de base de données impliquée dans la GuardDuty recherche.

Lambda

Détails de la fonction Lambda

- Nom de la fonction : nom de la fonction Lambda impliquée dans le résultat.
- Version de la fonction : version de la fonction Lambda impliquée dans le résultat.
- Description de la fonction : description de la fonction Lambda impliquée dans le résultat.
- Function ARN : nom de ressource Amazon (ARN) de la fonction Lambda impliquée dans la recherche.
- ID de révision : ID de révision de la version de la fonction Lambda.
- Rôle : rôle d'exécution de la fonction Lambda impliquée dans le résultat.
- VPCconfiguration — La VPC configuration Amazon, y compris l'VPCID, le groupe de sécurité et le sous-réseau IDs associés à votre fonction Lambda.
- VPCID : ID de l'Amazon VPC associé à la fonction Lambda impliquée dans la recherche.
- Sous-réseau IDs : ID des sous-réseaux associés à votre fonction Lambda.
- Groupe de sécurité : groupe de sécurité attaché à la fonction Lambda concernée. Cela inclut le nom et l'ID du groupe de sécurité.
- Balises : liste des balises attachées à cette ressource, répertoriées au format de paire `key:value`.

RDSdétails de l'utilisateur de la base de données (DB)

> **Note**
>
> Cette section s'applique aux résultats obtenus lorsque vous activez la fonctionnalité de RDS protection dans GuardDuty. Pour de plus amples informations, veuillez consulter GuardDuty RDSProtection.

La GuardDuty découverte fournit les informations suivantes relatives à l'utilisateur et à l'authentification de la base de données potentiellement compromise.

- Utilisateur : nom d'utilisateur utilisé pour effectuer la tentative de connexion anormale.
- Application : nom de l'application servant à effectuer la tentative de connexion anormale.

- Base de données : nom de l'instance de base de données impliquée dans la tentative de connexion anormale.
- SSL— Version du protocole Secure Socket Layer (SSL) utilisée pour le réseau.
- Méthode d'authentification : méthode d'authentification utilisée par l'utilisateur impliqué dans le résultat.

Surveillance du temps d'exécution : recherche de détails

> **Note**
>
> Ces informations ne peuvent être disponibles que GuardDuty si l'un desTypes de recherche liés à la surveillance du temps.

Cette section contient les détails de l'exécution, tels que les détails du processus et tout contexte requis. Les détails du processus décrivent les informations relatives au processus observé et le contexte d'exécution décrit toute information supplémentaire concernant l'activité potentiellement suspecte.

Détails du processus

- Nom : nom du processus.
- Chemin exécutable : chemin absolu du fichier exécutable du processus.
- Executable SHA -256 — Le `SHA256` hachage de l'exécutable du processus.
- Espace de noms PID : ID de processus du processus dans un espace de PID noms secondaire autre que l'espace de noms au niveau PID de l'hôte. Pour les processus se trouvant à l'intérieur d'un conteneur, il s'agit de l'ID de processus observé à l'intérieur du conteneur.
- Répertoire de travail actuel : répertoire de travail actuel du processus.
- ID de processus : ID attribué au processus par le système d'exploitation.
- startTime— Heure à laquelle le processus a commencé. Ceci est au format UTC de chaîne de date (`2023-03-22T19:37:20.168Z`).
- UUID— L'identifiant unique attribué au processus par GuardDuty.
- Parent UUID : ID unique du processus parent. Cet identifiant est attribué au processus parent par GuardDuty.
- Utilisateur : utilisateur qui a exécuté le processus.

- ID utilisateur : ID de l'utilisateur qui a exécuté le processus.
- ID utilisateur effectif : ID de l'utilisateur effectif du processus au moment de l'événement.
- Lignée : informations sur les ancêtres du processus.
  - ID de processus : ID attribué au processus par le système d'exploitation.
  - UUID— L'identifiant unique attribué au processus par GuardDuty.
  - Chemin exécutable : chemin absolu du fichier exécutable du processus.
  - ID utilisateur effectif : ID de l'utilisateur effectif du processus au moment de l'événement.
  - Parent UUID : ID unique du processus parent. Cet identifiant est attribué au processus parent par GuardDuty.
  - Heure de début : heure à laquelle le processus a démarré.
  - Espace de noms PID : ID de processus du processus dans un espace de PID noms secondaire autre que l'espace de noms au niveau PID de l'hôte. Pour les processus se trouvant à l'intérieur d'un conteneur, il s'agit de l'ID de processus observé à l'intérieur du conteneur.
  - ID utilisateur : ID de l'utilisateur qui a exécuté le processus.
  - Nom : nom du processus.

Contexte d'exécution

Parmi les champs suivants, un résultat généré peut inclure uniquement les champs correspondant au type de résultat.

- Source de montage : chemin sur l'hôte monté par le conteneur.
- Cible de montage : chemin du conteneur mappé au répertoire hôte.
- Type de système de fichiers : représente le type du système de fichiers monté.
- Indicateurs : représente les options qui contrôlent le comportement de l'événement impliqué dans ce résultat.
- Processus de modification : informations sur le processus qui a créé ou modifié un fichier binaire, un script ou une bibliothèque dans un conteneur lors de l'exécution.
- Modifié à : horodatage auquel le processus a créé ou modifié un binaire, un script ou une bibliothèque dans un conteneur au moment de l'exécution. Ce champ est au format de chaîne de UTC date (`2023-03-22T19:37:20.168Z`).
- Chemin de la bibliothèque : chemin d'accès à la nouvelle bibliothèque chargée.
- Valeur de préchargement LD : valeur de la variable d'environnement `LD_PRELOAD`.

- Chemin du socket : chemin d'accès au socket Docker auquel l'utilisateur a accédé.
- Chemin d'accès au binaire Runc : chemin d'accès au binaire `runc`.
- Chemin d'accès à l'agent de version : chemin d'accès au fichier de l'agent de version `cgroup`.
- Exemple de ligne de commande : exemple de ligne de commande impliquée dans l'activité potentiellement suspecte.
- Catégorie d'outil : catégorie à laquelle appartient l'outil. Voici quelques exemples : Backdoor Tool, Pentest Tool, Network Scanner et Network Sniffer.
- Nom de l'outil : nom de l'outil potentiellement suspect.
- Chemin du script : chemin d'accès au script exécuté qui a généré le résultat.
- Chemin du fichier de menaces : chemin suspect pour lequel les informations relatives aux menaces ont été trouvées.
- Nom du service : nom du service de sécurité qui a été désactivé.

EBSdétails de l'analyse des volumes

> **Note**
>
> Cette section s'applique aux résultats obtenus lorsque vous activez l'analyse des programmes malveillants GuardDuty initiée. Protection contre les logiciels malveillants pour EC2

L'analyse EBS des volumes fournit des détails sur le EBS volume attaché à l'EC2instance ou à la charge de travail du conteneur potentiellement compromise.

- ID de numérisation : identifiant de l'analyse des logiciels malveillants.
- Analyse démarrée à : date et heure du début de l'analyse des logiciels malveillants.
- Analyse terminée à : date et heure de fin de l'analyse des logiciels malveillants.
- ID de recherche du déclencheur : ID de recherche du GuardDuty résultat à l'origine de cette analyse des logiciels malveillants.
- Sources — Les valeurs potentielles sont `Bitdefender` et`Amazon`.
- Détections d'analyse : vue complète des détails et des résultats de chaque analyse des logiciels malveillants.

- Nombre d'éléments analysés : nombre total de fichiers numérisés. Fournit des détails tels que `totalGb`, `files` et `volumes`.
- Nombre d'éléments de menaces détectées : nombre total de `files` malveillants détectés lors de l'analyse.
- Informations sur les menaces les plus graves : informations sur la menace la plus grave détectée lors de l'analyse et sur le nombre de fichiers malveillants. Fournit des détails tels que `severity`, `threatName` et `count`.
- Menaces détectées par nom : élément du conteneur regroupant les menaces de tous niveaux de gravité. Fournit des détails tels que `itemCount`, `uniqueThreatNameCount`, `shortened` et `threatNames`.

Protection contre les logiciels malveillants pour la EC2 recherche de détails

> **Note**
>
> Cette section s'applique aux résultats obtenus lorsque vous activez l'analyse des programmes malveillants GuardDuty initiée. Protection contre les logiciels malveillants pour EC2

Lorsque la protection contre les programmes EC2 malveillants pour l'analyse détecte un logiciel malveillant, vous pouvez consulter les détails de l'analyse en sélectionnant le résultat correspondant sur la page Résultats de la https://console.aws.amazon.com/guardduty/console. La sévérité de votre protection contre les EC2 programmes malveillants dépend de la gravité de la GuardDuty détection.

> **Note**
>
> La balise `GuardDutyFindingDetected` indique que les instantanés contiennent des logiciels malveillants.

Les informations suivantes sont disponibles dans la section Menaces détectées du panneau de détails.

- Nom : nom de la menace, obtenu en groupant les fichiers par détection.
- Gravité : gravité de la menace détectée.

- Hash — Le SHA -256 du fichier.
- Chemin du fichier : emplacement du fichier malveillant dans le EBS volume.
- Nom du fichier : nom du fichier dans lequel la menace a été détectée.
- Volume ARN : le nombre ARN de EBS volumes numérisés.

Les informations suivantes sont disponibles dans la section Détails de l'analyse des logiciels malveillants du panneau des détails.

- ID de numérisation : ID de numérisation des logiciels malveillants.
- Analyse démarrée à : date et heure du début de l'analyse.
- Analyse terminée à : date et heure de fin de l'analyse.
- Fichiers analysés : nombre total de fichiers et de répertoires numérisés.
- Nombre total de Go numérisés : quantité de stockage analysée au cours du processus.
- ID de recherche du déclencheur : ID de recherche du GuardDuty résultat à l'origine de cette analyse des logiciels malveillants.
- Les informations suivantes sont disponibles dans la section Détails de volume du panneau des détails.
  - Volume ARN : nom de ressource Amazon (ARN) du volume.
  - Instantané ARN : ARN de l'instantané du EBS volume.
  - État : état de l'analyse du volume, tel que `Running`, `Skipped` et `Completed`.
  - Type de chiffrement : type de chiffrement utilisé pour chiffrer le volume. Par exemple, `CMCMK`.
  - Nom de l'appareil : nom de l'appareil. Par exemple, `/dev/xvda`.

Protection contre les logiciels malveillants pour S3 : recherche de détails

Les informations suivantes relatives à l'analyse des programmes malveillants sont disponibles lorsque vous activez à la fois GuardDuty la protection contre les programmes malveillants pour S3 dans votre Compte AWS :

- Menaces : liste des menaces détectées lors de l'analyse des logiciels malveillants.

  Pour plus d'informations sur le nombre de menaces que la découverte peut inclure, consultezQuotas dans la protection contre les malwares pour S3.

- Chemin de l'élément : liste des chemins d'éléments imbriqués et des détails de hachage de l'objet S3 scanné.
  - Chemin de l'élément imbriqué : chemin de l'élément de l'objet S3 scanné où la menace a été détectée.

    La valeur de ce champ n'est disponible que si l'objet de niveau supérieur est une archive et si une menace est détectée dans une archive.
  - Hachage : hachage de la menace détectée dans cette constatation.
- Sources — Les valeurs potentielles sont `Bitdefender` et`Amazon`.

Action

L'action d'un résultat donne des détails sur le type d'activité qui a déclenché le résultat. Les informations disponibles varient selon le type d'action.

Type d'action : type d'activité du résultat. Cette valeur peut être NETWORK_ CONNECTION, PORT_ PROBE, DNS_ REQUESTCALL, AWSAPI_ _ ou RDS_ LOGIN _ ATTEMPT. Les informations disponibles varient selon le type d'action :

- NETWORK_ CONNECTION — Indique que le trafic réseau a été échangé entre l'EC2instance identifiée et l'hôte distant. Ce type d'action contient les informations supplémentaires suivantes :
  - Direction de connexion : direction de connexion réseau observée dans l'activité qui a incité GuardDuty à générer le résultat. Il peut s'agir de l'une des valeurs suivantes :
    - INBOUND— Indique qu'un hôte distant a établi une connexion à un port local sur l'EC2instance identifiée dans votre compte.
    - OUTBOUND— Indique que l'EC2instance identifiée a établi une connexion avec un hôte distant.
    - UNKNOWN— Indique qu'il n' GuardDuty a pas été possible de déterminer le sens de la connexion.
  - Protocole : protocole de connexion réseau observé dans l'activité qui a incité GuardDuty à générer le résultat.
  - IP locale : adresse IP source d'origine du trafic ayant déclenché le résultat. Cette information permet de faire la distinction entre l'adresse IP d'une couche intermédiaire via laquelle les flux transitent et l'adresse IP source d'origine du trafic qui a déclenché la recherche. Par exemple, l'adresse IP d'un EKS pod par opposition à l'adresse IP de l'instance sur laquelle le EKS pod est exécuté.

  - Bloqué : indique si le port cible est bloqué.
- PORT_ PROBE — Indique qu'un hôte distant a sondé l'EC2instance identifiée sur plusieurs ports ouverts. Ce type d'action contient les informations supplémentaires suivantes :
  - IP locale : adresse IP source d'origine du trafic ayant déclenché le résultat. Cette information permet de faire la distinction entre l'adresse IP d'une couche intermédiaire via laquelle les flux transitent et l'adresse IP source d'origine du trafic qui a déclenché la recherche. Par exemple, l'adresse IP d'un EKS pod par opposition à l'adresse IP de l'instance sur laquelle le EKS pod est exécuté.
  - Bloqué : indique si le port cible est bloqué.
- DNS_ REQUEST — Indique que l'EC2instance identifiée a demandé un nom de domaine. Ce type d'action contient les informations supplémentaires suivantes :
  - Protocole : protocole de connexion réseau observé dans l'activité qui a incité GuardDuty à générer le résultat.
  - Bloqué : indique si le port cible est bloqué.
- AWS_ API _ CALL — Indique qu'un AWS API a été invoqué. Ce type d'action contient les informations supplémentaires suivantes :
  - API— Nom de l'APIopération qui a été invoquée et donc invitée GuardDuty à générer ce résultat.

    > **Note**
    >
    > Ces opérations peuvent également inclure des API événements non capturés par AWS CloudTrail. Pour plus d'informations, consultez la section APIÉvénements non capturés par CloudTrail.

  - Agent utilisateur : agent utilisateur à l'origine de la API demande. Cette valeur vous indique si l'appel a été effectué depuis le AWS Management Console, un AWS service, le AWS SDKs, ou le AWS CLI.
  - ERRORCODE— Si la recherche a été déclenchée par un échec d'APIappel, le code d'erreur correspondant à cet appel s'affiche.
  - Nom du service : DNS nom du service qui a tenté de passer l'APIappel qui a déclenché la recherche.
- RDS_ LOGIN _ ATTEMPT — Indique qu'une tentative de connexion à la base de données potentiellement compromise a été effectuée à partir d'une adresse IP distante.

- Adresse IP : adresse IP distante utilisée pour effectuer la tentative de connexion potentiellement suspecte.

Acteur ou cible

Un résultat a une section Acteur si le rôle de la ressource était `TARGET`. Cela indique que votre ressource a été ciblée par une activité suspecte, et la section Acteur contient des détails sur l'entité qui a ciblé votre ressource.

Un résultat a une section Cible si le rôle de la ressource était `ACTOR`. Cela indique que votre ressource a été impliquée dans une activité suspecte contre un hôte distant, et cette section contiendra des informations sur l'IP ou le domaine ciblé par votre ressource.

Les informations disponibles dans la section Acteur ou Cible peuvent inclure les éléments suivants :

- Affilié — Informations indiquant si le AWS compte de l'APIappelant distant est lié à votre GuardDuty environnement. Si cette valeur est la même`true`, l'APIappelant est affilié à votre compte d'une manière ou d'une autre ; si `false` l'APIappelant ne provient pas de votre environnement.
- ID de compte distant : ID de compte propriétaire de l'adresse IP sortante utilisée pour accéder à la ressource sur le réseau final.
- Adresse IP : adresse IP impliquée dans l'activité GuardDuty à l'origine de la recherche.
- Emplacement : informations de localisation de l'adresse IP impliquée dans l'activité GuardDuty à l'origine de la recherche.
- ISPOrganisation : informations relatives à l'organisation concernant l'adresse IP impliquée dans l'activité GuardDuty à l'origine du résultat.
- Port : numéro de port impliqué dans l'activité GuardDuty à l'origine de la recherche.
- Domaine : domaine impliqué dans l'activité qui a incité GuardDuty à générer le résultat.
- Domaine avec suffixe : domaine de deuxième et de premier niveau impliqué dans une activité susceptible d'inciter GuardDuty à générer le résultat. Pour obtenir la liste des domaines de premier et de deuxième niveau, consultez la liste des suffixes publics.

Informations supplémentaires

Tous les résultats ont une section Informations supplémentaires incluant les informations suivantes :

- Nom de la liste de menaces : nom de la liste de menaces qui inclut l'adresse IP ou le nom de domaine impliqué dans l'activité GuardDuty à l'origine de la découverte.
- Exemple : une valeur vraie ou fausse qui indique s'il s'agit d'un exemple de résultat.
- Archivé : une valeur vraie ou fausse qui indique si ce résultat a été archivé.
- Inhabituelle : détails d'une activité qui n'a pas été observée historiquement. Il peut s'agir d'un utilisateur inhabituel (non observé auparavant), d'un lieu, d'une heure, d'un compartiment, d'un comportement de connexion ou d'une ASN organisation.
- Protocole inhabituel : protocole de connexion réseau impliqué dans l'activité GuardDuty à l'origine du résultat.
- Informations sur l'agent : informations sur l'agent de sécurité actuellement déployé sur le EKS cluster de votre Compte AWS. Cela ne s'applique qu'aux types de recherche de EKS Runtime Monitoring.
  - Version de l'agent : version de l'agent GuardDuty de sécurité.
  - ID de l'agent : identifiant unique de l'agent GuardDuty de sécurité.

Preuve

Les résultats basés sur les renseignements sur les menaces comportent une section Preuve qui comprend les informations suivantes :

- Informations détaillées sur les menaces : nom de la liste des menaces sur laquelle `Threat name` figure la menace reconnue.
- Nom de la menace : nom de la famille de logiciels malveillants ou autre identifiant associé à la menace.
- Fichier de menace SHA256 : SHA256 du fichier à l'origine de la découverte.

Comportement anormal

Les types de résultats qui se terminent par AnomalousBehaviorindiquent que le résultat a été généré par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle ML évalue toutes les API demandes adressées à votre compte et identifie les événements anormaux associés aux tactiques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et les API informations spécifiques demandées.

Vous trouverez des détails sur les facteurs de la API demande qui sont inhabituels pour l'identité de l' CloudTrail utilisateur qui a invoqué la demande dans les détails de la recherche. Les identités sont définies par l' CloudTrail userIdentity élément, et les valeurs possibles sont les suivantes : `Root` `IAMUserAssumedRole`,`FederatedUser`,`AWSAccount`, ou`AWSService`.

Outre les détails disponibles pour tous les GuardDuty résultats associés à API l'activité, les AnomalousBehaviorrésultats comportent des détails supplémentaires qui sont décrits dans la section suivante. Ces détails peuvent être consultés dans la console et sont également disponibles dans les résultatsJSON.

- Anormal APIs : liste de API demandes invoquées par l'identité de l'utilisateur à proximité de la API demande principale associée à la recherche. Ce volet détaille plus en détail l'APIévénement de la manière suivante.
  - La première API liste est la principaleAPI, c'est-à-dire la API demande associée à l'activité observée présentant le plus haut risque. C'est ce API qui a déclenché la découverte et qui est en corrélation avec la phase d'attaque du type de découverte. C'est également ce API qui est détaillé dans la section Action de la console et dans les résultatsJSON.
  - Toutes les autres anomalies APIs répertoriées sont APIs des anomalies supplémentaires par rapport à l'identité utilisateur répertoriée observée à proximité du principalAPI. S'il n'y en a qu'une API sur la liste, le modèle ML n'a identifié aucune API demande supplémentaire provenant de cette identité d'utilisateur comme anormale.
  - La liste des APIs est divisée en fonction du fait qu'un API a été appelé avec succès ou s'il API a été appelé sans succès, ce qui signifie qu'une réponse d'erreur a été reçue. Le type de réponse d'erreur reçue est indiqué au-dessus de chaque appel API non réussi. Les types de réponse d'erreur possibles sont les suivants : `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` et `operation not permitted`.
  - APIssont classés en fonction du service qui leur est associé.
  - Pour plus de contexte, choisissez Historique APIs pour afficher les informations relatives au sommetAPIs, jusqu'à un maximum de 20, généralement visibles à la fois pour l'identité de l'utilisateur et pour tous les utilisateurs du compte. Ils APIs sont marqués comme rares (moins d'une fois par mois), peu fréquents (quelques fois par mois) ou fréquents (tous les jours ou toutes les semaines), selon la fréquence à laquelle ils sont utilisés dans votre compte.
- Comportement inhabituel (compte) : cette section fournit des informations supplémentaires sur le comportement profilé de votre compte.

> **Comportement profilé**
>
> GuardDuty se renseigne en permanence sur les activités de votre compte en fonction des événements survenus. Ces activités et leur fréquence observée sont connues sous le nom de comportement profilé.

Les informations suivies dans ce panneau incluent :

- ASNOrg — L'ASNorganisation à partir de laquelle l'APIappel anormal a été passé.
- Nom d'utilisateur : nom de l'utilisateur qui a effectué l'APIappel anormal.
- Agent utilisateur : agent utilisateur utilisé pour effectuer l'APIappel anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
- Type d'utilisateur : type d'utilisateur à l'origine de l'APIappel anormal. Les valeurs possibles sont `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.
- Compartiment : nom du compartiment S3 auquel on a accédé.

- Comportement inhabituel (identité de l'utilisateur) : cette section fournit des détails supplémentaires sur le comportement profilé de l'identité de l'utilisateur impliqué dans le résultat. Lorsqu'un comportement n'est pas identifié comme historique, cela signifie que le modèle GuardDuty ML n'a jamais vu l'identité de cet utilisateur effectuer cet API appel de cette manière au cours de la période de formation. Les informations supplémentaires suivantes concernant l'identité de l'utilisateur sont disponibles :
  - ASNOrg — L'ASNorganisation à partir de laquelle l'APIappel anormal a été passé.
  - Agent utilisateur : agent utilisateur utilisé pour effectuer l'APIappel anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
  - Compartiment : nom du compartiment S3 auquel on a accédé.
- Comportement inhabituel (compartiment) : cette section fournit des informations supplémentaires sur le comportement profilé du compartiment S3 associé au résultat. Lorsqu'un comportement n'est pas identifié comme historique, cela signifie que le modèle GuardDuty ML n'a jamais vu d'APIappels passés à ce compartiment de cette manière au cours de la période de formation. Les informations suivies dans cette section incluent :
  - ASNOrg — L'ASNorganisation à partir de laquelle l'APIappel anormal a été passé.
  - Nom d'utilisateur : nom de l'utilisateur qui a effectué l'APIappel anormal.

- Agent utilisateur : agent utilisateur utilisé pour effectuer l'APIappel anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
- Type d'utilisateur : type d'utilisateur à l'origine de l'APIappel anormal. Les valeurs possibles sont `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.

> **Note**
>
> Pour plus de détails sur les comportements historiques, choisissez Comportement historique dans la section Comportement inhabituel (compte), ID utilisateur ou Compartiment pour afficher les détails du comportement attendu dans votre compte pour chacune des catégories suivantes : Rare (moins d'une fois par mois), Peu fréquent (quelques fois par mois) ou Fréquent (quotidien ou hebdomadaire), selon la fréquence à laquelle ils sont utilisés dans votre compte.

- Comportement inhabituel (base de données) : cette section fournit des informations supplémentaires sur le comportement profilé de l'instance de base de données associée au résultat. Lorsqu'un comportement n'est pas identifié comme historique, cela signifie que le modèle GuardDuty ML n'a jamais connu de tentative de connexion de cette manière à cette instance de base de données au cours de la période de formation. Les informations suivies pour cette section dans le panneau de résultat incluent :
  - Nom d'utilisateur : nom d'utilisateur utilisé pour effectuer la tentative de connexion anormale.
  - ASNOrg — L'ASNorganisation à partir de laquelle la tentative de connexion anormale a été effectuée.
  - Nom de l'application : nom de l'application servant à effectuer la tentative de connexion anormale.
  - Nom de la base de données : nom de l'instance de base de données impliquée dans la tentative de connexion anormale.

  La section Comportement historique fournit plus de contexte sur les noms d'utilisateur, les ASNorganisations, les noms d'applications et les noms de base de données précédemment observés pour la base de données associée. Chaque valeur unique est associée à un nombre représentant le nombre de fois qu'elle a été observée lors d'un événement de connexion qui a abouti.
- Comportement inhabituel (cluster Kubernetes de compte, espace de noms Kubernetes et nom d'utilisateur Kubernetes) : cette section fournit des informations supplémentaires sur le comportement profilé du cluster Kubernetes et de l'espace de noms associé au résultat. Lorsqu'un

comportement n'est pas identifié comme historique, cela signifie que le modèle GuardDuty ML n'a pas précédemment observé ce compte, ce cluster, cet espace de noms ou ce nom d'utilisateur de cette manière. Les informations suivies pour cette section dans le panneau de résultat incluent :

- Nom d'utilisateur : utilisateur qui a appelé le Kubernetes API associé à la recherche.
- Nom d'utilisateur usurpé : l'utilisateur usurpé par `username`.
- Namespace : espace de noms Kubernetes au sein du cluster EKS Amazon où l'action s'est produite.
- Agent utilisateur : agent utilisateur associé à l'appel KubernetesAPI. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `kubectl`.
- API— Les Kubernetes API appelés par `username` le cluster Amazon. EKS
- ASNInformations — Les ASN informations, telles que l'organisation etISP, associées à l'adresse IP de l'utilisateur effectuant cet appel.
- Jour de la semaine : jour de la semaine où l'APIappel Kubernetes a été effectué.
- Autorisation — L'accès au verbe et à la ressource Kubernetes est vérifié pour indiquer s'ils `username` peuvent ou non utiliser Kubernetes. API
- Nom du compte de service : compte de service associé à la charge de travail Kubernetes qui fournit une identité à la charge de travail.
- Registre : registre de conteneurs associé à l'image de conteneur déployée dans le workload Kubernetes.
- Image : image du conteneur, sans les balises ni le résumé associés, déployée dans le workload Kubernetes.
- Config du préfixe d'image : préfixe d'image pour lequel la configuration de sécurité du conteneur et de la charge de travail est activée`privileged`, par exemple `hostNetwork` ou pour le conteneur utilisant l'image.
- Nom du sujet — Les sujets, tels que a `usergroup`, ou `serviceAccountName` qui sont liés à un rôle de référence dans un `RoleBinding` ou`ClusterRoleBinding`.
- Nom du rôle : nom du rôle impliqué dans la création ou la modification des rôles ou du `roleBinding`API.

Anomalies basées sur le volume S3

Cette section détaille les informations contextuelles relatives aux anomalies basées sur le volume S3. La fonction de recherche basée sur le volume (Exfiltration:S3/AnomalousBehavior) surveille le nombre inhabituel d'APIappels S3 effectués par les utilisateurs vers les compartiments S3, ce

qui indique une exfiltration potentielle de données. Les API appels S3 suivants sont surveillés pour détecter les anomalies en fonction du volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Les métriques suivantes aideront à établir une base de référence du comportement habituel lorsqu'une IAM entité accède à un compartiment S3. Pour détecter l'exfiltration de données, le résultat de détection d'anomalies basées sur le volume évalue toutes les activités par rapport à la référence comportementale habituelle. Choisissez Comportement historique dans les sections Comportement inhabituel (identité utilisateur), Volume observé (identité utilisateur) et Volume observé (compartiment) pour afficher les métriques suivantes, respectivement.

- Nombre d'`s3-api-name`APIappels appelés par l'IAMutilisateur ou le IAM rôle (dépend de celui qui a été émis) associés au compartiment S3 concerné au cours des dernières 24 heures.
- Nombre d'`s3-api-name`APIappels appelés par l'IAMutilisateur ou le IAM rôle (dépend de celui qui a été émis) associés à tous les compartiments S3 au cours des dernières 24 heures.
- Nombre d'`s3-api-name`APIappels concernant tous les IAM utilisateurs ou IAM rôles (en fonction de celui qui a été émis) associés au compartiment S3 concerné au cours des dernières 24 heures.

RDSanomalies liées à l'activité de connexion

Cette section détaille le nombre de tentatives de connexion effectuées par l'acteur inhabituel et est regroupée en fonction du résultat des tentatives de connexion. Les Types de résultat de la protection RDS identifient les comportements anormaux en surveillant les événements de connexion pour détecter les modèles inhabituels de `successfulLoginCount`, `failedLoginCount` et `incompleteConnectionCount`.

- successfulLoginCount— Ce compteur représente la somme des connexions réussies (combinaison correcte d'attributs de connexion) établies avec l'instance de base de données par l'acteur inhabituel. Les attributs de connexion incluent le nom d'utilisateur, le mot de passe et le nom de la base de données.
- failedLoginCount— Ce compteur représente la somme des tentatives de connexion échouées (infructueuses) effectuées pour établir une connexion à l'instance de base de données. Il indique

qu'un ou plusieurs attributs de la combinaison de connexion, tels que le nom d'utilisateur, le mot de passe ou le nom de base de données, étaient incorrects.

- incompleteConnectionCount— Ce compteur représente le nombre de tentatives de connexion qui ne peuvent être classées comme réussies ou échouées. Ces connexions sont fermées avant que la base de données ne fournisse une réponse. Par exemple, l'analyse des ports lorsque le port de base de données est connecté, mais qu'aucune information n'est envoyée à la base de données, ou lorsque la connexion a été interrompue avant la fin de la connexion lors d'une tentative réussie ou infructueuse.

GuardDuty recherche d'une agrégation

Tous les résultats sont dynamiques, ce qui signifie que si une nouvelle activité liée au même problème de sécurité est GuardDuty détectée, le résultat initial sera mis à jour avec les nouvelles informations, au lieu de générer un nouveau résultat. Ce comportement vous permet d'identifier les problèmes en cours sans avoir à consulter plusieurs rapports similaires. Il réduit également le bruit global lié aux problèmes de sécurité que vous connaissez déjà.

Par exemple, pour un résultat `UnauthorizedAccess:EC2/SSHBruteForce`, plusieurs tentatives d'accès à votre instance sont regroupées dans le même ID de résultat, ce qui augmente la valeur de Nombre dans les détails du résultat. En effet, cette découverte représente un problème de sécurité unique, l'instance indiquant que le SSH port de l'instance n'est pas correctement sécurisé contre ce type d'activité. Toutefois, si une activité d'SSHaccès ciblant une nouvelle instance de votre environnement est GuardDuty détectée, une nouvelle découverte sera créée avec un identifiant de recherche unique pour vous avertir de l'existence d'un problème de sécurité associé à la nouvelle ressource.

Lorsqu'un résultat est regroupé, il est mis à jour avec les informations de la dernière occurrence de cette activité. Dans l'exemple ci-dessus, cela signifie que si votre instance est la cible d'une tentative d'attaque en force de la part d'un nouvel acteur, les détails du résultat seront mis à jour pour refléter l'adresse IP distante de la source la plus récente et les informations plus anciennes seront remplacées. Les informations complètes sur les tentatives d'activité individuelles seront toujours disponibles dans vos journaux CloudTrail ou dans ceux de VPC flux.

Les critères qui incitent GuardDuty à générer un nouveau résultat au lieu d'agréger un résultat existant dépendent du type de recherche. Les critères de regroupement pour chaque type de résultat sont déterminés par nos ingénieurs en sécurité afin de vous donner la meilleure vue d'ensemble des problèmes de sécurité distincts au sein de votre compte.

Types de résultats

Pour plus d'informations sur les modifications importantes apportées aux types de GuardDuty recherche, y compris les types de recherche récemment ajoutés ou retirés, voirHistorique du document pour Amazon GuardDuty.

Pour plus d'informations sur les types de résultat désormais retirés, veuillez consulter Retrait de types de résultat.

GuardDuty Types de recherche EC2

Les résultats suivants sont propres aux ressources Amazon EC2 et ont toujours le type de ressource `Instance`. La gravité et les détails des résultats diffèrent selon le rôle de la ressource, qui indique si la ressource EC2 était la cible ou l'auteur d'une activité suspecte.

Les résultats répertoriés ici incluent les sources de données et les modèles utilisés pour générer ce type de résultat. Pour plus d'informations sur les sources de données et les modèles, veuillez consulter GuardDuty sources de données de base.

> **Note**
>
> Des détails de l'instance peuvent être manquants pour certains résultats EC2 si l'instance a déjà été résiliée ou si l'appel d'API sous-jacent faisait partie d'un appel d'API entre régions qui provenait d'une instance EC2 dans une région différente.

Pour tous les résultats EC2, il est recommandé d'examiner la ressource en question afin de déterminer si elle se comporte comme prévu. Si l'activité est autorisée, vous pouvez utiliser les listes de règles de suppression ou d'adresses IP approuvées pour éviter les notifications faussement positives pour cette ressource. En cas d'activité inattendue, la bonne pratique en matière de sécurité consiste à supposer que l'instance est compromise et à prendre les mesures détaillées dans Corriger une instance Amazon EC2 potentiellement compromise.

Rubriques

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS

- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint

- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

Une instance EC2 interroge une adresse IP associée à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance répertoriée dans votre environnement AWS interroge une adresse IP avec un serveur de commande et de contrôle connu. L'instance répertoriée est peut-être compromise. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui sont infectés et contrôlés par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer une attaque par déni de service distribué (DDoS).

> **Note**
>
> Si l'adresse IP demandée est liée à log4j, les champs du résultat associé incluront les valeurs suivantes :

- Service. Informations supplémentaires. threatListName = Amazon
- service.additionalInfo.threatName = lié à Log4j

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/C&CActivity.B!DNS

Une instance EC2 interroge un nom de domaine associé à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance répertoriée dans votre environnement AWS interroge un nom de domaine avec un serveur de commande et de contrôle connu. L'instance répertoriée est peut-être compromise. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui sont infectés et contrôlés par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer une attaque par déni de service distribué (DDoS).

> **Note**
>
> Si le nom de domaine demandé est lié à log4j, les champs du résultat associé incluront les valeurs suivantes :
>
> - Service. Informations supplémentaires. threatListName = Amazon

- service.additionalInfo.threatName = lié à Log4j

> **Note**
>
> Pour tester le GuardDuty mode de génération de ce type de recherche, vous pouvez effectuer une requête DNS depuis votre instance `dig` (sous Linux ou `nslookup` Windows) sur un domaine de test`guarddutyc2activityb.com`.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/DenialOfService.Dns

Une instance EC2 se comporte d'une manière pouvant indiquer qu'elle est utilisée pour réaliser une attaque Denial of Service (DoS) à l'aide du protocole DNS.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic DNS sortant. Cela peut indiquer que l'instance répertoriée est compromise et qu'elle est utilisée pour effectuer des attaques denial-of-service (DoS) à l'aide du protocole DNS.

> **Note**
>
> Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/DenialOfService.Tcp

Une instance EC2 se comporte d'une manière indiquant qu'elle est utilisée pour réaliser une attaque DoS (Denial of Service) à l'aide du protocole TCP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic TCP sortant. Cela peut indiquer que l'instance est compromise et qu'elle est utilisée pour effectuer des attaques denial-of-service (DoS) à l'aide du protocole TCP.

> **Note**
>
> Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/DenialOfService.Udp

Une instance EC2 se comporte d'une manière indiquant qu'elle est utilisée pour réaliser une attaque DoS (Denial of Service) à l'aide du protocole UDP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic UDP sortant. Cela peut indiquer que l'instance répertoriée est compromise et qu'elle est utilisée pour effectuer des attaques denial-of-service (DoS) à l'aide du protocole UDP.

> **Note**
>
> Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Une instance EC2 se comporte d'une manière pouvant indiquer qu'elle est utilisée pour réaliser une attaque Denial of Service (DoS) à l'aide du protocole UDP sur un port TCP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic UDP sortant ciblé sur un port qui est généralement utilisé pour les communications TCP. Cela peut indiquer que l'instance répertoriée est compromise et qu'elle est utilisée pour effectuer des attaques denial-of-service (DoS) à l'aide du protocole UDP sur un port TCP.

> **Note**
>
> Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/DenialOfService.UnusualProtocol

Une instance EC2 se comporte d'une manière pouvant indiquer qu'elle est utilisée pour réaliser une attaque Denial of Service (DoS) à l'aide d'un protocole inhabituel.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS génère un important volume de trafic sortant d'un type de protocole inhabituel qui n'est généralement pas utilisé par des instances EC2, comme Internet Group Management Protocol. Cela peut indiquer que l'instance est compromise et qu'elle est utilisée pour effectuer des attaques denial-of-service (DoS) à l'aide d'un protocole inhabituel. Ce résultat détecte les attaques DoS contre les adresses IP publiquement routables uniquement, qui sont les principales cibles des attaques DoS.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/Spambot

Une instance EC2 présente un comportement inhabituel en communiquant avec un hôte distant sur le port 25.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS communique avec un hôte distant sur le port 25. Ce comportement est inhabituel, car cette instance EC2 n'a aucun historique de communication sur le port 25. Ce dernier est généralement utilisé par les serveurs de

messagerie pour les communications SMTP. Ce résultat indique que votre instance EC2 est peut être compromise et utilisée dans le cadre d'envoi de courriers indésirables.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Behavior:EC2/NetworkPortUnusual

Une instance EC2 communique avec un hôte distant sur un port serveur inhabituel.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a jamais communiqué sur ce port distant auparavant.

> **Note**
>
> Si l'instance EC2 a communiqué sur le port 389 ou le port 1389, la gravité du résultat associé sera modifiée en Élevée et les champs de recherche incluront la valeur suivante :
>
> - service.additionalInfo.context = possible rappel log4j

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Behavior:EC2/TrafficVolumeUnusual

Une instance EC2 génère un volume de trafic réseau inhabituellement élevé à destination d'un hôte distant.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a jamais envoyé un tel volume de trafic vers cet hôte distant auparavant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

CryptoCurrency:EC2/BitcoinTool.B

Une instance EC2 interroge une adresse IP associée à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS interroge une adresse IP associée à une activité liée au Bitcoin ou à une autre cryptomonnaie. Le Bitcoin est une cryptomonnaie et un système de paiement numérique mondiaux pouvant faire l'objet d'échanges contre d'autres devises, produits et services. Le bitcoin est une récompense pour le minage de Bitcoins et est très recherché par les acteurs de la menace.

Recommandations de correction :

Si vous utilisez cette instance EC2 pour exploiter ou gérer de la cryptomonnaie, ou si cette instance est impliquée d'une autre manière dans une activité de blockchain, ce résultat peut être une activité attendue pour votre environnement. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `CryptoCurrency:EC2/BitcoinTool.B`. Le deuxième critère de filtrage doit être l' ID d'instance de l'instance impliquée dans l'activité de blockchain. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Une instance EC2 interroge un nom de domaine associé à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS interroge un nom de domaine associé à une activité liée au Bitcoin ou à une autre cryptomonnaie. Le Bitcoin est une cryptomonnaie et un système de paiement numérique mondiaux pouvant faire l'objet d'échanges contre d'autres devises, produits et services. Le bitcoin est une récompense pour le minage de Bitcoins et est très recherché par les acteurs de la menace.

Recommandations de correction :

Si vous utilisez cette instance EC2 pour exploiter ou gérer de la cryptomonnaie, ou si cette instance est impliquée d'une autre manière dans une activité de blockchain, ce résultat peut être une activité attendue pour votre environnement. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Le deuxième critère de filtrage doit être l' ID d'instance de l'instance impliquée dans l'activité de blockchain. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

DefenseEvasion:EC2/UnusualDNSResolver

Une instance Amazon EC2 communique avec un résolveur DNS public inhabituel.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance Amazon EC2 répertoriée de votre environnement AWS se comporte différemment du comportement de référence. Cette instance EC2 n'a aucun historique récent de communication avec ce résolveur DNS public. Le champ Unusual du panneau des détails de recherche de la GuardDuty console peut fournir des informations sur le résolveur DNS demandé.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

DefenseEvasion:EC2/UnusualDoHActivity

Une instance Amazon EC2 effectue une communication DNS sur HTTPS (DoH) inhabituelle.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance Amazon EC2 répertoriée au sein de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a aucun historique récent de communications DNS sur HTTPS (DoH) avec ce serveur DoH public. Le champ Inhabituel dans les détails du résultat peut fournir des informations sur le serveur DoH interrogé.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

DefenseEvasion:EC2/UnusualDoTActivity

Une instance Amazon EC2 effectue une communication DNS sur TLS (DoT) inhabituelle.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS se comporte différemment de la référence établie. Cette instance EC2 n'a aucun historique récent de communications DNS sur TLS (DoT) avec ce serveur DoT public. Le champ Inhabituel dans le volet des détails du résultat peut fournir des informations sur le serveur DoT interrogé.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Impact:EC2/AbusedDomainRequest.Reputation

Une instance EC2 interroge un nom de domaine de mauvaise réputation associé à des domaines abusifs connus.

Gravité par défaut : moyenne

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée au sein de votre environnement AWS interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP abusifs connus. Les noms de domaine de premier niveau (TLD) et les noms de domaine de deuxième niveau (2LD) fournissant des enregistrements de sous-domaines gratuits ainsi que les fournisseurs de DNS dynamiques sont des exemples de domaines utilisés de manière abusive. Les acteurs de la menace ont tendance à utiliser ces services pour enregistrer des domaines gratuitement ou à faible coût. Les domaines de mauvaise réputation de cette catégorie peuvent également être des domaines expirés renvoyés à l'adresse IP de stationnement d'un bureau d'enregistrement et peuvent donc ne plus être actifs. Une adresse IP de stationnement est l'endroit où un bureau d'enregistrement dirige le trafic vers des domaines qui n'ont été liés à aucun service. L'instance Amazon EC2 répertoriée peut être compromise, car les acteurs malveillants utilisent couramment ces bureaux d'enregistrement ou ces services pour la distribution de logiciels malveillants et de commande et de contrôle.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Impact:EC2/BitcoinDomainRequest.Reputation

Une instance EC2 interroge un nom de domaine de mauvaise réputation associé à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée de votre environnement AWS interroge un nom de domaine de mauvaise réputation associé à une activité liée au Bitcoin ou à une autre cryptomonnaie. Le Bitcoin est une cryptomonnaie et un système de paiement numérique mondiaux pouvant faire l'objet d'échanges contre d'autres devises, produits et services. Le bitcoin est une récompense pour le minage de Bitcoins et est très recherché par les acteurs de la menace.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si vous utilisez cette instance EC2 pour exploiter ou gérer de la cryptomonnaie, ou si cette instance est impliquée d'une autre manière dans une activité de blockchain, ce résultat peut représenter une activité attendue pour votre environnement. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `Impact:EC2/BitcoinDomainRequest.Reputation`. Le deuxième critère de filtrage doit être l' ID d'instance de l'instance impliquée dans l'activité de blockchain. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

Impact:EC2/MaliciousDomainRequest.Reputation

Une instance EC2 interroge un domaine de mauvaise réputation associé à des domaines malveillants connus.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée au sein de votre environnement AWS interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP malveillants connus. Par exemple, les domaines peuvent être associés à une adresse IP de gouffre connue. Les domaines de gouffre sont des domaines qui étaient auparavant contrôlés par un acteur menaçant, et les demandes qui leur sont adressées peuvent indiquer que l'instance est compromise. Ces domaines peuvent également être corrélés à des campagnes malveillantes ou à des algorithmes de génération de domaines connus.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Impact:EC2/PortSweep

Une instance EC2 analyse un port sur un grand nombre d'adresses IP.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée dans votre environnement AWS analyse un port sur un grand nombre d'adresses IP publiquement routables. Ce type d'activité est généralement utilisé pour rechercher des hôtes vulnérables à exploiter. Dans le panneau des informations de recherche de votre GuardDuty console, seule l'adresse IP distante la plus récente est affichée

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Impact:EC2/SuspiciousDomainRequest.Reputation

Une instance EC2 interroge un nom de domaine de mauvaise réputation qui est suspect par nature en raison de son ancienneté ou de sa faible popularité.

Gravité par défaut : faible

- Source de données : journaux DNS

Ce résultat vous informe que l'instance Amazon EC2 répertoriée dans votre environnement AWS interroge un nom de domaine de mauvaise réputation suspecté d'être malveillant. Nous avons remarqué des caractéristiques de ce domaine qui étaient cohérentes avec les domaines malveillants précédemment observés, mais notre modèle de réputation n'a pas pu les relier définitivement à une menace connue. Ces domaines sont généralement récemment observés ou reçoivent un faible trafic.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Impact:EC2/WinRMBruteForce

Une instance EC2 exécute une attaque sortante par force brute de Windows Remote Management.

Gravité par défaut : faible*

> **Note**
>
> La gravité de ce résultat est faible si votre instance EC2 était la cible d'une attaque par force brute. La gravité de ce résultat est élevée si votre instance EC2 est utilisée pour procéder à l'attaque par force brute.

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée dans votre environnement AWS exécute une attaque par force brute de Windows Remote Management (WinRM) visant à accéder au service Windows Remote Management sur les systèmes Windows.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Recon:EC2/PortProbeEMRUnprotectedPort

Un port non protégé lié à EMR d'une instance EC2 est en cours d'exploration par un hôte malveillant connu.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous indique qu'un port sensible lié à l'EMR sur l'instance EC2 répertoriée faisant partie d'un cluster de votre AWS environnement n'est pas bloqué par un groupe de sécurité, une liste de contrôle d'accès (ACL) ou un pare-feu sur hôte tel que Linux IPtables. Cette découverte indique également que des scanners connus sur Internet explorent activement ce port. Les ports qui peuvent déclencher ce résultat, tels que le port 8088 (port YARN Web UI) sont susceptibles d'être utilisés pour l'exécution de code à distance.

Recommandations de correction :

Il est recommandé de bloquer l'accès ouvert aux ports sur les clusters à partir d'Internet et de restreindre l'accès uniquement aux adresses IP qui requièrent un accès à ces ports. Pour de plus amples informations, veuillez consulter Groupes de sécurité pour les clusters EMR.

Recon:EC2/PortProbeUnprotectedPort

Un port non protégé d'une instance EC2 est en train d'être analysé par un hôte malveillant connu.

Gravité par défaut : faible*

> **Note**
>
> La gravité par défaut de ce résultat est faible. Toutefois, si le port examiné est utilisé par Elasticsearch (9200 ou 9300), le niveau de gravité du résultat est élevé.

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'un port de l'instance EC2 répertoriée de votre environnement AWS n'est pas bloqué par un groupe de sécurité, une liste de contrôle d'accès (ACL) ou un pare-feu sur l'hôte, comme Linux IPTables, et qu'il est en train d'être analysé activement par des analyseurs connus sur Internet.

Si ce port est le port 22 ou 3389 et que vous utilisez ces ports pour vous connecter à votre instance, vous pouvez toujours limiter leur exposition en autorisant uniquement leur accès aux adresses IP de l'espace d'adressage IP de votre réseau d'entreprise. Pour de plus amples informations sur la restriction de l'accès au port 22 sous Linux, veuillez consulter Autorisation du trafic entrant pour vos instances Linux. Pour savoir comment restreindre l'accès au port 3389 sous Windows, veuillez consulter Autorisation du trafic entrant pour vos instances Windows.

GuardDuty ne génère pas ce résultat pour les ports 443 et 80.

Recommandations de correction :

Dans certains cas, les instances peuvent être intentionnellement exposées, par exemple si elles hébergent des serveurs Web. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression

doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `Recon:EC2/PortProbeUnprotectedPort`. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui hébergent ces outils. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

Recon:EC2/Portscan

Une instance EC2 balaie les ports sortants vers un hôte distant.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS est impliquée dans une possible attaque par balayage de ports, car elle tente de se connecter à plusieurs ports sur une courte période. L'objectif d'une attaque par balayage de ports consiste à localiser les ports ouverts pour identifier les services exécutés par la machine et son système d'exploitation.

Recommandations de correction :

Ce résultat peut être un faux positif lorsque des applications d'évaluation de vulnérabilité sont déployées sur des instances EC2 dans votre environnement, car ces applications effectuent des analyses de port pour vous alerter à propos de ports ouverts mal configurés. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `Recon:EC2/Portscan`. Le second critère de filtre doit correspondre à l'instance ou aux instances qui hébergent ces outils d'évaluation de vulnérabilité. Vous pouvez utiliser l'attribut ID d'image d'instance ou Valeur de balise en fonction des critères identifiables avec les instances qui hébergent ces outils. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre instance est probablement compromise, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/BlackholeTraffic

Une instance EC2 tente de communiquer avec une adresse IP d'un hôte distant qui est un trou noir connu.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS pourrait être compromise, car elle tente de communiquer avec une adresse IP d'un trou noir (ou gouffre). Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire. Une adresse IP de trou noir désigne une machine hôte qui n'est pas en cours d'exécution ou une adresse à laquelle aucun hôte n'a été attribué.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/BlackholeTraffic!DNS

Une instance EC2 interroge le nom d'un domaine qui est redirigé vers l'adresse IP d'un trou noir.

Gravité par défaut : moyenne

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS pourrait être compromise, car elle interroge le nom d'un domaine qui est redirigé vers l'adresse IP d'un trou noir. Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/DGADomainRequest.B

Une instance EC2 interroge des domaines générés par des algorithmes. Ces domaines sont couramment utilisés par des programmes malveillants et peuvent constituer une indication d'instance EC2 compromise.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS tente d'interroger des DGA (algorithmes de génération de noms de domaine). Votre instance EC2 pourrait être compromise.

Ces algorithmes servent à générer périodiquement un grand nombre de noms de domaine qui peuvent être utilisés comme points de rendez-vous avec leurs serveurs de commande et de contrôle. Les serveurs de commande et de contrôle sont des ordinateurs qui émettent des commandes aux membres d'un botnet, qui est un ensemble d'appareils connectés à Internet qui sont infectés et contrôlés par un type courant de programme malveillant. Le grand nombre de points de rendez-vous potentiels rend l'arrêt des botnets difficile, car les ordinateurs infectés tentent de contacter certains de ces noms de domaine chaque jour pour recevoir des mises à jour ou des commandes.

> **Note**
>
> Ce résultat est basé sur une analyse de noms de domaine utilisant une heuristique avancée et peut donc identifier de nouveaux DGA qui ne sont pas présents dans les flux d'intelligence de menaces.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/DGADomainRequest.C!DNS

Une instance EC2 interroge des domaines générés par des algorithmes. Ces domaines sont couramment utilisés par des programmes malveillants et peuvent constituer une indication d'instance EC2 compromise.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS tente d'interroger des DGA (algorithmes de génération de noms de domaine). Votre instance EC2 pourrait être compromise.

Ces algorithmes servent à générer périodiquement un grand nombre de noms de domaine qui peuvent être utilisés comme points de rendez-vous avec leurs serveurs de commande et de contrôle. Les serveurs de commande et de contrôle sont des ordinateurs qui émettent des commandes aux membres d'un botnet, qui est un ensemble d'appareils connectés à Internet qui sont infectés et contrôlés par un type courant de programme malveillant. Le grand nombre de points de rendez-vous potentiels rend l'arrêt des botnets difficile, car les ordinateurs infectés tentent de contacter certains de ces noms de domaine chaque jour pour recevoir des mises à jour ou des commandes.

> **Note**
>
> Ce résultat est basé sur les domaines DGA connus issus des flux GuardDuty de renseignements sur les menaces.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/DNSDataExfiltration

Une instance EC2 exfiltre des données via des requêtes DNS.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS exécute un programme malveillant qui utilise des requêtes DNS pour transférer des données sortantes. Ce type de transfert de données indique qu'une instance est compromise et peut entraîner l'exfiltration de données. Généralement, le trafic DNS n'est pas bloqué par des pare-feu. Par exemple, un programme malveillant dans une instance EC2 compromise peut encoder des données, (comme votre numéro de carte de crédit) dans une requête DNS et les envoyer à un serveur DNS distant contrôlé par un pirate.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/DriveBySourceTraffic!DNS

Une instance EC2 interroge le nom de domaine d'un hôte distant qui est la source connue d'attaques de type « drive-by download ».

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe que l'instance EC2 répertoriée de votre environnement AWS pourrait être compromise, car elle interroge un nom de domaine qui est un hôte distant étant une source connue d'attaques de type « drive-by-download ». Il s'agit de téléchargements involontaires de logiciels d'Internet qui peuvent déclencher l'installation automatique de virus, logiciels espions ou programmes malveillants.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/DropPoint

Une instance EC2 tente de communiquer avec une adresse IP d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS tente de communiquer avec une adresse IP d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/DropPoint!DNS

Une instance EC2 interroge le nom de domaine d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Source de données : journaux DNS

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS interroge le nom de domaine d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Trojan:EC2/PhishingDomainRequest!DNS

Une instance EC2 interroge des domaines impliqués dans des attaques d'hameçonnage. Votre instance EC2 pourrait être compromise.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS tente d'interroger un domaine impliqué dans des attaques de hameçonnage. Les domaines de hameçonnage sont créés par des pirates se faisant passer pour une institution légitime afin de pousser des utilisateurs à fournir des données sensibles, telles que des informations personnelles identifiables, des coordonnées bancaires, des informations de carte bancaire ou des mots de passe. Votre instance EC2 essaie peut-être de récupérer des données sensibles stockées sur un site Web d'hameçonnage ou d'en configurer un. Votre instance EC2 pourrait être compromise.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Une instance EC2 établit des connexions à une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS communique avec une adresse IP figurant sur une liste de menaces que vous avez téléchargée. Dans GuardDuty, une liste de menaces comporte des adresses IP malveillantes connues. GuardDuty génère des résultats en fonction des listes de menaces chargées. La liste de menaces utilisée pour générer ce résultat sera répertoriée dans les détails du résultat.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

UnauthorizedAccess:EC2/MetadataDNSRebind

Une instance EC2 effectue des recherches DNS résolues en service de métadonnées d'instance.

Gravité par défaut : élevée

- Source de données : journaux DNS

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS interroge un domaine qui se résout en adresse IP des métadonnées EC2 (169.254.169.254). Une requête DNS de ce type peut indiquer que l'instance est une cible d'une technique de reliaison DNS. Celle-ci qui peut être utilisée pour obtenir des métadonnées à partir d'une instance EC2, y compris les informations d'identification IAM associées à l'instance.

La reliaison DNS implique de tromper une application s'exécutant sur l'instance EC2 pour charger des données de retour à partir d'une URL, où le nom de domaine de l'URL se résout en adresse IP des métadonnées EC2 (169.254.169.254). Cela conduit l'application à accéder aux métadonnées EC2 et éventuellement à les mettre à la disposition du pirate.

Il est possible d'accéder aux métadonnées EC2 à l'aide de la fonction de reliaison DNS uniquement si l'instance EC2 exécute une application vulnérable qui permet l'injection d'URL, ou si une personne accède à l'URL dans un navigateur Web s'exécutant sur l'instance EC2.

Recommandations de correction :

En réponse à ce résultat, vous devez évaluer s'il existe une application vulnérable en cours d'exécution sur l'instance EC2 ou si une personne a utilisé un navigateur pour accéder au domaine identifié dans le résultat. Si la cause première est une application vulnérable, vous devez corriger la vulnérabilité. Si une personne a navigué dans le domaine identifié, vous devez bloquer le domaine ou empêcher les utilisateurs d'y accéder. Si vous déterminez que ce résultat était lié à l'un ou l'autre des cas ci-dessus, révoquez la session associée à l'instance EC2.

Certains clients AWS mappent intentionnellement l'adresse IP des métadonnées à un nom de domaine sur leurs serveurs DNS faisant autorité. Si c'est le cas dans votre environnement ,

nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `UnauthorizedAccess:EC2/MetaDataDNSRebind`. Le deuxième critère de filtrage doit être le DNS request domain (Domaine de demande DNS) et la valeur doit correspondre au domaine que vous avez mappé sur l'adresse IP des métadonnées (169.254.169.254). Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

UnauthorizedAccess:EC2/RDPBruteForce

Une instance EC2 a été impliquée dans des attaques en force RDP.

Gravité par défaut : faible*

> **Note**
>
> La gravité de ce résultat est faible si votre instance EC2 était la cible d'une attaque par force brute. La gravité de ce résultat est élevée si votre instance EC2 est utilisée pour procéder à l'attaque par force brute.

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS a été impliquée dans une attaque en force visant à obtenir les mots de passe de services RDP sur des systèmes Windows. Cela peut être signe d'un accès non autorisé à vos ressources AWS.

Recommandations de correction :

Si le rôle de ressource de votre instance est `ACTOR`, cela indique que votre instance a été utilisée pour procéder à des attaques par force brute RDP. À moins que cette instance ait une raison légitime de contacter l'adresse IP répertoriée en tant que `Target`, il est recommandé de supposer que votre instance est compromise et de prendre les mesures répertoriées dans Corriger une instance Amazon EC2 potentiellement compromise.

Si le rôle de ressource de votre instance est `TARGET`, ce résultat peut être corrigé en sécurisant votre port RDP uniquement pour des adresses IP approuvées via des groupes de sécurité, des listes de

contrôle d'accès ou des pare-feu. Pour plus d'informations, veuillez consulter Conseils pour sécuriser vos instances EC2 (Linux) (langue française non garantie).

UnauthorizedAccess:EC2/SSHBruteForce

Une instance EC2 a été impliquée dans des attaques en force SSH.

Gravité par défaut : faible*

> **Note**
>
> La gravité de ce résultat est faible si une attaque par force brute vise l'une de vos instances EC2. La gravité de ce résultat est élevée si votre instance EC2 est utilisée pour effectuer l'attaque par force brute.

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS a été impliquée dans une attaque en force visant à obtenir les mots de passe de services SSH sur des systèmes Linux. Cela peut être signe d'un accès non autorisé à vos ressources AWS.

> **Note**
>
> Ce résultat est généré uniquement par la surveillance du trafic de sur le port 22. Si vos services SSH sont configurées de façon à utiliser d'autres ports, ce résultat n'est pas généré.

Recommandations de correction :

Si la cible de la tentative d'attaque en force est un hôte bastion, cela peut représenter le comportement attendu pour votre environnement AWS. Dans ce cas, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `UnauthorizedAccess:EC2/SSHBruteForce`. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image

d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui hébergent ces outils. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

Si cette activité n'est pas attendue pour votre environnement et que le rôle de ressource de votre instance est `TARGET`, ce résultat peut être corrigé en sécurisant votre port SSH uniquement pour des adresses IP approuvées via des groupes de sécurité, des listes de contrôle d'accès ou des pare-feu. Pour plus d'informations, veuillez consulter Conseils pour sécuriser vos instances EC2 (Linux) (langue française non garantie).

Si le rôle de ressource de votre instance est `ACTOR`, cela indique que l'instance a été utilisée pour procéder à des attaques par force brute SSH. À moins que cette instance ait une raison légitime de contacter l'adresse IP répertoriée en tant que `Target`, il est recommandé de supposer que votre instance est compromise et de prendre les mesures répertoriées dans Corriger une instance Amazon EC2 potentiellement compromise.

UnauthorizedAccess:EC2/TorClient

Votre instance EC2 est en train de se connecter à un nœud Tor Guard ou Authority.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS est en train de se connecter à un nœud Tor Guard ou Authority. Tor est un logiciel permettant d'activer les communications anonymes. Les nœuds Tor Guards et Authority agissent en tant que passerelles initiales dans un réseau Tor. Ce trafic peut indiquer que cette instance EC2 a été compromise et agit en tant que client sur un réseau Tor. Ce résultat peut être le signe d'un accès non autorisé à vos ressources AWS dans le but de masquer la véritable identité du pirate.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

UnauthorizedAccess:EC2/TorRelay

Votre instance EC2 est en train de se connecter à un réseau Tor en tant que relais Tor.

Gravité par défaut : élevée

- Source de données : journaux de flux VPC

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS est en train de se connecter à un réseau Tor d'une façon qui suggère qu'elle agit en tant que relais Tor. Tor est un logiciel permettant d'activer les communications anonymes. Tor augmente l'anonymat de la communication en réacheminant le trafic potentiellement illicite du client d'un relais Tor à un autre.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d'informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

GuardDuty IAMtypes de recherche

Les résultats suivants sont spécifiques aux IAM entités et aux clés d'accès et ont toujours un type de ressource de`AccessKey`. La gravité et les détails des résultats diffèrent selon le type de résultat.

Les résultats répertoriés ici incluent les sources de données et les modèles utilisés pour générer ce type de résultat. Pour plus d'informations, consultez GuardDuty sources de données de base.

Pour tous IAM les résultats connexes, nous vous recommandons d'examiner l'entité en question et de vous assurer que ses autorisations respectent les meilleures pratiques du moindre privilège. Si cette activité est inattendue, les informations d'identification peuvent être compromises. Pour plus d'informations sur la correction des résultats, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Rubriques

- CredentialAccess:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/AnomalousBehavior
- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux

- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Un API utilisateur utilisé pour accéder à un AWS environnement a été invoqué de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes effectuées à proximité par une seule identité d'utilisateur. L'APIobservation est généralement associée à la phase d'accès aux informations d'identification d'une attaque lorsqu'un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre environnement. Les APIs éléments de cette catégorie sont `GetPasswordDataGetSecretValue`,`BatchGetSecretValue`, et`GenerateDbAuthToken`.

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Vous trouverez des informations sur les facteurs de la API demande qui sont inhabituels pour l'identité de l'utilisateur qui a invoqué la demande dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

DefenseEvasion:IAMUser/AnomalousBehavior

Un instrument API utilisé pour échapper aux mesures défensives a été invoqué de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes effectuées à proximité par une seule identité d'utilisateur. Ce qui est API observé est généralement associé à des tactiques d'évasion défensive où un adversaire essaie de couvrir ses traces et d'éviter d'être détecté. APIsdans cette catégorie figurent généralement des opérations de suppression, de désactivation ou d'arrêt, telles que`DeleteFlowLogs`,`DisableAlarmActions`, ou`StopLogging`.

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Vous trouverez des informations sur les facteurs de la API demande qui sont inhabituels pour l'identité de l'utilisateur qui a invoqué la demande dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Discovery:IAMUser/AnomalousBehavior

Un API outil couramment utilisé pour découvrir des ressources a été invoqué de manière anormale.

Gravité par défaut : faible

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes effectuées à proximité par une seule identité d'utilisateur. L'APIobservation est généralement associée à la phase de découverte d'une attaque, au cours de laquelle un adversaire collecte des informations pour déterminer si votre AWS environnement est susceptible d'être victime d'une attaque de plus grande envergure. APIsdans cette catégorie figurent généralement des opérations d'obtention, de description ou de liste, telles que`DescribeInstances`,`GetRolePolicy`, ou`ListAccessKeys`.

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Vous trouverez des informations sur les facteurs de la API demande qui sont inhabituels pour l'identité de l'utilisateur qui a invoqué la demande dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Exfiltration:IAMUser/AnomalousBehavior

Un outil API couramment utilisé pour collecter des données à partir d'un AWS environnement a été invoqué de manière anormale.

Gravité par défaut : élevée

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes effectuées à proximité par une seule identité d'utilisateur. Ce qui est API observé est généralement associé à des tactiques d'exfiltration dans le cadre desquelles un adversaire tente de collecter des données sur votre réseau en utilisant le packaging et le cryptage pour éviter d'être détecté. APIspour ce type de recherche sont uniquement des opérations de gestion (plan de contrôle) et sont généralement liées à S3, aux instantanés et aux bases de données, telles que,`PutBucketReplication`, `CreateSnapshot` ou. `RestoreDBInstanceFromDBSnapshot`

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Vous trouverez des informations sur les facteurs de la API demande qui sont inhabituels pour l'identité de l'utilisateur qui a invoqué la demande dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d’informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Impact:IAMUser/AnomalousBehavior

Une API méthode couramment utilisée pour altérer des données ou des processus dans un AWS environnement a été invoquée de manière anormale.

Gravité par défaut : élevée

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes

effectuées à proximité par une seule identité d'utilisateur. Ce qui est API observé est généralement associé à des tactiques d'impact dans le cadre desquelles un adversaire tente de perturber les opérations et de manipuler, d'interrompre ou de détruire les données de votre compte. APIspour ce type de recherche sont généralement des opérations de suppression, de mise à jour ou de saisie, telles que`DeleteSecurityGroup`,`UpdateUser`, ou`PutBucketPolicy`.

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Vous trouverez des informations sur les facteurs de la API demande qui sont inhabituels pour l'identité de l'utilisateur qui a invoqué la demande dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

InitialAccess:IAMUser/AnomalousBehavior

Une méthode API couramment utilisée pour obtenir un accès non autorisé à un AWS environnement a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes effectuées à proximité par une seule identité d'utilisateur. L'APIobservation est généralement associée à la phase d'accès initiale d'une attaque lorsqu'un adversaire tente d'accéder à votre environnement. APIsdans cette catégorie figurent généralement des opérations get token ou de session, telles que`GetFederationToken`,`StartSession`, ou`GetAuthorizationToken`.

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires.

Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Vous trouverez des informations sur les facteurs de la API demande qui sont inhabituels pour l'identité de l'utilisateur qui a invoqué la demande dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

PenTest:IAMUser/KaliLinux

An API a été invoqué depuis une machine Kali Linux.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Cette découverte vous indique qu'une machine exécutant Kali Linux passe des API appels en utilisant des informations d'identification appartenant au AWS compte répertorié dans votre environnement. Kali Linux est un outil de test d'intrusion populaire que les professionnels de la sécurité utilisent pour identifier les faiblesses des EC2 instances nécessitant des correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses EC2 de configuration et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

PenTest:IAMUser/ParrotLinux

An API a été invoqué depuis une machine Parrot Security Linux.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une machine exécutant Parrot Security Linux passe des API appels en utilisant des informations d'identification appartenant au AWS compte répertorié dans votre environnement. Parrot Security Linux est un outil de test d'intrusion populaire que les professionnels de la sécurité utilisent pour identifier les faiblesses des EC2 instances nécessitant des correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses EC2 de configuration et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

PenTest:IAMUser/PentooLinux

An API a été invoqué depuis une machine Pentoo Linux.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Cette découverte vous indique qu'une machine exécutant Pentoo Linux passe des API appels en utilisant des informations d'identification appartenant au AWS compte répertorié dans votre environnement. Pentoo Linux est un outil de test d'intrusion populaire que les professionnels de la sécurité utilisent pour identifier les faiblesses des EC2 instances nécessitant des correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses EC2 de configuration et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Persistence:IAMUser/AnomalousBehavior

Une méthode API couramment utilisée pour maintenir un accès non autorisé à un AWS environnement a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes effectuées à proximité par une seule identité d'utilisateur. Ce qui est API observé est généralement associé à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre environnement et tente de conserver cet accès. APIsdans cette catégorie figurent généralement des opérations de création, d'importation ou de modification, telles que`CreateAccessKey`,`ImportKeyPair`, ou`ModifyInstanceAttribute`.

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Les détails sur les facteurs de la API demande qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande figurent dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d’informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Policy:IAMUser/RootCredentialUsage

Un API a été invoqué à l'aide des informations de connexion de l'utilisateur root.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion ou événements CloudTrail de données

Ce résultat vous informe que les informations d'identification de connexion de l'utilisateur root de l' Compte AWS répertorié dans votre environnement sont utilisées pour effectuer des demandes aux services AWS . Il est recommandé aux utilisateurs de ne jamais utiliser les informations de connexion de l'utilisateur root pour accéder aux AWS services. Au lieu de cela, AWS les services doivent être accessibles en utilisant les informations d'identification temporaires avec le moindre

privilège provenant de AWS Security Token Service (STS). Dans les situations où AWS STS ce n'est pas pris en charge, les informations IAM d'identification de l'utilisateur sont recommandées. Pour plus d'informations, consultez la section IAMMeilleures pratiques.

> **Note**
>
> Si la détection des menaces S3 est activée pour le compte, ce résultat peut être généré en réponse à des tentatives d'exécution d'opérations du plan de données S3 sur des ressources S3 à l'aide des informations d'identification de connexion de l'utilisateur root de l' Compte AWS. L'APIappel utilisé sera répertorié dans les détails de la recherche. Si la détection des menaces S3 n'est pas activée, cette découverte ne peut être déclenchée que par le journal des événementsAPIs. Pour de plus amples informations sur la détection des menaces S3, veuillez consulter Protection S3.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Une méthode API couramment utilisée pour obtenir des autorisations de haut niveau sur un AWS environnement a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une API demande anormale a été observée dans votre compte. Cette constatation peut inclure une seule demande API ou une série de API demandes connexes effectuées à proximité par une seule identité d'utilisateur. Ce qui est API observé est généralement associé à des tactiques d'augmentation de privilèges dans le cadre desquelles un adversaire tente d'obtenir des autorisations de niveau supérieur sur un environnement. APIsdans cette catégorie, impliquent généralement des opérations qui modifient IAM les politiques, les rôles et les utilisateurs, telles que`AssociateIamInstanceProfile`,`AddUserToGroup`, ou`PutUserPolicy`.

Cette API demande a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de la API demande, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et le API détail spécifique demandé. Les détails sur les facteurs de la API demande qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande figurent dans les détails de la recherche.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Recon:IAMUser/MaliciousIPCaller

An API a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une API opération permettant de répertorier ou de décrire les AWS ressources d'un compte au sein de votre environnement a été invoquée à partir d'une adresse IP figurant sur une liste de menaces. Un attaquant peut utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos AWS ressources afin de trouver des informations d'identification plus précieuses ou de déterminer les capacités des informations d'identification qu'il possède déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Recon:IAMUser/MaliciousIPCaller.Custom

An API a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une API opération permettant de répertorier ou de décrire les AWS ressources d'un compte au sein de votre environnement a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée. La liste de menaces utilisée sera répertoriée dans les détails du résultat. Un attaquant peut utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos AWS ressources afin de trouver des informations d'identification plus précieuses ou de déterminer les capacités des informations d'identification qu'il possède déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Recon:IAMUser/TorIPCaller

An API a été invoqué depuis l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Cette découverte vous indique qu'une API opération permettant de répertorier ou de décrire les AWS ressources d'un compte au sein de votre environnement a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Un attaquant utiliserait Tor pour masquer sa véritable identité.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail la journalisation a été désactivée.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'un CloudTrail sentier de votre AWS environnement a été désactivé. Il peut s'agir d'une tentative de la part d'un pirate de désactiver la journalisation pour éliminer toute trace de leur activité tout en accédant à vos ressources AWS à des fins malveillantes. Ce résultat peut également être déclenché par une suppression ou une mise à jour réussie d'un journal de suivi. Ce résultat peut également être déclenché par la suppression réussie d'un compartiment S3 qui stocke les journaux d'un journal associé à GuardDuty.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Stealth:IAMUser/PasswordPolicyChange

La stratégie de mot de passe du compte a été affaiblie.

Gravité par défaut : faible*

> **Note**
>
> La gravité de ce résultat peut être faible, moyenne ou élevée en fonction de la gravité des modifications apportées à la stratégie de mot de passe.

- Source de données : événements CloudTrail de gestion

La politique de mot de passe du AWS compte a été affaiblie sur le compte répertorié dans votre AWS environnement. Par exemple, elle a été supprimée ou mise à jour pour exiger moins de caractères ou prolonger la période d'expiration des mots de passe ou ne pas exiger de symboles et de nombres. Cette constatation peut également être déclenchée par une tentative de mise à jour ou de suppression de la politique de mot de passe de votre AWS compte. La politique de mot de passe du AWS compte définit les règles qui régissent les types de mots de passe qui peuvent être définis pour vos IAM utilisateurs. Une stratégie de mots de passe affaiblie permet de créer des mots de passe faciles à mémoriser et potentiellement plus faciles à deviner, ce qui crée un risque de sécurité.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Plusieurs connexions réussies à la console ont été observées dans le monde entier.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat indique que plusieurs connexions réussies à la console pour le même IAM utilisateur ont été observées à peu près au même moment dans différentes zones géographiques. Ces modèles de localisation d'accès anormaux et risqués indiquent un accès non autorisé potentiel à vos AWS ressources.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Les informations d'identification créées exclusivement pour une EC2 instance via un rôle de lancement d'instance sont utilisées à partir d'un autre compte interne AWS.

Gravité par défaut : élevée*

> **Note**
>
> La gravité par défaut de ce résultat est élevée. Toutefois, s'il a API été invoqué par un compte affilié à votre AWS environnement, le niveau de gravité est moyen.

- Source de données : événements CloudTrail de gestion ou événements de données S3

Ce résultat vous informe lorsque les informations d'identification de votre EC2 instance sont utilisées pour appeler à APIs partir d'une adresse IP appartenant à un AWS compte différent de celui dans lequel l'EC2instance associée est exécutée.

AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exempleEC2, AWS applications ou Lambda). Toutefois, les utilisateurs autorisés peuvent exporter les informations d'identification de leurs EC2 instances pour passer des API appels légitimes. Si le `remoteAccountDetails.Affiliated` champ est `True` celui qui API a été invoqué depuis un compte associé à votre AWS environnement. Pour exclure une attaque potentielle et vérifier la légitimité de l'activité, contactez l'IAMutilisateur auquel ces informations d'identification sont attribuées.

> **Note**
>
> S'il GuardDuty observe une activité continue depuis un compte distant, son modèle d'apprentissage automatique (ML) l'identifiera comme un comportement attendu. Par conséquent, GuardDuty cessera de générer ce résultat pour l'activité de ce compte distant. GuardDuty continuera à générer des informations sur les nouveaux comportements d'autres comptes distants et réévaluera les comptes distants appris à mesure que le comportement évolue au fil du temps.

Recommandations de correction :

En réponse à ce résultat, vous pouvez utiliser le flux de travail suivant pour déterminer un plan d'action :

1. Identifiez le compte distant concerné depuis le champ `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Déterminez ensuite si ce compte est affilié à votre GuardDuty environnement depuis le `service.action.awsApiCallAction.remoteAccountDetails.affiliated` terrain.
3. Si le compte est affilié, contactez le propriétaire du compte distant et le propriétaire des informations d'identification de l'EC2instance pour enquêter.
4. Si le compte n'est pas affilié, évaluez d'abord si le compte est associé à votre organisation mais qu'il ne fait pas partie de votre configuration GuardDuty multi-comptes, ou s'il n' GuardDuty a pas encore été activé dans le compte. Sinon, contactez le propriétaire des EC2 informations

d'identification pour déterminer s'il existe un cas d'utilisation pour un compte distant d'utiliser ces informations d'identification.

5. Si le propriétaire des informations d'identification ne reconnaît pas le compte distant, il est possible que les informations d'identification aient été compromises par un acteur malveillant opérant au sein d' AWS. Vous devez suivre les étapes recommandées dans Corriger une instance Amazon EC2 potentiellement compromise pour sécuriser votre environnement.

   En outre, vous pouvez envoyer un rapport d'abus à l'équipe de AWS confiance et de sécurité afin de lancer une enquête sur le compte distant. Lorsque vous soumettez votre rapport à AWS Trust and Safety, incluez tous JSON les détails du résultat.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Les informations d'identification créées exclusivement pour une EC2 instance via un rôle de lancement d'instance sont utilisées à partir d'une adresse IP externe.

Gravité par défaut : élevée

- Source de données : événements CloudTrail de gestion ou événements de données S3

Ce résultat vous indique qu'un hôte extérieur AWS a tenté d'exécuter des AWS API opérations à l'aide AWS d'informations d'identification temporaires créées sur une EC2 instance de votre AWS environnement. L'EC2instance répertoriée est peut-être compromise et les informations d'identification temporaires de cette instance ont peut-être été exfiltrées vers un hôte distant situé en dehors de. AWS AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exempleEC2, AWS applications ou Lambda). Toutefois, les utilisateurs autorisés peuvent exporter les informations d'identification de leurs EC2 instances pour passer des API appels légitimes. Pour exclure une attaque potentielle et vérifier la légitimité de l'activité, vérifiez si l'utilisation des informations d'identification de l'instance provenant de l'adresse IP distante dans le résultat est prévue.

> **Note**
>
> S'il GuardDuty observe une activité continue depuis un compte distant, son modèle d'apprentissage automatique (ML) l'identifiera comme un comportement attendu. Par conséquent, GuardDuty cessera de générer ce résultat pour l'activité de ce compte distant.

GuardDuty continuera à générer des informations sur les nouveaux comportements d'autres comptes distants et réévaluera les comptes distants appris à mesure que le comportement évolue au fil du temps.

Recommandations de correction :

Ce résultat est généré lorsque le réseau est configuré pour acheminer le trafic Internet de manière à ce qu'il sorte d'une passerelle locale plutôt que d'une passerelle VPC Internet ()IGW. Les configurations courantes, telles que l'utilisation AWS Outpostsou VPC VPN les connexions, peuvent entraîner le routage du trafic de cette façon. Si ce comportement est attendu, nous vous recommandons d'utiliser des règles de suppression et de créer une règle composée de deux critères de filtrage. Le premier critère est le type de résultat, qui devrait être `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Le deuxième critère de filtre est l'IPv4adresse de l'APIappelant avec l'adresse IP ou la CIDR plage de votre passerelle Internet locale. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression.

Note

S'il GuardDuty observe une activité continue provenant d'une source externe, son modèle d'apprentissage automatique identifiera ce comportement comme attendu et cessera de générer ce résultat pour l'activité provenant de cette source. GuardDuty continuera à générer des résultats concernant de nouveaux comportements à partir d'autres sources et réévaluera les sources apprises à mesure que les comportements évoluent au fil du temps.

Si cette activité est inattendue, vos informations d'identification peuvent être compromises, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

An API a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une API opération (par exemple, une tentative de lancement d'une EC2 instance, de création d'un nouvel IAM utilisateur ou de modification de vos AWS privilèges) a été invoquée à partir d'une adresse IP malveillante connue. Cela peut indiquer un accès non autorisé aux AWS ressources de votre environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Un API a été invoqué à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une API opération (par exemple, une tentative de lancement d'une EC2 instance, de création d'un nouvel IAM utilisateur ou de modification de AWS privilèges) a été invoquée à partir d'une adresse IP figurant sur une liste de menaces que vous avez téléchargée. Dans , une liste de menaces comporte des adresses IP malveillantes connues. Cela peut indiquer un accès non autorisé aux AWS ressources de votre environnement.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

UnauthorizedAccess:IAMUser/TorIPCaller

An API a été invoqué depuis l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une API opération (par exemple, une tentative de lancement d'une EC2 instance, de création d'un nouvel IAM utilisateur ou de modification de vos AWS privilèges) a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à vos ressources AWS dans le but de masquer la véritable identité du pirate.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour plus d'informations, voir Corriger les informations d'identification potentiellement compromises AWS.

GuardDuty Types de recherche S3

Les résultats suivants sont spécifiques aux ressources Amazon S3 et auront un type de ressource indiquant `S3Bucket` si la source de données est constituée d'événements de CloudTrail données pour S3 ou `AccessKey` si la source de données est constituée d'événements CloudTrail de gestion. La gravité et les détails des résultats diffèrent selon le type de résultat et l'autorisation associée au compartiment.

Les résultats répertoriés ici incluent les sources de données et les modèles utilisés pour générer ce type de résultat. Pour plus d'informations sur les sources de données et les modèles, veuillez consulter GuardDuty sources de données de base.

> **Important**
>
> Les résultats contenant une source de CloudTrail données contenant des événements de données pour S3 ne sont générés que si la protection S3 est activée pour GuardDuty. La protection S3 est activée par défaut dans tous les comptes créés après le 31 juillet 2020. Pour en savoir plus sur l'activation de la protection S3, veuillez consulter GuardDuty Protection S3.

Pour tous les résultats de type `S3Bucket`, il est recommandé d'examiner les autorisations sur le compartiment en question et les autorisations de tous les utilisateurs impliqués dans le résultat. Si l'activité est inattendue, veuillez consulter les recommandations de correction détaillées dans Corriger un compartiment S3 potentiellement compromis.

Rubriques

Discovery:S3/AnomalousBehavior

Une API couramment utilisée pour découvrir des objets S3 a été invoquée de manière anormale.

Gravité par défaut : faible

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une entité IAM a invoqué une API S3 pour découvrir des compartiments S3 dans votre environnement, comme `ListObjects`. Ce type d'activité est associé à la phase de découverte d'une attaque au cours de laquelle un attaquant collecte des informations pour déterminer si votre AWS environnement est susceptible d'être victime d'une attaque de plus grande envergure. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, veuillez consulter Détails du résultat.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

Discovery:S3/MaliciousIPCaller

Une API S3 couramment utilisée pour découvrir des ressources dans un AWS environnement a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3 a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à la phase de découverte d'une attaque lorsqu'un adversaire collecte des informations sur votre AWS environnement. Exemples : `GetObjectAcl` et `ListObjects`.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Discovery:S3/MaliciousIPCaller.Custom

Une API S3 a été invoquée depuis une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une API S3, comme `GetObjectAcl` ou `ListObjects`, a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. Ce type d'activité est associé à la phase de découverte d'une attaque au cours de laquelle un pirate collecte des informations pour déterminer si votre environnement AWS est vulnérable à une attaque de plus grande envergure.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Discovery:S3/TorIPCaller

Une API S3 a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une API S3, comme `GetObjectAcl` ou `ListObjects`, a été invoquée depuis une adresse IP du nœud de sortie Tor. Ce type d'activité est associé à la phase de

découverte d'une attaque au cours de laquelle un attaquant collecte des informations pour déterminer si votre AWS environnement est vulnérable à une attaque de plus grande envergure. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Exfiltration:S3/AnomalousBehavior

Une entité IAM a invoqué une API S3 de manière suspecte.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une entité IAM effectue des appels d'API qui impliquent un compartiment S3 et que cette activité diffère de la référence établie de cette entité. L'appel d'API utilisé dans cette activité est associé à la phase d'exfiltration d'une attaque, au cours de laquelle un pirate tente de collecter des données. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, veuillez consulter Détails du résultat.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Exfiltration:S3/MaliciousIPCaller

Une API S3 couramment utilisée pour collecter des données à partir d'un AWS environnement a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3 a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques d'exfiltration dans le cadre desquelles un adversaire tente de collecter des données sur votre réseau. Exemples : `GetObject` et `CopyObject`.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Impact:S3/AnomalousBehavior.Delete

Une entité IAM a invoqué une API S3 qui tente de supprimer des données de manière suspecte.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous indique qu'une entité IAM de votre AWS environnement effectue des appels d'API impliquant un compartiment S3, et que ce comportement est différent de la base de référence établie pour cette entité. L'appel d'API utilisé dans cette activité est associé à une attaque visant à supprimer des données. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par

exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, veuillez consulter Détails du résultat.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

Nous recommandons un audit du contenu de votre compartiment S3 afin de déterminer si la version précédente de l'objet peut ou doit être restaurée.

Impact:S3/AnomalousBehavior.Permission

Une API couramment utilisée pour définir les autorisations de liste de contrôle d'accès (ACL) a été invoquée de manière anormale.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous indique qu'une entité IAM de votre AWS environnement a modifié une politique de compartiment ou une ACL sur les compartiments S3 répertoriés. Cette modification peut exposer publiquement vos compartiments S3 à tous les utilisateurs authentifiés. AWS

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande,

l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, veuillez consulter Détails du résultat.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Nous recommandons un audit du contenu de votre compartiment S3 pour vous assurer qu'aucun objet n'a été autorisé à être consulté publiquement de manière inattendue.

Impact:S3/AnomalousBehavior.Write

Une entité IAM a invoqué une API S3 qui tente d'écrire des données de manière suspecte.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous indique qu'une entité IAM de votre AWS environnement effectue des appels d'API impliquant un compartiment S3, et que ce comportement est différent de la base de référence établie pour cette entité. L'appel d'API utilisé dans cette activité est associé à une attaque qui tente d'écrire des données. Cette activité est suspecte, car la l'entité IAM a invoqué l'API de façon inhabituelle. Par exemple, une entité IAM sans historique appelle une API S3, ou une entité IAM invoque une API S3 depuis un emplacement inhabituel.

Cette API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection d'anomalies. Le modèle de ML évalue toutes les demandes d'API dans votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il suit différents facteurs liés aux demandes d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande, l'API spécifique demandée, le compartiment demandé et le nombre d'appels d'API effectués. Pour plus d'informations sur les facteurs de la demande d'API qui sont inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande, veuillez consulter Détails du résultat.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

Nous recommandons un audit du contenu de votre compartiment S3 pour vous assurer que cet appel d'API n'a pas écrit de données malveillantes ou non autorisées.

Impact:S3/MaliciousIPCaller

Une API S3 couramment utilisée pour altérer des données ou des processus dans un AWS environnement a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3 a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques d'impact dans le cadre desquelles un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre AWS environnement. Exemples : `PutObject` et `PutObjectAcl`.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

PenTest:S3/KaliLinux

Une API S3 a été invoquée par une machine Kali Linux.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous indique qu'une machine exécutant Kali Linux effectue des appels à l'API S3 en utilisant les informations d'identification qui appartiennent à votre AWS compte. Vos informations d'identification pourraient être compromises. Kali Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses de configuration EC2 et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

PenTest:S3/ParrotLinux

Une API S3 a été invoquée par une machine Parrot Security Linux.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous indique qu'une machine exécutant Parrot Security Linux passe des appels à l'API S3 en utilisant les informations d'identification qui appartiennent à votre AWS compte. Vos informations d'identification pourraient être compromises. Parrot Security Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les pirates utilisent également cet outil pour identifier les faiblesses de la configuration EC2 et accéder à votre environnement AWS sans y être autorisés.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

PenTest:S3/PentooLinux

Une API S3 a été invoquée par une machine Pentoo Linux.

Gravité par défaut : moyenne

- Source de données : événements de CloudTrail données pour S3

Cette découverte vous indique qu'une machine exécutant Pentoo Linux passe des appels à l'API S3 en utilisant les informations d'identification qui appartiennent à votre AWS compte. Vos informations d'identification pourraient être compromises. Pentoo Linux est un outil de test d'intrusion populaire que des professionnels de la sécurité utilisent pour identifier les faiblesses des instances EC2 qui nécessitent l'application de correctifs. Les attaquants utilisent également cet outil pour détecter les faiblesses de configuration EC2 et obtenir un accès non autorisé à votre AWS environnement.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

Policy:S3/AccountBlockPublicAccessDisabled

Une entité IAM a invoqué une API utilisée pour désactiver le blocage de l'accès public S3 sur un compte.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que le blocage de l'accès public Amazon S3 a été désactivé au niveau du compte. Lorsque les paramètres de blocage de l'accès public S3 sont activés, ils sont utilisés pour filtrer les stratégies ou les listes de contrôle d'accès (ACL) sur les compartiments en tant que mesure de sécurité afin d'empêcher l'exposition publique accidentelle des données.

Généralement, le blocage de l'accès public S3 est désactivé dans un compte pour autoriser l'accès public à un compartiment ou aux objets du compartiment. Lorsque le blocage de l'accès public S3 est désactivé pour un compte, l'accès à vos compartiments est contrôlé par les stratégies, les ACL ou les paramètres de blocage de l'accès public au niveau du compartiment appliqués à vos compartiments individuels. Cela ne signifie pas nécessairement que les compartiments sont partagés publiquement,

mais que vous devez auditer les autorisations appliquées aux compartiments pour confirmer qu'elles fournissent le niveau d'accès approprié.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Policy:S3/BucketAnonymousAccessGranted

Un principal IAM a accordé l'accès à un compartiment S3 à Internet en modifiant les stratégies de compartiment ou les ACL.

Gravité par défaut : élevée

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que le compartiment S3 répertorié a été rendu public sur Internet, car une entité IAM a modifié une stratégie de compartiment ou une ACL sur ce compartiment. Après la détection d'un changement de stratégie ou d'ACL, il utilise un raisonnement automatisé basé sur Zelkova pour déterminer si le compartiment est accessible au public.

> **Note**
>
> Si les ACL ou les stratégies de compartiment d'un compartiment sont configurées pour tout refuser ou refuser explicitement, ce résultat peut ne pas refléter l'état actuel du compartiment. Ce résultat ne reflétera aucun paramètre de blocage de l'accès public S3 qui aurait pu être activé pour votre compartiment S3. Dans de tels cas, la valeur `effectivePermission` du résultat sera marquée comme `UNKNOWN`.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Policy:S3/BucketBlockPublicAccessDisabled

Une entité IAM a invoqué une API utilisée pour désactiver le blocage de l'accès public S3 sur un compartiment.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe que le blocage de l'accès public a été désactivé pour le compartiment S3 répertorié. Lorsque les paramètres de blocage de l'accès public S3 sont activés, ils sont utilisés pour filtrer les stratégies ou les listes de contrôle d'accès (ACL) appliquées aux compartiments en tant que mesure de sécurité afin d'empêcher l'exposition publique accidentelle des données.

Généralement, le blocage de l'accès public S3 est désactivé sur un compartiment pour autoriser l'accès public au compartiment ou aux objets qu'il contient. Lorsque le blocage de l'accès public S3 est désactivé pour un compartiment, les stratégies ou listes ACL appliquées au compartiment en contrôlent l'accès. Cela ne signifie pas que le compartiment est partagé publiquement, mais vous devez auditer les stratégies et les listes ACL appliquées au compartiment pour confirmer que les autorisations appropriées sont appliquées.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

Policy:S3/BucketPublicAccessGranted

Un directeur IAM a accordé l'accès public à un compartiment S3 à tous les AWS utilisateurs en modifiant les politiques de compartiment ou les ACL.

Gravité par défaut : élevée

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique que le compartiment S3 répertorié a été exposé publiquement à tous les AWS utilisateurs authentifiés car une entité IAM a modifié une politique de compartiment ou une

ACL sur ce compartiment S3. Après la détection d'un changement de stratégie ou d'ACL, il utilise un raisonnement automatisé basé sur Zelkova pour déterminer si le compartiment est accessible au public.

> **Note**
>
> Si les ACL ou les stratégies de compartiment d'un compartiment sont configurées pour tout refuser ou refuser explicitement, ce résultat peut ne pas refléter l'état actuel du compartiment. Ce résultat ne reflétera aucun paramètre de blocage de l'accès public S3 qui aurait pu être activé pour votre compartiment S3. Dans de tels cas, la valeur `effectivePermission` du résultat sera marquée comme `UNKNOWN`.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, consultez Corriger un compartiment S3 potentiellement compromis.

Stealth:S3/ServerAccessLoggingDisabled

La journalisation des accès au serveur S3 a été désactivée pour un compartiment.

Gravité par défaut : faible

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique que la journalisation des accès au serveur S3 est désactivée pour un compartiment de votre AWS environnement. Si cette option est désactivée, aucun journal des requêtes Web n'est créé pour les tentatives d'accès au compartiment S3 identifié. Toutefois, les appels de l'API de gestion S3 au compartiment, tels que DeleteBucket, sont toujours suivis. Si la journalisation des événements de données S3 est activée CloudTrail pour ce compartiment, les demandes Web relatives aux objets du compartiment seront toujours suivies. La désactivation de la journalisation est une technique utilisée par des utilisateurs non autorisés pour éviter la détection. Pour en savoir plus sur les journaux S3, veuillez consulter Journalisation des accès au serveur S3 et Options de journalisation S3 (langue française non garantie).

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Une API S3 a été invoquée depuis une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3, comme `PutObject` ou `PutObjectAcl`, a été invoquée depuis une adresse IP figurant sur une liste de menaces que vous avez chargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d’informations, consultez Corriger un compartiment S3 potentiellement compromis.

UnauthorizedAccess:S3/TorIPCaller

Une API S3 a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : élevée

- Source de données : événements de CloudTrail données pour S3

Ce résultat vous informe qu'une opération d'API S3, comme `PutObject` ou `PutObjectAcl`, a été invoquée depuis une adresse IP du nœud de sortie Tor. Tor est un logiciel permettant d'activer

les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cette découverte peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour plus d'informations, voir Corriger un compartiment S3 potentiellement compromis.

EKStypes de recherche de journaux d'audit

Les résultats suivants sont propres aux ressources Kubernetes et ont toujours un type de ressource `EKSCluster`. La gravité et les détails des résultats diffèrent selon le type de résultat.

Pour tous les résultats de type Kubernetes, nous vous recommandons d'examiner la ressource en question afin de déterminer si l'activité est attendue ou potentiellement malveillante. Pour obtenir des conseils sur la correction d'une ressource Kubernetes compromise identifiée par une GuardDuty découverte, consultez. Correction des résultats de la surveillance des journaux d'audit EKS

> **Note**
>
> Si l'activité à l'origine de ces résultats est attendue, envisagez d'ajouter Règles de suppression pour éviter de futures alertes.

Rubriques

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Avant la version 1.14 de Kubernetes, le `system:unauthenticated` groupe était associé à `system:discovery` et par défaut. `system:basic-user` ClusterRoles Cette association peut autoriser un accès involontaire de la part d'utilisateurs anonymes. Les mises à jour du cluster ne révoquent pas ces autorisations. Même si vous avez mis à jour votre cluster vers la version 1.14 ou ultérieure, ces autorisations peuvent toujours être activées. Nous vous recommandons de dissocier ces autorisations du groupe `system:unauthenticated`. Pour obtenir des conseils sur la révocation de ces autorisations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon.

CredentialAccess:Kubernetes/MaliciousIPCaller

Un code API couramment utilisé pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. Ce qui est API observé est généralement associé aux tactiques d'accès aux informations d'identification dans le cadre desquelles un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Un code API couramment utilisé pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoqué à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP figurant sur une liste de menaces que vous avez téléchargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. Ce qui est API observé est généralement associé aux tactiques d'accès aux informations d'identification dans le cadre desquelles un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer le API et et à révoquer les autorisations, le cas échéant, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Une méthode API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été correctement invoquée par l'`system:anonymous`utilisateur. APIles appels effectués par `system:anonymous` ne sont pas authentifiés. Ce qui API est observé est généralement associé aux tactiques d'accès aux informations d'identification dans le cadre desquelles un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'APIaction signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler toute modification apportée par un adversaire à votre cluster. Pour plus d'informations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de EKS l'utilisateur Amazon.

Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/TorIPCaller

Une méthode API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Cette découverte vous indique qu'un API a été invoqué depuis l'adresse IP d'un nœud de sortie Tor. Ce qui est API observé est généralement associé aux tactiques d'accès aux informations d'identification dans le cadre desquelles un adversaire tente de collecter des mots de passe, des noms d'utilisateur et des clés d'accès pour votre cluster Kubernetes. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire

à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à vos ressources de cluster Kubernetes dans le but de masquer la véritable identité du pirate.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Un moyen API couramment utilisé pour échapper aux mesures défensives a été invoqué à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. Ce qui est API observé est généralement associé à des tactiques d'évasion défensive où un adversaire tente de cacher ses actions pour éviter d'être détecté.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Une méthode API couramment utilisée pour contourner les mesures défensives a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP figurant sur une liste de menaces que vous avez téléchargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. Ce qui est API observé est généralement associé à des tactiques d'évasion défensive où un adversaire tente de cacher ses actions pour éviter d'être détecté.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Une méthode API couramment utilisée pour contourner les mesures défensives a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été correctement invoquée par l'`system:anonymous`utilisateur. APIles appels effectués par `system:anonymous` ne sont pas

authentifiés. Ce qui API est observé est généralement associé à des tactiques d'évasion défensive où un adversaire tente de cacher ses actions pour éviter d'être détecté. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'APIaction signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler toute modification apportée par un adversaire à votre cluster. Pour plus d'informations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de EKS l'utilisateur Amazon.

Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/TorIPCaller

Une méthode API couramment utilisée pour contourner les mesures défensives a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Cette découverte vous indique qu'un API a été invoqué depuis l'adresse IP d'un nœud de sortie Tor. Ce qui est API observé est généralement associé à des tactiques d'évasion défensive où un adversaire tente de cacher ses actions pour éviter d'être détecté. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à votre cluster Kubernetes dans le but de masquer la véritable identité de l'adversaire.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer

les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/MaliciousIPCaller

Un outil API couramment utilisé pour découvrir des ressources dans un cluster Kubernetes a été invoqué à partir d'une adresse IP.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'observation API est couramment utilisée lors de la phase de découverte d'une attaque au cours de laquelle un attaquant collecte des informations pour déterminer si votre cluster Kubernetes est vulnérable à une attaque de plus grande envergure.

> **Pour un accès non authentifié**
>
> MaliciousIPCallerles résultats ne sont pas générés pour un accès non authentifié. SuccessfulAnonymousAccessles résultats sont générés pour un accès anonyme ou non authentifié.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire

à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Un outil API couramment utilisé pour découvrir des ressources dans un cluster Kubernetes a été invoqué à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'un API a été invoqué à partir d'une adresse IP figurant sur une liste de menaces que vous avez téléchargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. L'observation API est couramment utilisée lors de la phase de découverte d'une attaque au cours de laquelle un attaquant collecte des informations pour déterminer si votre cluster Kubernetes est vulnérable à une attaque de plus grande envergure.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Un outil API couramment utilisé pour découvrir des ressources dans un cluster Kubernetes a été invoqué par un utilisateur non authentifié.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été correctement invoquée par l'`system:anonymous`utilisateur. APIles appels effectués par `system:anonymous` ne sont pas authentifiés. L'observation API est généralement associée à la phase de découverte d'une attaque lorsqu'un adversaire collecte des informations sur votre cluster Kubernetes. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'APIaction signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Ce type de recherche exclut les API points de terminaison du bilan de santé tels que `/healthz/livez`,`/readyz`, et`/version`.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler toute modification apportée par un adversaire à votre cluster. Pour plus d'informations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de EKS l'utilisateur Amazon.

Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/TorIPCaller

Une méthode API couramment utilisée pour découvrir des ressources dans un cluster Kubernetes a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Cette découverte vous indique qu'un API a été invoqué depuis l'adresse IP d'un nœud de sortie Tor. L'observation API est couramment utilisée lors de la phase de découverte d'une attaque au

cours de laquelle un attaquant collecte des informations pour déterminer si votre cluster Kubernetes est vulnérable à une attaque de plus grande envergure. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à votre cluster Kubernetes dans le but de masquer la véritable identité de l'adversaire.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer la APIand révocation des autorisations, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Execution:Kubernetes/ExecInKubeSystemPod

Une commande a été exécutée dans un pod au sein de l'espace de noms **`kube-system`**.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Cette découverte vous indique qu'une commande a été exécutée dans un pod au sein de l'espace de `kube-system` noms à l'aide de Kubernetes exec. API `kube-system`l'espace de noms est un espace de noms par défaut, principalement utilisé pour les composants au niveau du système tels que `kube-dns` et. `kube-proxy` Il est très rare d'exécuter des commandes dans des pods ou des conteneurs situés sous un espace de noms `kube-system`, ce qui peut indiquer une activité suspecte.

Recommandations de correction :

Si l'exécution de cette commande est inattendue, les informations d'identification de l'utilisateur utilisées pour exécuter la commande peuvent être compromises. Révoquez l'accès de l'utilisateur

et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/MaliciousIPCaller

Une méthode API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'observation API est généralement associée à des tactiques d'impact dans le cadre desquelles un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre AWS environnement.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

Une méthode API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP figurant sur une liste de menaces que vous avez téléchargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. L'observation API est généralement associée à des tactiques d'impact dans le cadre desquelles un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre AWS environnement.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

Un outil API couramment utilisé pour altérer les ressources d'un cluster Kubernetes a été invoqué par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été correctement invoquée par l'`system:anonymous`utilisateur. APIles appels effectués par `system:anonymous` ne sont pas authentifiés. L'observation API est généralement associée à la phase d'impact d'une attaque lorsqu'un adversaire altère les ressources de votre cluster. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'APIaction signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été

accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler toute modification apportée par un adversaire à votre cluster. Pour plus d'informations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de EKS l'utilisateur Amazon.

Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/TorIPCaller

Une méthode API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Cette découverte vous indique qu'un API a été invoqué depuis l'adresse IP d'un nœud de sortie Tor. L'APIobservation est généralement associée à des tactiques d'impact dans le cadre desquelles un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre AWS environnement. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé à votre cluster Kubernetes dans le but de masquer la véritable identité de l'adversaire.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Persistence:Kubernetes/ContainerWithSensitiveMount

Un conteneur a été lancé avec un chemin d'accès de l'hôte externe sensible monté à l'intérieur.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe qu'un conteneur a été lancé avec une configuration incluant un chemin d'accès de l'hôte sensible avec accès en écriture dans la section `volumeMounts`. Cela rend le chemin d'accès de l'hôte sensible accessible et inscriptible depuis l'intérieur du conteneur. Cette technique est couramment utilisée par des adversaires pour accéder au système de fichiers de l'hôte.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent être compromises. Révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression composée de critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit être identique au `imagePrefix` spécifié dans le résultat. Pour de plus amples informations sur la création de règles de suppression, veuillez consulter Règles de suppression (langue française non garantie).

Persistence:Kubernetes/MaliciousIPCaller

Une méthode API couramment utilisée pour obtenir un accès permanent à un cluster Kubernetes a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. Ce qui est API observé est généralement associé à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de conserver cet accès.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Une méthode API couramment utilisée pour obtenir un accès permanent à un cluster Kubernetes a été invoquée à partir d'une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été invoquée à partir d'une adresse IP figurant sur une liste de menaces que vous avez téléchargée. La liste des menaces associée à ce résultat est répertoriée dans la section Informations supplémentaires des détails d'un résultat. Ce qui est API observé est généralement associé à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de conserver cet accès.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il

s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Une méthode API couramment utilisée pour obtenir des autorisations de haut niveau sur un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération a été correctement invoquée par l'`system:anonymous`utilisateur. APIles appels effectués par `system:anonymous` ne sont pas authentifiés. Ce qui API est observé est généralement associé aux tactiques de persistance selon lesquelles un adversaire a obtenu l'accès à votre cluster et tente de conserver cet accès. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'APIaction signalée dans le résultat et peut être autorisé sur d'autres actions. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` sur votre cluster et vous assurer que toutes les autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, vous devez révoquer l'accès de l'utilisateur et annuler toute modification apportée par un adversaire à votre cluster. Pour plus d'informations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de EKS l'utilisateur Amazon.

Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Persistence:Kubernetes/TorIPCaller

Une méthode API couramment utilisée pour obtenir un accès permanent à un cluster Kubernetes a été invoquée à partir de l'adresse IP d'un nœud de sortie Tor.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Cette découverte vous indique qu'un API a été invoqué depuis l'adresse IP d'un nœud de sortie Tor. Ce qui est API observé est généralement associé à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de conserver cet accès. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

Recommandations de correction :

Si l'utilisateur indiqué dans le résultat de la `KubernetesUserDetails` section l'est`system:anonymous`, déterminez pourquoi l'utilisateur anonyme a été autorisé à invoquer les autorisations API et à les révoquer, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'EKSutilisateur Amazon. S'il s'agit d'un utilisateur authentifié, vérifiez si l'activité était légitime ou malveillante. Si l'activité était malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Le compte de service par défaut a reçu des privilèges d'administrateur sur un cluster Kubernetes.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe que le compte de service par défaut pour un espace de noms de votre cluster Kubernetes a reçu des privilèges d'administrateur. Kubernetes crée un compte de service par défaut pour tous les espaces de noms du cluster. Il attribue automatiquement le compte de service par défaut en tant qu'identité aux pods qui n'ont pas été explicitement associés à un autre compte

de service. Si le compte de service par défaut possède des privilèges d'administrateur, des pods peuvent être lancés involontairement avec des privilèges d'administrateur. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous ne devez pas utiliser le compte de service par défaut pour accorder des autorisations aux pods. Vous devez plutôt créer un compte de service dédié pour chaque charge de travail et accorder l'autorisation à ce compte en fonction des besoins. Pour résoudre ce problème, vous devez créer des comptes de service dédiés pour tous vos pods et charges de travail et mettre à jour les pods et les charges de travail afin d'effectuer une migration du compte de service par défaut vers leurs comptes dédiés. Vous devez ensuite supprimer l'autorisation d'administrateur du compte de service par défaut. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Policy:Kubernetes/AnonymousAccessGranted

L'**`system:anonymous`**utilisateur a obtenu l'APIautorisation d'accéder à un cluster Kubernetes.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe qu'un utilisateur de votre cluster Kubernetes est parvenu à créer une `ClusterRoleBinding` ou une `RoleBinding` pour lier l'utilisateur à un rôle `system:anonymous`. Cela permet un accès non authentifié aux API opérations autorisées par le rôle. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

Recommandations de correction :

Vous devez examiner les autorisations accordées à l'utilisateur `system:anonymous` ou au groupe `system:unauthenticated` de votre cluster et révoquer les accès anonymes inutiles. Pour plus d'informations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de EKS l'utilisateur Amazon. Si les autorisations ont été accordées de manière malveillante, vous devez révoquer l'accès de l'utilisateur qui les a accordées et annuler toute modification apportée par

un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Policy:Kubernetes/ExposedDashboard

Le tableau de bord d'un cluster Kubernetes a été exposé sur Internet

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe que le tableau de bord Kubernetes de votre cluster a été exposé sur Internet par un service d'équilibreur de charge. Un tableau de bord exposé permet d'accéder à l'interface de gestion de votre cluster depuis Internet et permet aux adversaires d'exploiter les éventuelles failles d'authentification et de contrôle d'accès.

Recommandations de correction :

Vous devez vous assurer que l'authentification et l'autorisation fortes sont appliquées sur le tableau de bord Kubernetes. Vous devez également implémenter le contrôle d'accès au réseau pour restreindre l'accès au tableau de bord à partir d'adresses IP spécifiques.

Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Policy:Kubernetes/KubeflowDashboardExposed

Le tableau de bord Kubeflow d'un cluster Kubernetes a été exposé sur Internet

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe que le tableau de bord Kubeflow de votre cluster a été exposé sur Internet par un service d'équilibreur de charge. Un tableau de bord Kubeflow exposé permet d'accéder à l'interface de gestion de votre environnement Kubeflow depuis Internet et permet aux adversaires d'exploiter les éventuelles failles d'authentification et de contrôle d'accès.

Recommandations de correction :

Vous devez vous assurer que l'authentification et l'autorisation fortes sont appliquées sur le tableau de bord Kubeflow. Vous devez également implémenter le contrôle d'accès au réseau pour restreindre l'accès au tableau de bord à partir d'adresses IP spécifiques.

Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Un conteneur privilégié avec accès au niveau racine a été lancé sur votre cluster Kubernetes.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe qu'un conteneur privilégié a été lancé sur votre cluster Kubernetes à l'aide d'une image qui n'a jamais été utilisée auparavant pour lancer des conteneurs privilégiés dans votre cluster. Un conteneur privilégié dispose d'un accès au niveau racine à l'hôte. Les adversaires peuvent lancer des conteneurs privilégiés comme tactique d'escalade des privilèges pour accéder à l'hôte puis le compromettre.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent être compromises. Révoquez l'accès de l'utilisateur et annulez les modifications apportées par un adversaire à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Un Kubernetes API couramment utilisé pour accéder aux secrets a été invoqué de manière anormale.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération anormale visant à récupérer des secrets de cluster sensibles a été invoquée par un utilisateur Kubernetes de votre cluster. Ce qui API est observé est généralement associé à des tactiques d'accès aux informations d'identification qui peuvent entraîner une escalade des privilèges et un accès accru au sein de votre cluster. Si ce comportement n'est pas attendu, cela peut indiquer soit une erreur de configuration, soit le fait que vos AWS informations d'identification sont compromises.

L'observation API a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle ML évalue toutes les API activités des utilisateurs au sein de votre EKS cluster et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle ML suit plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'agent utilisateur utilisé et l'espace de noms utilisé par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations accordées à l'utilisateur Kubernetes dans votre cluster et assurez-vous que toutes ces autorisations sont nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Un rôle trop permissif RoleBinding ou ClusterRoleBinding un espace de noms sensible ont été créés ou modifiés dans votre cluster Kubernetes.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si un RoleBinding ou ClusterRoleBinding implique le ClusterRoles `admin` ou`cluster-admin`, la gravité est élevée.

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe qu'un utilisateur de votre cluster Kubernetes a créé une `RoleBinding` ou une `ClusterRoleBinding` pour lier un utilisateur à un rôle avec des autorisations d'administrateur ou des espaces de noms sensibles. Si ce comportement n'est pas attendu, cela peut indiquer soit une erreur de configuration, soit le fait que vos AWS informations d'identification sont compromises.

L'observation API a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle ML évalue toutes les API activités des utilisateurs au sein de votre EKS cluster. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle ML suit également plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'agent utilisateur utilisé et l'espace de noms utilisé par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations accordées à l'utilisateur Kubernetes. Ces autorisations sont définies dans le rôle et les sujets concernés dans `RoleBinding` et `ClusterRoleBinding`. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Une commande a été exécutée à l'intérieur d'un pod de manière anormale.

Gravité par défaut : moyenne

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une commande a été exécutée dans un pod à l'aide de l'exec Kubernetes. API L'exec Kubernetes API permet d'exécuter des commandes arbitraires dans un

pod. Si ce comportement n'est pas attendu pour l'utilisateur, l'espace de noms ou le pod, cela peut indiquer une erreur de configuration ou que vos AWS informations d'identification sont compromises.

L'observation API a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle ML évalue toutes les API activités des utilisateurs au sein de votre EKS cluster. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle ML suit également plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'agent utilisateur utilisé et l'espace de noms utilisé par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si l'exécution de cette commande est inattendue, les informations d'identification de l'utilisateur utilisées pour exécuter la commande peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Une charge de travail a été lancée avec un conteneur privilégié de manière anormale.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une charge de travail a été lancée avec un conteneur privilégié dans votre EKS cluster Amazon. Un conteneur privilégié dispose d'un accès au niveau racine à l'hôte. Les utilisateurs non autorisés peuvent lancer des conteneurs privilégiés comme tactique d'escalade des privilèges pour d'abord accéder à l'hôte, puis le compromettre.

La création ou la modification du conteneur observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle ML

évalue toutes les activités des utilisateurs API et des images de conteneurs au sein de votre EKS cluster. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle ML suit également plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'agent utilisateur utilisé, les images du conteneur observées dans votre compte et l'espace de noms géré par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression avec des critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit avoir la même valeur que le champ `imagePrefix` spécifié dans le résultat. Pour de plus amples informations, veuillez consulter Règles de suppression.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Une charge de travail a été déployée de manière anormale, avec un chemin d'accès de l'hôte sensible installé à l'intérieur de la charge de travail.

Gravité par défaut : élevée

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe qu'une charge de travail a été lancée avec un conteneur qui incluait un chemin d'accès de l'hôte sensible dans la section `volumeMounts`. Cela rend potentiellement le chemin d'accès de l'hôte sensible accessible et inscriptible depuis l'intérieur du conteneur. Cette

technique est couramment utilisée par des utilisateurs non autorisés pour accéder au système de fichiers de l'hôte.

La création ou la modification du conteneur observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle ML évalue toutes les activités des utilisateurs API et des images de conteneurs au sein de votre EKS cluster. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle ML suit également plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'agent utilisateur utilisé, les images du conteneur observées dans votre compte et l'espace de noms géré par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression avec des critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit avoir la même valeur que le champ `imagePrefix` spécifié dans le résultat. Pour de plus amples informations, veuillez consulter Règles de suppression.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Une charge de travail a été lancée de manière anormale.

Gravité par défaut : faible*

> **Note**
>
> Le niveau de gravité par défaut est faible. Toutefois, si la charge de travail contient un nom d'image potentiellement suspect, tel qu'un outil pentest connu, ou si un conteneur exécute

une commande potentiellement suspecte au lancement, telle que des commandes shell inverses, le niveau de gravité de ce type de résultat sera considéré comme moyen.

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une charge de travail Kubernetes a été créée ou modifiée de manière anormale, par exemple une API activité, de nouvelles images de conteneur ou une configuration de charge de travail risquée, au sein de votre cluster Amazon. EKS Les utilisateurs non autorisés peuvent lancer des conteneurs comme tactique pour exécuter du code arbitraire pour d'abord accéder à l'hôte, puis le compromettre.

La création ou la modification du conteneur observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection des GuardDuty anomalies. Le modèle ML évalue toutes les activités des utilisateurs API et des images de conteneurs au sein de votre EKS cluster. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle ML suit également plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'agent utilisateur utilisé, les images du conteneur observées dans votre compte et l'espace de noms géré par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Si ce lancement de conteneur est inattendu, les informations d'identification de l'utilisateur utilisées pour lancer le conteneur peuvent avoir été compromises. Révoquez l'accès de l'utilisateur et annulez toute modification apportée par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

Si ce lancement de conteneur est prévu, il est recommandé d'utiliser une règle de suppression avec des critères de filtre basés sur le champ `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Dans les critères de filtre, le champ `imagePrefix` doit avoir la même valeur que le champ

`imagePrefix` spécifié dans le résultat. Pour de plus amples informations, veuillez consulter Règles de suppression.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Rôle hautement permissif ou ClusterRole créé ou modifié de manière anormale.

Gravité par défaut : faible

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous indique qu'une API opération anormale visant à créer un `Role` ou `ClusterRole` avec des autorisations excessives a été déclenchée par un utilisateur Kubernetes de votre cluster Amazon. EKS Les acteurs peuvent utiliser la création de rôles avec de puissantes autorisations pour éviter d'utiliser des rôles intégrés de type administrateur et éviter d'être détectés. Les autorisations excessives peuvent entraîner une escalade des privilèges, l'exécution de code à distance et éventuellement le contrôle d'un espace de noms ou d'un cluster. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification sont compromises.

L'observation API a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle ML évalue toutes les API activités des utilisateurs au sein de votre EKS cluster Amazon et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle ML suit également plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'agent utilisateur utilisé, les images du conteneur observées dans votre compte et l'espace de noms géré par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations définies dans `Role` ou `ClusterRole` pour vous assurer que toutes les autorisations sont nécessaires et respectez le principe du moindre privilège. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un utilisateur a vérifié son autorisation d'accès de manière anormale.

Gravité par défaut : faible

- Fonctionnalité : journaux EKS d'audit

Ce résultat vous informe qu'un utilisateur de votre cluster Kubernetes est parvenu à vérifier si les puissantes autorisations connues pouvant entraîner une escalade des privilèges et l'exécution de code à distance sont autorisées ou non. Par exemple, une commande couramment utilisée pour vérifier les autorisations d'un utilisateur est `kubectl auth can-i`. Si ce comportement n'est pas prévu, cela peut indiquer une erreur de configuration ou que vos informations d'identification ont été compromises.

L'observation API a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle ML évalue toutes les API activités des utilisateurs au sein de votre EKS cluster Amazon et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle ML suit également plusieurs facteurs de l'APIopération, tels que l'utilisateur qui fait la demande, l'emplacement d'où la demande a été faite, l'autorisation vérifiée et l'espace de noms utilisé par l'utilisateur. Vous pouvez trouver les détails de la API demande qui sont inhabituels dans le panneau des détails de recherche de la GuardDuty console.

Recommandations de correction :

Examinez les autorisations accordées à l'utilisateur Kubernetes pour vous assurer qu'elles sont toutes nécessaires. Si les autorisations ont été accordées par erreur ou de manière malveillante, révoquez l'accès de l'utilisateur et annulez les modifications apportées par un utilisateur non autorisé à votre cluster. Pour de plus amples informations, veuillez consulter Correction des résultats de la surveillance des journaux d'audit EKS.

Si vos AWS informations d'identification sont compromises, consultezCorriger les informations d'identification potentiellement compromises AWS.

Types de recherche liés à la surveillance du temps

Amazon GuardDuty génère les résultats de surveillance du temps d'exécution suivants pour identifier les menaces potentielles en fonction du comportement au niveau du système d'exploitation des EC2 hôtes et des conteneurs Amazon dans vos EKS clusters Amazon, les charges de travail ECS Fargate et Amazon et les instances Amazon. EC2

> **Note**
>
> Les types de résultat de la surveillance d'exécution sont basés sur les journaux d'exécution collectés auprès des hôtes. Les journaux contiennent des champs tels que les chemins d'accès aux fichiers qui peuvent être contrôlés par un acteur malveillant. Ces champs sont également inclus dans les GuardDuty résultats pour fournir un contexte d'exécution. Lorsque vous traitez les résultats de Runtime Monitoring en dehors de GuardDuty la console, vous devez nettoyer les champs de recherche. Par exemple, vous pouvez HTML encoder les champs de recherche lorsque vous les affichez sur une page Web.

Rubriques

- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/SuspiciousShellCreated
- PrivilegeEscalation:Runtime/ElevationToRoot

CryptoCurrency:Runtime/BitcoinTool.B

Une EC2 instance ou un conteneur Amazon interroge une adresse IP associée à une activité liée aux cryptomonnaies.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou un conteneur dans votre AWS environnement interroge une adresse IP associée à une activité liée aux cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si vous utilisez cette EC2 instance ou un conteneur pour extraire ou gérer des cryptomonnaies, ou si l'un ou l'autre de ces éléments est impliqué d'une autre manière dans l'activité de la blockchain, le CryptoCurrency:Runtime/BitcoinTool.B résultat peut représenter l'activité attendue pour votre environnement. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère de filtre doit utiliser l'attribut Type de résultat avec la valeur `CryptoCurrency:Runtime/BitcoinTool.B`. Le deuxième critère de filtre doit être l'ID d'instance de l'instance ou l'ID d'image de conteneur du conteneur impliqué dans une activité liée à la cryptomonnaie ou à la blockchain. Pour de plus amples informations, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Backdoor:Runtime/C&CActivity.B

Une EC2 instance ou un conteneur Amazon interroge une adresse IP associée à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou un conteneur de votre AWS environnement interroge une adresse IP associée à un serveur de commande et de contrôle (C&C) connu. L'instance ou le conteneur répertorié est peut-être potentiellement compromis. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet qui peuvent inclure des serveursPCs, des appareils mobiles et des appareils connectés à Internet des objets infectés et contrôlés par un type courant de maliciel. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. En fonction de l'objectif et de la structure du botnet, le serveur C&C peut également émettre des commandes pour lancer une attaque par déni de service distribué ()DDoS.

> **Note**
>
> Si l'adresse IP demandée est liée à log4j, les champs du résultat associé incluront les valeurs suivantes :
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

UnauthorizedAccess:Runtime/TorRelay

Votre EC2 instance Amazon ou un conteneur établit des connexions à un réseau Tor en tant que relais Tor.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'une EC2 instance ou un conteneur de votre AWS environnement établit des connexions à un réseau Tor d'une manière qui suggère qu'il agit comme un relais Tor. Tor est un logiciel permettant d'activer les communications anonymes. Tor augmente l'anonymat de la communication en réacheminant le trafic potentiellement illicite du client d'un relais Tor à un autre.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

UnauthorizedAccess:Runtime/TorClient

Votre EC2 instance Amazon ou un conteneur établit des connexions avec un nœud Tor Guard ou Authority.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'une EC2 instance ou un conteneur de votre AWS environnement établit des connexions avec un nœud Tor Guard ou Authority. Tor est un logiciel permettant d'activer les communications anonymes. Les nœuds Tor Guards et Authority agissent en tant que passerelles initiales dans un réseau Tor. Ce trafic peut indiquer que cette EC2 instance ou le conteneur a été potentiellement compromis et agit en tant que client sur un réseau Tor. Cette découverte peut indiquer un accès non autorisé à vos AWS ressources dans le but de cacher la véritable identité de l'attaquant.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/BlackholeTraffic

Une EC2 instance ou un conteneur Amazon tente de communiquer avec l'adresse IP d'un hôte distant connu sous la forme d'un trou noir.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une EC2 instance répertoriée ou un conteneur de votre AWS environnement est peut-être compromis parce qu'il tente de communiquer avec l'adresse IP d'un trou noir (ou puits). Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire. Une adresse IP de trou noir désigne une machine hôte qui n'est pas en cours d'exécution ou une adresse à laquelle aucun hôte n'a été attribué.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DropPoint

Une EC2 instance ou un conteneur Amazon tente de communiquer avec l'adresse IP d'un hôte distant connu pour contenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une EC2 instance ou un conteneur de votre AWS environnement tente de communiquer avec l'adresse IP d'un hôte distant connu pour contenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Une EC2 instance ou un conteneur Amazon interroge un nom de domaine associé à une activité de cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou un conteneur de votre AWS environnement demande un nom de domaine associé au Bitcoin ou à une autre activité liée aux cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si vous utilisez cette EC2 instance ou ce conteneur pour extraire ou gérer des cryptomonnaies, ou si l'un ou l'autre de ces éléments est impliqué d'une autre manière dans l'activité de la blockchain, la

CryptoCurrency:Runtime/BitcoinTool.B!DNS découverte peut être une activité attendue pour votre environnement. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Le deuxième critère de filtre doit être l'ID d'instance de l'instance ou l'ID d'image de conteneur du conteneur impliqué dans une activité de cryptomonnaie ou de blockchain. Pour de plus amples informations, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Backdoor:Runtime/C&CActivity.B!DNS

Une EC2 instance ou un conteneur Amazon interroge un nom de domaine associé à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement interroge un nom de domaine associé à un serveur de commande et de contrôle (C&C) connu. L'EC2instance répertoriée ou le conteneur est peut-être compromis. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à InternetPCs, notamment des serveurs, des appareils mobiles et des appareils connectés à l'Internet des objets, infectés et contrôlés par un type courant de maliciel. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. En fonction de l'objectif et de la structure du botnet, le serveur C&C peut également émettre des commandes pour lancer une attaque par déni de service distribué ()DDoS.

> **Note**
>
> Si le nom de domaine demandé est lié à log4j, les champs du résultat associé incluront les valeurs suivantes :

- `service.additionalInfo.threatListName = Amazon`
- `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Pour tester le mode GuardDuty de génération de ce type de recherche, vous pouvez effectuer une DNS demande depuis votre instance (`dig`sous Linux ou `nslookup` Windows) par rapport à un domaine de test`guarddutyc2activityb.com`.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/BlackholeTraffic!DNS

Une EC2 instance ou un conteneur Amazon interroge un nom de domaine qui est redirigé vers une adresse IP de trou noir.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement est peut-être compromis car il interroge un nom de domaine qui est redirigé vers une adresse IP de trou noir. Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DropPoint!DNS

Une EC2 instance ou un conteneur Amazon interroge le nom de domaine d'un hôte distant connu pour contenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une EC2 instance ou un conteneur de votre AWS environnement interroge le nom de domaine d'un hôte distant connu pour contenir des informations d'identification et d'autres données volées capturées par un logiciel malveillant.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DGADomainRequest.C!DNS

Une EC2 instance ou un conteneur Amazon interroge des domaines générés de manière algorithmique. Ces domaines sont couramment utilisés par les malwares et peuvent indiquer la compromission d'une EC2 instance ou d'un conteneur.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement essaie d'interroger les domaines de l'algorithme de génération de domaines (DGA). Votre ressource a peut-être été compromise.

DGAssont utilisés pour générer périodiquement un grand nombre de noms de domaine qui peuvent être utilisés comme points de rendez-vous avec leurs serveurs de commande et de contrôle (C&C). Les serveurs de commande et de contrôle sont des ordinateurs qui émettent des commandes aux membres d'un botnet, qui est un ensemble d'appareils connectés à Internet qui sont infectés et contrôlés par un type courant de programme malveillant. Le grand nombre de points de rendez-vous potentiels rend l'arrêt des botnets difficile, car les ordinateurs infectés tentent de contacter certains de ces noms de domaine chaque jour pour recevoir des mises à jour ou des commandes.

> **Note**
>
> Ce résultat est basé sur des DGA domaines connus issus de flux de renseignements sur les GuardDuty menaces.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DriveBySourceTraffic!DNS

Une EC2 instance ou un conteneur Amazon interroge le nom de domaine d'un hôte distant qui est une source connue d'attaques de téléchargement Drive-By.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement est peut-être compromis car il interroge le nom de domaine d'un hôte distant qui est une source

connue d'attaques de téléchargement au volant. Il s'agit de téléchargements involontaires de logiciels d'Internet qui peuvent initier l'installation automatique de virus, logiciels espions ou programmes malveillants.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/PhishingDomainRequest!DNS

Une EC2 instance ou un conteneur Amazon interroge des domaines impliqués dans des attaques de phishing.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une EC2 instance ou un conteneur de votre AWS environnement tente d'interroger un domaine impliqué dans des attaques de phishing. Les domaines de hameçonnage sont créés par des pirates se faisant passer pour une institution légitime afin de pousser des utilisateurs à fournir des données sensibles, telles que des informations personnelles identifiables, des coordonnées bancaires, des informations de carte bancaire ou des mots de passe. Votre EC2 instance ou le conteneur essaie peut-être de récupérer des données sensibles stockées sur un site Web de phishing, ou tente peut-être de configurer un site Web de phishing. Votre EC2 instance ou le conteneur est peut-être compromis.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/AbusedDomainRequest.Reputation

Une EC2 instance ou un conteneur Amazon interroge un nom de domaine de mauvaise réputation associé à des domaines connus pour être utilisés abusivement.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP connus pour être utilisés de manière abusive. Les noms de domaine de premier niveau (TLDs) et les noms de domaine de deuxième niveau (2LDs) fournissant des enregistrements de sous-domaines gratuits ainsi que les fournisseurs dynamiques DNS sont des exemples de domaines utilisés abusivement. Les acteurs de la menace ont tendance à utiliser ces services pour enregistrer des domaines gratuitement ou à faible coût. Les domaines de mauvaise réputation de cette catégorie peuvent également être des domaines expirés renvoyés à l'adresse IP de stationnement d'un bureau d'enregistrement et peuvent donc ne plus être actifs. Une adresse IP de stationnement est l'endroit où un bureau d'enregistrement dirige le trafic vers des domaines qui n'ont été liés à aucun service. L'EC2instance Amazon répertoriée ou le conteneur peuvent être compromis car les acteurs malveillants utilisent généralement ces bureaux d'enregistrement ou ces services pour la distribution de logiciels malveillants et de contrôle.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/BitcoinDomainRequest.Reputation

Une EC2 instance ou un conteneur Amazon interroge un nom de domaine de mauvaise réputation associé à une activité liée aux cryptomonnaies.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation associé à Bitcoin ou à une autre activité liée aux cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si vous utilisez cette EC2 instance ou le conteneur pour extraire ou gérer des cryptomonnaies, ou si ces ressources sont impliquées d'une autre manière dans l'activité de la blockchain, ce résultat peut représenter une activité attendue pour votre environnement. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère de filtre doit utiliser l'attribut Type de résultat avec la valeur `Impact:Runtime/BitcoinDomainRequest.Reputation`. Le deuxième critère de filtre doit être l'ID d'instance de l'instance ou l'ID d'image de conteneur du conteneur impliqué dans une activité liée à la cryptomonnaie ou à la blockchain. Pour de plus amples informations, veuillez consulter Règles de suppression.

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/MaliciousDomainRequest.Reputation

Une EC2 instance ou un conteneur Amazon interroge un domaine de mauvaise réputation associé à des domaines malveillants connus.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation associé à des domaines ou adresses IP malveillants connus. Par exemple, les domaines peuvent être associés à une adresse IP de gouffre connue. Les domaines de gouffre sont des domaines qui étaient auparavant contrôlés par un acteur menaçant, et les demandes qui leur sont adressées peuvent indiquer que l'instance est compromise. Ces domaines peuvent également être corrélés à des campagnes malveillantes ou à des algorithmes de génération de domaines connus.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Une EC2 instance ou un conteneur Amazon interroge un nom de domaine de mauvaise réputation qui est de nature suspecte en raison de son ancienneté ou de sa faible popularité.

Gravité par défaut : faible

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique que l'EC2instance répertoriée ou le conteneur de votre AWS environnement interroge un nom de domaine de mauvaise réputation soupçonné d'être malveillant. Nous avons remarqué des caractéristiques de ce domaine qui étaient cohérentes avec les domaines malveillants précédemment observés, mais notre modèle de réputation n'a pas pu le relier définitivement à une menace connue. Ces domaines sont généralement récemment observés ou reçoivent un faible trafic.

Les domaines de mauvaise réputation sont basés sur un modèle de score de réputation. Ce modèle évalue et classe les caractéristiques d'un domaine afin de déterminer sa probabilité d'être malveillant.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Une EC2 instance ou un conteneur Amazon effectue des DNS recherches qui concernent le service de métadonnées de l'instance.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

> **Note**
>
> Actuellement, ce type de recherche n'est pris en charge que pour AMD64 l'architecture.

Ce résultat vous indique qu'une EC2 instance ou un conteneur de votre AWS environnement interroge un domaine qui correspond à l'adresse IP des EC2 métadonnées (169.254.169.254). Une DNS requête de ce type peut indiquer que l'instance est la cible d'une technique de DNS reliaison. Cette technique peut être utilisée pour obtenir des métadonnées d'une EC2 instance, y compris les IAM informations d'identification associées à l'instance.

DNSla reliaison consiste à inciter une application exécutée sur l'EC2instance à charger les données de retour depuis unURL, où le nom de domaine indiqué correspond à l'URLadresse IP EC2 des métadonnées ()`169.254.169.254`. Cela permet à l'application d'accéder aux EC2 métadonnées et de les mettre éventuellement à la disposition de l'attaquant.

Il est possible d'accéder aux EC2 métadonnées à l'aide de la DNS reliaison uniquement si l'EC2instance exécute une application vulnérable qui autorise l'injection deURLs, ou si quelqu'un y accède URL dans un navigateur Web exécuté sur l'EC2instance.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

En réponse à cette constatation, vous devez évaluer si une application vulnérable est exécutée sur l'EC2instance ou sur le conteneur, ou si quelqu'un a utilisé un navigateur pour accéder au domaine identifié dans la constatation. Si la cause première est une application vulnérable, corrigez la vulnérabilité. Si une personne a navigué dans le domaine identifié, bloquez le domaine ou empêchez les utilisateurs d'y accéder. Si vous déterminez que cette constatation est liée à l'un des cas ci-dessus, révoquez la session associée à l'EC2instance.

Certains AWS clients associent intentionnellement l'adresse IP des métadonnées à un nom de domaine sur leurs DNS serveurs officiels. Si c'est le cas dans votre environnement , nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère de filtre doit utiliser l'attribut Type de résultat avec la valeur `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. Le deuxième critère de filtre doit être le domaine de DNS demande ou l'ID d'image du conteneur. La valeur du domaine de DNS demande doit correspondre au domaine que vous avez mappé à l'adresse IP des métadonnées (`169.254.169.254`). Pour plus d'informations sur la création de règles de suppression, veuillez consulter Règles de suppression (langue française non garantie).

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/NewBinaryExecuted

Un fichier binaire récemment créé ou modifié dans un conteneur a été exécuté.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe qu'un fichier binaire récemment créé ou modifié dans un conteneur a été exécuté. Il est recommandé de conserver les conteneurs immuables au moment de l'exécution, et les fichiers binaires, les scripts ou les bibliothèques ne doivent pas être créés ou modifiés pendant la durée de vie du conteneur. Ce comportement indique qu'un acteur malveillant a accédé au conteneur, a téléchargé et exécuté un logiciel malveillant ou un autre logiciel dans le cadre de la compromission potentielle. Bien que ce type d'activité puisse indiquer un compromis, il s'agit également d'un modèle d'utilisation courant. Par conséquent, GuardDuty utilise des mécanismes pour identifier les instances suspectes de cette activité et génère ce type de recherche uniquement pour les instances suspectes.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Un processus à l'intérieur d'un conteneur communique avec le démon Docker à l'aide du socket Docker.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Le socket Docker est un socket de domaine Unix que le démon Docker (`dockerd`) utilise pour communiquer avec ses clients. Un client peut effectuer diverses actions, telles que la création de conteneurs en communiquant avec le démon Docker via le socket Docker. Il est suspect qu'un processus de conteneur accède au socket Docker. Un processus de conteneur peut échapper au conteneur et obtenir un accès au niveau de l'hôte en communiquant avec le socket Docket et en créant un conteneur privilégié.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

PrivilegeEscalation:Runtime/RuncContainerEscape

Une tentative d'évasion du conteneur via RunC a été détectée.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

RunC est le runtime de conteneur de bas niveau que les environnements d'exécution de conteneurs de haut niveau, tels que Docker et Containerd, utilisent pour générer et exécuter des conteneurs. RunC est toujours exécuté avec les privilèges root car il doit effectuer la tâche de bas niveau consistant à créer un conteneur. Un acteur malveillant peut obtenir un accès au niveau de l'hôte en modifiant ou en exploitant une vulnérabilité dans le binaire RunC.

Cette découverte détecte la modification du binaire RunC et les tentatives potentielles d'exploitation des vulnérabilités RunC suivantes :

- CVE-2019-5736— L'exploitation de CVE-2019-5736 implique le remplacement du binaire RunC depuis un conteneur. Ce résultat est invoqué lorsque le binaire RunC est modifié par un processus à l'intérieur d'un conteneur.
- CVE-2024-21626— L'exploitation de CVE-2024-21626 implique de définir le répertoire de travail actuel (CWD) ou un conteneur sur un descripteur `/proc/self/fd/FileDescriptor` de fichier ouvert. Ce résultat est invoqué lorsqu'un processus de conteneur contenant un répertoire de travail actuel `/proc/self/fd/` est détecté, par exemple,`/proc/self/fd/7`.

Cette découverte peut indiquer qu'un acteur malveillant a tenté de procéder à une exploitation dans l'un des types de conteneurs suivants :

- Un nouveau conteneur avec une image contrôlée par un pirate.

- Un conteneur existant auquel l'acteur avait accès avec des autorisations d'écriture sur le binaire RunC au niveau de l'hôte.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Une tentative d'évasion du conteneur par le biais d'un agent CGroups de démoulage a été détectée.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe qu'une tentative de modification du fichier de l'agent de version d'un groupe de contrôle (cgroup) a été détectée. Linux utilise des groupes de contrôle (cgroups) pour limiter, prendre en compte et isoler l'utilisation des ressources d'un ensemble de processus. Chaque cgroup possède un fichier d'agent de version (`release_agent`), un script que Linux exécute lorsqu'un processus au sein du cgroup se termine. Le fichier de l'agent de version est toujours exécuté au niveau de l'hôte. Un acteur malveillant à l'intérieur d'un conteneur peut s'échapper vers l'hôte en écrivant des commandes arbitraires dans le fichier de l'agent de version qui appartient à un cgroup. Lorsqu'un processus à l'intérieur de ce cgroup se termine, les commandes écrites par l'acteur sont exécutées.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

DefenseEvasion:Runtime/ProcessInjection.Proc

Une injection de processus utilisant le système de fichiers proc a été détectée dans un conteneur ou une instance AmazonEC2.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

L'injection de processus est une technique utilisée par les acteurs malveillants pour injecter du code dans les processus afin d'échapper aux défenses et d'augmenter potentiellement les privilèges. Le système de fichiers proc (procfs) est un système de fichiers spécial sous Linux qui présente la mémoire virtuelle du processus sous forme de fichier. Le chemin de ce fichier est `/proc/PID/mem`, où `PID` est ID unique du processus. Un acteur malveillant peut écrire dans ce fichier pour injecter du code dans le processus. Ce résultat identifie les tentatives potentielles d'écriture dans ce fichier.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre type de ressource a peut-être été compromis. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Une injection de processus utilisant un appel système ptrace a été détectée dans un conteneur ou une EC2 instance Amazon.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

L'injection de processus est une technique utilisée par les acteurs malveillants pour injecter du code dans les processus afin d'échapper aux défenses et d'augmenter potentiellement les privilèges. Un

processus peut utiliser l'appel système ptrace pour injecter du code dans un autre processus. Ce résultat identifie une tentative potentielle d'injection de code dans un processus à l'aide de l'appel système ptrace.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre type de ressource a peut-être été compromis. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Une injection de processus via une écriture directe dans la mémoire virtuelle a été détectée dans un conteneur ou une EC2 instance Amazon.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

L'injection de processus est une technique utilisée par les acteurs malveillants pour injecter du code dans les processus afin d'échapper aux défenses et d'augmenter potentiellement les privilèges. Un processus peut utiliser un appel système, comme `process_vm_writev`, pour injecter directement du code dans la mémoire virtuelle d'un autre processus. Ce résultat identifie une tentative potentielle d'injection de code dans un processus à l'aide d'un appel système pour écrire dans la mémoire virtuelle du processus.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre type de ressource a peut-être été compromis. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/ReverseShell

Un processus dans un conteneur ou une EC2 instance Amazon a créé un shell inversé.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Un shell inversé est une session shell créée sur une connexion initiée entre l'hôte cible et l'hôte de l'acteur. C'est le contraire d'un shell normal initié depuis l'hôte de l'acteur vers l'hôte de la cible. Les acteurs malveillants créent un shell inversé pour exécuter des commandes sur la cible après avoir obtenu un accès initial à celle-ci. Ce résultat identifie une tentative potentielle de création d'un shell inverse.

Recommandations de correction :

Si cette activité est inattendue, votre type de ressource a peut-être été compromis.

DefenseEvasion:Runtime/FilelessExecution

Un processus dans un conteneur ou une EC2 instance Amazon exécute du code depuis la mémoire.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe lorsqu'un processus est exécuté à l'aide d'un fichier exécutable en mémoire sur le disque. Il s'agit d'une technique de contournement de la défense courante qui évite d'écrire le fichier exécutable malveillant sur le disque pour échapper à la détection basée sur l'analyse du système de fichiers. Bien que cette technique soit utilisée par des logiciels malveillants, elle présente également des cas d'utilisation légitimes. L'un des exemples est un compilateur just-in-time (JIT) qui écrit du code compilé en mémoire et l'exécute à partir de la mémoire.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/CryptoMinerExecuted

Un conteneur ou une EC2 instance Amazon exécute un fichier binaire associé à une activité d'extraction de cryptomonnaies.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un conteneur ou une EC2 instance de votre AWS environnement exécute un fichier binaire associé à une activité d'extraction de cryptomonnaies. Les acteurs malveillants peuvent chercher à prendre le contrôle des ressources de calcul afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

L'agent d'exécution surveille les événements provenant de plusieurs types de ressource. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans le panneau des résultats de la GuardDuty console.

Recommandations de correction :

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console et consultezCorriger les résultats de la surveillance de l'exécution.

Execution:Runtime/NewLibraryLoaded

Une bibliothèque récemment créée ou modifiée a été chargée par un processus à l'intérieur d'un conteneur.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat indique qu'une bibliothèque a été créée ou modifiée dans un conteneur pendant l'exécution et chargée par un processus exécuté dans le conteneur. Il est recommandé de conserver les conteneurs immuables au moment de l'exécution, et à ne pas créer ou modifier les fichiers binaires, les scripts ou les bibliothèques pendant la durée de vie du conteneur. Le chargement d'une bibliothèque récemment créée ou modifiée dans un conteneur peut indiquer une activité suspecte. Ce comportement indique qu'un acteur malveillant a potentiellement accédé au conteneur, a téléchargé et exécuté un logiciel malveillant ou un autre logiciel dans le cadre de la compromission potentielle. Bien que ce type d'activité puisse indiquer un compromis, il s'agit également d'un modèle d'utilisation courant. Par conséquent, GuardDuty utilise des mécanismes pour identifier les instances suspectes de cette activité et génère ce type de recherche uniquement pour les instances suspectes.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un processus à l'intérieur d'un conteneur a monté un système de fichiers hôte au moment de l'exécution.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Plusieurs techniques de fuite de conteneur impliquent le montage d'un système de fichiers hôte dans un conteneur lors de l'exécution. Ce résultat indique qu'un processus à l'intérieur d'un conteneur a potentiellement tenté de monter un système de fichiers hôte, ce qui peut indiquer une tentative de fuite vers l'hôte.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Un processus utilisait des appels système **`userfaultfd`** pour traiter les défauts de page dans l'espace utilisateur.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Généralement, les erreurs de page sont gérées par le noyau dans l'espace du noyau. Cependant, l'appel système `userfaultfd` permet à un processus de gérer les erreurs de page sur un système de fichiers dans l'espace utilisateur. Il s'agit d'une fonctionnalité utile qui permet d'implémenter des systèmes de fichiers de l'espace utilisateur. D'autre part, il peut également être utilisé par un processus potentiellement malveillant pour interrompre le noyau depuis l'espace utilisateur. L'interruption du noyau à l'aide d'un appel système `userfaultfd` est une technique d'exploitation courante pour étendre les fenêtres de course pendant l'exploitation des conditions de course du noyau. L'utilisation de `userfaultfd` peut indiquer une activité suspecte sur l'instance Amazon Elastic Compute Cloud (AmazonEC2).

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/SuspiciousTool

Un conteneur ou une EC2 instance Amazon exécute un fichier binaire ou un script fréquemment utilisé dans des scénarios de sécurité offensifs tels que le pentesting d'engagement.

Gravité par défaut : variable

La gravité de cette constatation peut être élevée ou faible, selon que l'outil suspect détecté est considéré comme étant à double usage ou s'il est exclusivement destiné à un usage offensif.

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'un outil suspect a été exécuté sur une EC2 instance ou un conteneur au sein de votre AWS environnement. Cela inclut les outils utilisés dans les missions de pentesting, également appelés outils de porte dérobée, scanners réseau et renifleurs de réseau. Tous ces outils peuvent être utilisés dans des contextes bénins, mais ils sont également fréquemment utilisés par des acteurs malveillants à des fins malveillantes. L'observation d'outils de sécurité offensifs peut indiquer que l'EC2instance ou le conteneur associé a été compromis.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/SuspiciousCommand

Une commande suspecte a été exécutée sur une EC2 instance Amazon ou un conteneur, ce qui indique une compromission.

Gravité par défaut : variable

En fonction de l'impact du schéma malveillant observé, la gravité de ce type de découverte peut être faible, moyenne ou élevée.

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une commande suspecte a été exécutée et qu'une EC2 instance Amazon ou un conteneur de votre AWS environnement a été compromis. Cela peut signifier qu'un fichier a été téléchargé depuis une source suspecte puis exécuté, ou qu'un processus en cours d'exécution affiche un schéma malveillant connu dans sa ligne de commande. Cela indique en outre qu'un logiciel malveillant est en cours d'exécution sur le système.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

DefenseEvasion:Runtime/SuspiciousCommand

Une commande a été exécutée sur l'EC2instance Amazon répertoriée ou sur un conteneur. Elle tente de modifier ou de désactiver un mécanisme de défense Linux, tel qu'un pare-feu ou des services système essentiels.

Gravité par défaut : variable

Selon le mécanisme de défense qui a été modifié ou désactivé, la gravité de ce type de découverte peut être élevée, moyenne ou faible.

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une commande visant à masquer une attaque aux services de sécurité du système local a été exécutée. Cela inclut des actions telles que la désactivation du pare-feu Unix, la modification des tables IP locales, la suppression d'crontabentrées, la désactivation d'un service local ou la prise en charge de la fonction. `LDPreload` Toute modification est hautement suspecte et constitue un indicateur potentiel de compromission. Par conséquent, ces mécanismes détectent ou empêchent toute nouvelle compromission du système.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

DefenseEvasion:Runtime/PtraceAntiDebugging

Un processus dans un conteneur ou une EC2 instance Amazon a exécuté une mesure anti-débogage à l'aide de l'appel système ptrace.

Gravité par défaut : faible

- Fonctionnalité : surveillance d'exécution

Ce résultat indique qu'un processus exécuté sur une EC2 instance Amazon ou un conteneur au sein de votre AWS environnement a utilisé l'appel système ptrace avec l'`PTRACE_TRACEME`option. Cette activité provoquerait le détachement d'un débogueur attaché du processus en cours d'exécution. Si aucun débogueur n'est attaché, cela n'a aucun effet. Cependant, l'activité en elle-même suscite des soupçons. Cela peut indiquer qu'un logiciel malveillant est en cours d'exécution sur le système. Les malwares utilisent fréquemment des techniques anti-débogage pour échapper à l'analyse, et ces techniques peuvent être détectées au moment de l'exécution.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/MaliciousFileExecuted

Un fichier exécutable malveillant connu a été exécuté sur une EC2 instance Amazon ou un conteneur.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'un exécutable malveillant connu a été exécuté sur une EC2 instance Amazon ou un conteneur au sein de votre AWS environnement. Cela indique clairement que l'instance ou le conteneur a été potentiellement compromis et qu'un logiciel malveillant a été exécuté.

Les malwares utilisent fréquemment des techniques anti-débogage pour échapper à l'analyse, et ces techniques peuvent être détectées au moment de l'exécution.

GuardDuty examine l'activité et le contexte d'exécution associés afin de générer ce résultat uniquement lorsque l'activité et le contexte associés sont potentiellement suspects.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/SuspiciousShellCreated

Un service réseau ou un processus accessible par le réseau sur une EC2 instance Amazon ou dans un conteneur a lancé un processus shell interactif.

Gravité par défaut : faible

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un service accessible par le réseau sur une EC2 instance Amazon ou dans un conteneur de votre AWS environnement a lancé un shell interactif. Dans certaines circonstances, ce scénario peut indiquer un comportement post-exploitation. Les shells interactifs permettent aux attaquants d'exécuter des commandes arbitraires sur une instance ou un conteneur compromis.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console. Vous pouvez consulter les informations du processus accessibles par le réseau dans les détails du processus parent.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

PrivilegeEscalation:Runtime/ElevationToRoot

Un processus exécuté sur l'EC2instance ou le conteneur Amazon répertorié a assumé les privilèges root.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un processus exécuté sur le site Amazon répertorié EC2 ou dans le conteneur répertorié au sein de votre AWS environnement a acquis les privilèges root à la suite d'une exécution `setuid` binaire inhabituelle ou suspecte. Cela indique qu'un processus en cours d'exécution a été potentiellement compromis, EC2 par exemple par un exploit ou par une `setuid` exploitation. En utilisant les privilèges root, l'attaquant peut potentiellement exécuter des commandes sur l'instance ou le conteneur.

Bien qu' GuardDuty il soit conçu pour ne pas générer ce type de constatation pour les activités impliquant une utilisation régulière de la `sudo` commande, il générera ce résultat lorsqu'il identifie l'activité comme inhabituelle ou suspecte.

GuardDuty examine l'activité et le contexte d'exécution associés, et génère ce type de recherche uniquement lorsque l'activité et le contexte associés sont inhabituels ou suspects.

L'agent d'exécution surveille les événements provenant de plusieurs ressources. Pour identifier la ressource affectée, consultez le type de ressource dans les détails des résultats de la GuardDuty console.

Recommandations de correction :

Si cette activité est inattendue, votre ressource a peut-être été compromise. Pour de plus amples informations, veuillez consulter Corriger les résultats de la surveillance de l'exécution.

Protection contre les programmes malveillants pour les types de détection EC2

GuardDuty Malware Protection for EC2 fournit une protection antimalware unique permettant à EC2 de détecter toutes les menaces détectées lors de l'analyse d'une instance EC2 ou d'une charge de travail de conteneur. Le résultat inclut le nombre total de détections effectuées pendant l'analyse et, en fonction de leur gravité, fournit des détails sur les 32 principales menaces détectées. Contrairement à d'autres GuardDuty résultats, les résultats de Malware Protection for EC2 ne sont pas mis à jour lorsque la même instance EC2 ou la même charge de travail de conteneur est à nouveau analysée.

Une nouvelle protection contre les programmes malveillants détectée par EC2 est générée pour chaque analyse qui détecte un logiciel malveillant. Les résultats de la protection contre les programmes malveillants pour EC2 incluent des informations sur le scan correspondant à l'origine du résultat ainsi que sur le GuardDuty résultat à l'origine de ce scan. Il est ainsi plus facile de corréler le comportement suspect avec le logiciel malveillant détecté.

> **Note**
>
> Lorsqu'une activité malveillante est GuardDuty détectée sur une charge de travail de conteneur, Malware Protection for EC2 ne génère aucun résultat de niveau EC2.

Les résultats suivants concernent spécifiquement la protection contre les GuardDuty logiciels malveillants pour EC2.

Rubriques

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile

- Execution:Kubernetes/MaliciousFile
- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

Un fichier malveillant a été détecté sur une instance EC2.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur l'instance EC2 répertoriée dans votre AWS environnement. Cette instance répertoriée est peut-être compromise. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Execution:ECS/MaliciousFile

Un fichier malveillant a été détecté sur un cluster ECS.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur un workload de conteneur appartenant à un cluster ECS. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est inattendue, votre conteneur appartenant au cluster ECS peut être compromis. Pour plus d'informations, consultez Corriger un cluster potentiellement compromis ECS.

Execution:Kubernetes/MaliciousFile

Un fichier malveillant a été détecté sur un cluster Kubernetes.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur un workload de conteneur appartenant à un cluster Kubernetes. S'il s'agit d'un cluster géré par EKS, les détails des résultats fourniront des informations supplémentaires sur la ressource EKS affectée. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Execution:Container/MaliciousFile

Un fichier malveillant a été détecté sur un conteneur autonome.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers malveillants sur un workload de conteneur et qu'aucune information sur le cluster n'a été identifiée. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour plus d’informations, consultez Corriger un conteneur autonome potentiellement compromis.

Execution:EC2/SuspiciousFile

Un fichier suspect a été détecté sur une instance EC2.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur une instance EC2. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type `SuspiciousFile` indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour plus d’informations, consultez Corriger une instance Amazon EC2 potentiellement compromise.

Execution:ECS/SuspiciousFile

Un fichier suspect a été détecté sur un cluster ECS.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur un conteneur appartenant à un cluster ECS. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type `SuspiciousFile` indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est inattendue, votre conteneur appartenant au cluster ECS peut être compromis. Pour plus d’informations, consultez Corriger un cluster potentiellement compromis ECS.

Execution:Kubernetes/SuspiciousFile

Un fichier suspect a été détecté sur un cluster Kubernetes.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur un conteneur appartenant à un cluster Kubernetes. S'il s'agit d'un cluster géré par EKS, les détails des résultats fourniront des informations supplémentaires sur le service EKS concerné. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type `SuspiciousFile` indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en

réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Execution:Container/SuspiciousFile

Un fichier suspect a été détecté sur un conteneur autonome.

Gravité par défaut : varie en fonction de la menace détectée.

- Fonctionnalité : Protection contre les logiciels malveillants EBS

Ce résultat indique que l'analyse GuardDuty Malware Protection for EC2 a détecté un ou plusieurs fichiers suspects sur un conteneur sans aucune information sur le cluster. Pour plus d'informations, veuillez consulter la section Menaces détectées dans le détail des résultats.

Les détections de type `SuspiciousFile` indiquent que des programmes potentiellement indésirables tels que des logiciels publicitaires, des logiciels espions ou des outils à double usage sont présents sur une ressource affectée. Ces programmes peuvent avoir un impact négatif sur vos ressources ou être utilisés par des pirates à des fins malveillantes. Par exemple, les outils de mise en réseau peuvent être utilisés de manière légitime ou malveillante par des adversaires comme outils de piratage pour tenter de compromettre des ressources.

Lorsqu'un fichier suspect est détecté, déterminez si vous vous attendez à voir le fichier détecté dans votre AWS environnement. Si le fichier est inattendu, suivez les recommandations décrites dans la section suivante.

Recommandations de correction :

Si cette activité est inattendue, la charge de travail de votre conteneur peut être compromise. Pour plus d'informations, voir Corriger un conteneur autonome potentiellement compromis.

Protection contre les programmes malveillants pour le type de recherche S3

GuardDuty génère un résultat uniquement lorsqu'il détecte une menace potentielle pour votre sécurité Compte AWS. Une détection de Malware Protection for S3 indique que l'objet chargé à l'origine de l'analyse des programmes malveillants contient un fichier potentiellement malveillant.

Pour GuardDuty qu'Amazon génère un résultat dans votre compte Compte AWS, activez à la fois la protection contre GuardDuty les logiciels malveillants pour S3. La meilleure pratique consiste d'abord à activer GuardDuty puis à activer la protection contre les programmes malveillants pour S3. Si cet ordre est différent pour vous, assurez-vous de l'activer GuardDuty avant qu'un objet S3 ne soit chargé dans votre compartiment protégé.

> **Note**
>
> GuardDuty Impossible de générer une recherche pour un objet S3 qui a été scanné avant l'activation GuardDuty. Pour scanner un objet S3 existant, vous pouvez le télécharger à nouveau.

Object:S3/MaliciousFile

Un fichier malveillant a été détecté sur un objet S3 scanné.

Gravité par défaut : élevée

- Fonctionnalité : Protection contre les logiciels malveillants pour S3

Ce résultat indique qu'une analyse des programmes malveillants a détecté que l'objet S3 répertorié était malveillant. Pour plus d'informations, consultez la section Menaces détectées dans le panneau des détails de la recherche.

Correction des recommandations :

Si cette découverte était inattendue, l'objet S3 est potentiellement malveillant. Pour plus d'informations sur les étapes de correction recommandées, consultezCorriger un objet S3 potentiellement malveillant.

Types de résultat de la protection RDS GuardDuty

La protection RDS GuardDuty détecte les comportements de connexion anormaux sur votre instance de base de données. Les résultats suivants sont propres à la RDSBases de données Amazon Aurora et Amazon prises en charge et leur type de ressource sera `RDSDBInstance`. La gravité et les détails des résultats diffèrent selon le type de résultat.

Rubriques

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte de manière anormale.

Gravité par défaut : variable

> **Note**
>
> Selon le comportement anormal associé à ce résultat, la gravité par défaut peut être Faible, Moyenne ou Élevée.
>
> - Faible : si le nom d'utilisateur associé à ce résultat s'est connecté à partir d'une adresse IP associée à un réseau privé.
> - Moyenne : si le nom d'utilisateur associé à ce résultat s'est connecté à partir d'une adresse IP publique.

- Élevée : s'il existe un modèle constant de tentatives de connexion infructueuses à partir d'adresses IP publiques indiquant des stratégies d'accès trop permissives.

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une connexion réussie anormale a été observée sur une base de données RDS dans votre environnement AWS. Cela peut indiquer qu'un utilisateur inconnu s'est connecté à une base de données RDS pour la première fois. Un scénario courant est celui d'un utilisateur interne se connectant à une base de données à laquelle des applications accèdent par programmation et non des utilisateurs individuels.

Cette connexion réussie a été identifiée comme anormale par le modèle de machine learning (ML) de détection d'anomalies GuardDuty. Le modèle de ML évalue tous les événements de connexion à la base de données dans votre RDSBases de données Amazon Aurora et Amazon prises en charge et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de l'activité de connexion RDS, tels que l'utilisateur qui a fait la demande, l'emplacement d'origine la demande et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur les événements de connexion potentiellement inhabituels, veuillez consulter RDSanomalies liées à l'activité de connexion.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour détecter les activités effectuées par l'utilisateur anormal. Les résultats de gravité moyenne ou élevée peuvent indiquer que la stratégie d'accès à la base de données est trop permissive et que les informations d'identification des utilisateurs ont peut-être été divulguées ou compromises. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion réussie.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Une ou plusieurs tentatives de connexion infructueuses inhabituelles ont été observées sur une base de données RDS de votre compte.

Gravité par défaut : faible

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'un ou plusieurs échecs de connexion anormaux ont été observés sur une base de données RDS de votre environnement AWS L'échec des tentatives de connexion à partir d'adresses IP publiques peut indiquer que la base de données RDS de votre compte a fait l'objet d'une tentative d'attaque par force brute par un acteur potentiellement malveillant.

Ces échecs de connexion ont été identifiés comme anormaux par le modèle de machine learning (ML) de détection d'anomalies GuardDuty. Le modèle de ML évalue tous les événements de connexion à la base de données dans votre RDSBases de données Amazon Aurora et Amazon prises en charge et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de l'activité de connexion RDS, tels que l'utilisateur qui a fait la demande, l'emplacement d'origine la demande et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur les activités de connexion RDS potentiellement inhabituelles, veuillez consulter RDSanomalies liées à l'activité de connexion.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la base de données est exposée au public ou que la stratégie d'accès à la base de données est trop permissive. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion échouée.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte à partir d'une adresse IP publique de manière anormale en suivant un modèle constant de tentatives de connexion infructueuses inhabituelles.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une connexion anormale impliquant une force brute réussie a été observée sur une base de données RDS dans votre environnement AWS. Avant une connexion réussie anormale, un modèle constant de tentatives de connexion infructueuses inhabituelles a été observé. Cela indique que l'utilisateur et le mot de passe associés à la base de données RDS dans votre compte ont peut-être été compromis et qu'un acteur potentiellement malveillant a peut-être accédé à la base de données RDS.

Cette connexion réussie par force brute a été identifiée comme anormale par le modèle de machine learning (ML) de détection d'anomalies GuardDuty. Le modèle de ML évalue tous les événements de connexion à la base de données dans votre RDSBases de données Amazon Aurora et Amazon prises en charge et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Le modèle ML suit divers facteurs de l'activité de connexion RDS, tels que l'utilisateur qui a fait la demande, l'emplacement d'origine la demande et les détails spécifiques de connexion à la base de données utilisés. Pour plus d'informations sur les activités de connexion RDS potentiellement inhabituelles, veuillez consulter RDSanomalies liées à l'activité de connexion.

Recommandations de correction :

Cette activité indique que les informations d'identification de la base de données ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour prendre connaissance des activités effectuées par l'utilisateur potentiellement compromis. Un modèle constant de tentatives de connexion infructueuses inhabituelles indique une stratégie d'accès à la base de données trop permissive ou que la base de données peut également avoir été exposée publiquement. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion réussie.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une activité de connexion RDS réussie s'est produite à partir d'une adresse IP associée à une activité malveillante connue dans votre environnement AWS. Cela indique que l'utilisateur et le mot de passe associés à la base de données RDS dans votre compte ont peut-être été compromis et qu'un acteur potentiellement malveillant a peut-être accédé à la base de données RDS.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour prendre connaissance des activités effectuées par l'utilisateur compromis. Cette activité peut également indiquer qu'il existe une stratégie d'accès trop permissive à la base de données ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion réussie.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Une adresse IP associée à une activité malveillante connue a tenté en vain de se connecter à une base de données RDS dans votre compte.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une adresse IP associée à une activité malveillante connue a tenté de se connecter à une base de données RDS dans votre environnement AWS, mais n'a pas fourni le nom d'utilisateur ou le mot de passe correct. Cela indique qu'un acteur potentiellement malveillant tente peut-être de compromettre la base de données RDS dans votre compte.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion échouée.

Discovery:RDS/MaliciousIPCaller

Une adresse IP associée à une activité malveillante connue a effectué une recherche dans une base de données RDS de votre compte. Aucune tentative d'authentification n'a été effectuée.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une adresse IP associée à une activité malveillante connue a effectué une recherche dans une base de données RDS dans votre environnement AWS, bien qu'aucune tentative de connexion n'ait été effectuée. Cela peut indiquer qu'un acteur potentiellement malveillant tente de rechercher une infrastructure accessible au public.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion échouée.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un utilisateur est parvenu à se connecter à une base de données RDS de votre compte à partir d'une adresse IP du nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'un utilisateur est parvenu à se connecter à une base de données RDS de votre environnement AWS, à partir d'une adresse IP du nœud de sortie Tor. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé aux ressources RDS dans votre compte, dans le but de masquer la véritable identité de l'utilisateur anonyme.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que les informations d'identification de l'utilisateur ont peut-être été exposées ou compromises. Il est recommandé de modifier le mot de passe de l'utilisateur de base de données associé et de consulter les journaux d'audit disponibles pour prendre connaissance des activités effectuées par l'utilisateur compromis. Cette activité peut également indiquer qu'il existe une stratégie d'accès trop permissive à la base de données ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion réussie.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Une adresse IP Tor a tenté de se connecter sans succès à une base de données RDS dans votre compte.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une adresse IP de nœud de sortie Tor a tenté de se connecter à une base de données RDS dans votre environnement AWS, mais n'a pas fourni le nom d'utilisateur ou le mot de passe correct. Tor est un logiciel permettant d'activer les communications anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un

accès non autorisé aux ressources RDS dans votre compte, dans le but de masquer la véritable identité de l'utilisateur anonyme.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion échouée.

Discovery:RDS/TorIPCaller

Une adresse IP du nœud de sortie Tor a effectué une recherche dans une base de données RDS de votre compte, aucune tentative d'authentification n'a eu lieu.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité de connexion RDS

Ce résultat vous informe qu'une adresse IP du nœud de sortie Tor a effectué une recherche dans une base de données RDS dans votre environnement AWS, bien qu'aucune tentative de connexion n'ait eu lieu. Cela peut indiquer qu'un acteur potentiellement malveillant tente de rechercher une infrastructure accessible au public. Tor est un logiciel permettant d'activer les communications anonymes. Il chiffre et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Cela peut être le signe d'un accès non autorisé aux ressources RDS dans votre compte, dans le but de masquer la véritable identité de l'acteur potentiellement malveillant.

Recommandations de correction :

Si cette activité est inattendue pour la base de données associée, cela peut indiquer que la stratégie d'accès à la base de données est trop permissive ou que la base de données est exposée au public. Il est recommandé de placer la base de données dans un VPC privé et de limiter les règles du groupe de sécurité afin d'autoriser le trafic provenant uniquement des sources nécessaires. Pour de plus amples informations, veuillez consulter Correction d'une base de données potentiellement compromise avec des événements de connexion échouée.

Types de résultat de la protection Lambda

Cette section décrit les types de résultat propres à vos ressources AWS Lambda et pour lesquels le `resourceType` est répertorié comme `Lambda`. Pour tous les résultats Lambda, nous vous recommandons d'examiner la ressource en question et de déterminer si elle se comporte comme prévu. Si l'activité est autorisée, vous pouvez utiliser des règles de suppression ou des adresses IP approuvées et des listes de menaces pour éviter les notifications faussement positives pour cette ressource.

Si l'activité est inattendue, la bonne pratique en matière de sécurité consiste à partir du principe que Lambda a été potentiellement compromis et à suivre les recommandations de correction.

Rubriques

Backdoor:Lambda/C&CActivity.B

Une fonction Lambda interroge une adresse IP associée à un serveur de commande et de contrôle connu.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous informe que la fonction Lambda répertoriée dans votre environnement AWS interroge une adresse IP associée à un serveur de commande et de contrôle connu. La fonction Lambda associée au résultat généré est potentiellement compromise. Les serveurs de commande et de contrôle sont des ordinateurs qui lancent des commandes vers les membres d'un botnet.

Un botnet est un ensemble d'appareils connectés à Internet (PC, serveurs, appareils mobiles et appareils de l'Internet des objets, etc.) qui est infecté et contrôlé par un type courant de programme malveillant. Les botnets sont souvent utilisés pour distribuer des programmes malveillants et voler des informations, telles que des numéros de carte de crédit. Selon l'objectif et la structure du botnet, le serveur de commande et de contrôle peut également être amené à émettre des commandes pour lancer un déni de service distribué (DDoS).

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter Corriger une fonction Lambda potentiellement compromise.

CryptoCurrency:Lambda/BitcoinTool.B

Une fonction Lambda interroge une adresse IP associée à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous informe que la fonction Lambda répertoriée de votre environnement AWS interroge une adresse IP associée à une activité liée au Bitcoin ou à une autre cryptomonnaie. Les acteurs malveillants peuvent chercher à prendre le contrôle des fonctions Lambda afin de les réutiliser de manière malveillante à des fins d'exploitation non autorisée de cryptomonnaies.

Recommandations de correction :

Si vous utilisez cette fonction Lambda pour exploiter ou gérer des cryptomonnaies, ou si cette fonction est impliquée d'une autre manière dans une activité de blockchain, il s'agit potentiellement d'une activité attendue pour votre environnement. Si c'est le cas dans votre environnement AWS, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur CryptoCurrency:Lambda/BitcoinTool.B. Le deuxième critère de filtre doit être le nom de la fonction Lambda de la fonction impliquée dans l'activité de blockchain. Pour plus d'informations sur la création de règles de suppression, veuillez consulter Règles de suppression (langue française non garantie).

Si cette activité est imprévue, il est possible que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter Corriger une fonction Lambda potentiellement compromise.

Trojan:Lambda/BlackholeTraffic

Une fonction Lambda tente de communiquer avec une adresse IP d'un hôte distant qui est un trou noir connu.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous informe qu'une fonction Lambda répertoriée dans votre environnement AWS essaie de communiquer avec l'adresse IP d'un trou noir (ou gouffre). Les trous noirs sont des zones du réseau où le trafic entrant ou sortant est supprimé silencieusement sans informer la source que les données n'ont pas atteint leur destinataire. Une adresse IP de trou noir désigne une machine hôte qui n'est pas en cours d'exécution ou une adresse à laquelle aucun hôte n'a été attribué. La fonction Lambda répertoriée est potentiellement compromise.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter Corriger une fonction Lambda potentiellement compromise.

Trojan:Lambda/DropPoint

Une fonction Lambda tente de communiquer avec une adresse IP d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous informe qu'une fonction Lambda répertoriée de votre environnement AWS tente de communiquer avec une adresse IP d'un hôte distant connu pour contenir les informations d'identification et d'autres données volées capturées par des programmes malveillants.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter Corriger une fonction Lambda potentiellement compromise.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Une fonction Lambda établit des connexions à une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous informe qu'une fonction Lambda de votre environnement AWS communique avec une adresse IP figurant sur une liste de menaces que vous avez téléchargée. Dans GuardDuty, une liste de menaces comporte des adresses IP malveillantes connues. GuardDuty génère des résultats en fonction des listes de menaces chargées. Vous pouvez afficher les détails de la liste des menaces dans les détails du résultat de la console GuardDuty.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter Corriger une fonction Lambda potentiellement compromise.

UnauthorizedAccess:Lambda/TorClient

Une fonction Lambda est en train de se connecter à un nœud Tor Guard ou Authority.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous informe qu'une fonction Lambda de votre environnement AWS est en train de se connecter à un nœud Tor Guard ou Authority. Tor est un logiciel permettant d'activer les communications anonymes. Le nœud Tor Guard et Authority agit en tant que passerelles initiales dans un réseau Tor. Ce trafic peut indiquer que cette fonction Lambda a été potentiellement compromise. Il agit désormais en tant que client sur un réseau Tor.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter Corriger une fonction Lambda potentiellement compromise.

UnauthorizedAccess:Lambda/TorRelay

Une fonction Lambda est en train de se connecter à un réseau Tor en tant que relais Tor.

Gravité par défaut : élevée

- Fonctionnalité : surveillance de l'activité du réseau Lambda

Ce résultat vous informe qu'une fonction Lambda de votre environnement AWS est en train de se connecter à un réseau Tor d'une façon qui suggère qu'elle agit en tant que relais Tor. Tor est un logiciel permettant d'activer les communications anonymes. Tor active une communication anonyme en réacheminant le trafic potentiellement illicite du client d'un relais Tor à un autre.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre fonction Lambda soit compromise. Pour de plus amples informations, veuillez consulter Corriger une fonction Lambda potentiellement compromise.

Retrait de types de résultat

Un résultat est une notification qui contient des détails sur un problème de sécurité potentiel découvert par GuardDuty. Pour plus d'informations sur les modifications importantes apportées aux types de résultats GuardDuty, y compris les types de résultats récemment ajoutés ou hors-service, consultez Historique du document pour Amazon GuardDuty.

Les types de résultat suivants ont été retirés et ne sont plus générés par GuardDuty.

> **Important**
>
> Vous ne pouvez PAS réactiver des types de résultat GuardDuty retirés.

Rubriques

Exfiltration:S3/ObjectRead.Unusual

Une entité IAM a invoqué une API S3 de manière suspecte.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

- Source de données : événements de données CloudTrail pour S3

Ce résultat vous informe qu'une entité IAM de votre environnement AWS effectue des appels d'API qui impliquent un compartiment S3 et qui diffèrent de la base de référence établie de cette entité. L'appel d'API utilisé dans cette activité est associé à la phase d'exfiltration d'une attaque, au cours de laquelle un pirate tente de collecter des données. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter Corriger un compartiment S3 potentiellement compromis.

Impact:S3/PermissionsModification.Unusual

Une entité IAM a invoqué une API pour modifier les autorisations sur une ou plusieurs ressources S3.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'une entité IAM effectue des appels d'API conçus pour modifier les autorisations sur un ou plusieurs compartiments ou objets de votre environnement AWS. Cette action peut être effectuée par un pirate pour permettre le partage d'informations en dehors du compte. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter Corriger un compartiment S3 potentiellement compromis.

Impact:S3/ObjectDelete.Unusual

Une entité IAM a invoqué une API utilisée pour supprimer les données dans un compartiment S3.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'une entité IAM spécifique de votre environnement AWS effectue des appels d'API conçus pour supprimer les données du compartiment S3 répertorié en supprimant le compartiment lui-même. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter Corriger un compartiment S3 potentiellement compromis.

Discovery:S3/BucketEnumeration.Unusual

Une entité IAM a invoqué une API S3 utilisée pour découvrir les compartiments S3 au sein de votre réseau.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'une entité IAM a invoqué une API S3 pour découvrir des compartiments S3 dans votre environnement, comme `ListBuckets`. Ce type d'activité est associé à la phase de découverte d'une attaque au cours de laquelle un pirate collecte des informations pour déterminer si votre environnement AWS est vulnérable à une attaque de plus grande envergure. Cette activité est suspecte, car la manière dont l'entité IAM a invoqué l'API était inhabituelle. Par exemple, cette entité IAM n'avait jamais invoqué ce type d'API, ou l'API avait été invoquée depuis un emplacement inhabituel.

Recommandations de correction :

Si cette activité est inattendue pour le principal associé, cela peut indiquer que les informations d'identification ont été exposées ou que vos autorisations S3 ne sont pas suffisamment restrictives. Pour de plus amples informations, veuillez consulter Corriger un compartiment S3 potentiellement compromis.

Persistence:IAMUser/NetworkPermissions

Une entité IAM a invoqué une API couramment utilisée pour modifier les permissions d'accès réseau pour les groupes de sécurité, les circuits et les listes de contrôle d'accès (ACL) dans votre compte AWS.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'un principal spécifique (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur) de votre environnement AWS présente un comportement différent de la référence établie. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché lorsque les paramètres de configuration réseau sont modifiés dans des circonstances suspectes, par exemple lorsqu'un principal invoque l'API `CreateSecurityGroup` alors qu'il ne l'a jamais fait auparavant. Les pirates essaient souvent de modifier des groupes de sécurité, ce qui permet le trafic entrant sur les différents ports afin d'améliorer leur capacité à accéder à une instance EC2.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Persistence:IAMUser/ResourcePermissions

Un principal a invoqué une API couramment utilisée pour modifier les stratégies d'accès de sécurité de diverses ressources de votre Compte AWS.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'un principal spécifique (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur) de votre environnement AWS présente un comportement différent de la référence établie. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché lorsqu'une modification au niveau des stratégies ou des autorisations associées aux ressources AWS est détectée, par exemple lorsqu'un principal de votre environnement AWSinvoque l'API `PutBucketPolicy`, alors qu'il ne l'a jamais fait auparavant. Certains services,

comme Amazon S3, prennent en charge les autorisations associées à des ressources et permettant à un ou plusieurs principaux d'accéder à la ressource. Avec des informations d'identification volées, des pirates peuvent modifier les stratégies associées à une ressource pour y obtenir l'accès.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Persistence:IAMUser/UserPermissions

Un principal a appelé une API couramment utilisée pour ajouter, modifier ou supprimer des utilisateurs IAM, groupes ou stratégies de votre compte AWS.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'un principal spécifique (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur) de votre environnement AWS présente un comportement différent de la référence établie. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché par des modifications suspectes apportées aux autorisations relatives aux utilisateurs dans votre environnement AWS, par exemple lorsqu'un principal de votre environnement AWS invoque l'`AttachUserPolicy`API alors qu'il ne l'a jamais fait auparavant. Les pirates peuvent utiliser des informations d'identification volées pour créer des utilisateurs, ajouter des stratégies d'accès aux utilisateurs existants ou créer des clés d'accès afin de maximiser leur accès à un compte, même si leur point d'accès d'origine est fermé. Par exemple, le propriétaire du compte peut remarquer qu'un utilisateur IAM ou un mot de passe particulier a été volé et le supprimer du compte. Cependant, il est possible qu'il ne supprime pas d'autres utilisateurs créés par un principal administrateur créé de façon frauduleuse, en laissant leur compte AWS accessible au pirate.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Un principal a tenté de s'attribuer à lui-même une stratégie très permissive.

Gravité par défaut : faible*

> **Note**
>
> La gravité de ce résultat est faible si la tentative d'escalade des privilèges n'a pas abouti. Elle est moyenne si la tentative d'escalade des privilèges a réussi.

Ce résultat signifie qu'une entité IAM spécifique de votre environnement AWS présente un comportement pouvant indiquer une attaque d'escalade des privilèges. Ce résultat est déclenché lorsqu'un utilisateur ou un rôle IAM tente de s'attribuer à lui-même une stratégie très permissive. Si l'utilisateur ou le rôle en question n'est pas censé disposer de privilèges d'administration, soit les informations d'identification de l'utilisateur sont compromises, soit les autorisations du rôle ne sont pas configurées correctement.

Les pirates utiliseront des informations d'identification volées pour créer des utilisateurs, ajouter des stratégies d'accès aux utilisateurs existants ou créer des clés d'accès afin de maximiser leur accès à un compte, même si leur point d'accès d'origine est fermé. Par exemple, le propriétaire du compte peut remarquer que les informations d'identification de connexion d'un utilisateur IAM spécifique ont été volées et les supprimer du compte, mais ne pas supprimer d'autres utilisateurs qui ont été créés par le principal administrateur frauduleusement créé, laissant leur compte AWS toujours accessible au pirate.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Recon:IAMUser/NetworkPermissions

Un principal a invoqué une API couramment utilisée pour modifier les permissions d'accès réseau pour les groupes de sécurité, les circuits et les listes de contrôle d'accès (ACL) dans votre compte AWS.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'un principal spécifique (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur) de votre environnement AWS présente un comportement différent de la référence établie. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché lorsque des autorisations d'accès à des ressources dans votre compte AWS sont examinées dans des circonstances suspectes. Par exemple, si un principal a appelé l'API `DescribeInstances` alors qu'il ne l'a jamais fait auparavant. Un pirate pourrait utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos ressources AWS afin de trouver des informations d'identification plus utiles ou de déterminer les capacités des informations d'identification dont ils disposent déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Recon:IAMUser/ResourcePermissions

Un principal a invoqué une API couramment utilisée pour modifier les stratégies d'accès de sécurité de diverses ressources de votre compte AWS.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat vous informe qu'un principal spécifique (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur) de votre environnement AWS présente un comportement différent de la référence établie. Ce principal n'a jamais appelé cette API auparavant.

Ce résultat est déclenché lorsque des autorisations d'accès à des ressources dans votre compte AWS sont examinées dans des circonstances suspectes. Par exemple, si un principal a appelé l'API `DescribeInstances` alors qu'il ne l'a jamais fait auparavant. Un pirate pourrait utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos ressources AWS afin de trouver des informations d'identification plus utiles ou de déterminer les capacités des informations d'identification dont ils disposent déjà.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Recon:IAMUser/UserPermissions

Un principal a appelé une API couramment utilisée pour ajouter, modifier ou supprimer des utilisateurs IAM, groupes ou stratégies de votre compte AWS.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat est déclenché lorsque des autorisations d'utilisateurs dans votre environnement AWS sont examinées dans des circonstances suspectes. Par exemple, si un principal (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur IAM) a invoqué l'API `ListInstanceProfilesForRole` alors qu'il ne l'a jamais fait auparavant. Un pirate pourrait utiliser des informations d'identification volées pour effectuer ce type de reconnaissance de vos ressources AWS afin de trouver des informations d'identification plus utiles ou de déterminer les capacités des informations d'identification dont ils disposent déjà.

Ce résultat vous informe qu'un principal spécifique de votre environnement AWS présente un comportement différent de la référence établie. Ce principal n'a jamais appelé cette API auparavant de cette manière.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

ResourceConsumption:IAMUser/ComputeResources

Un principal a appelé une API couramment utilisée pour lancer des ressources de calcul comme des instances EC2.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat est déclenché lorsque des instances EC2 dans le compte répertorié au sein de votre environnement AWS sont lancées dans des circonstances suspectes. Ce résultat indique qu'un principal spécifique de votre environnement AWS présente un comportement différent de celui de la référence établie ; par exemple, si un principal (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur IAM) a invoqué l'API `RunInstances` alors qu'il ne l'a jamais fait auparavant. Cela peut être le signe qu'un pirate utilise des informations d'identification volées pour voler du temps de calcul

(peut-être pour le minage de monnaie cryptographique ou le cassage d'un mot de passe). Cela peut également indiquer qu'un pirate utilise une instance EC2 de votre environnement AWS et ses informations d'identification pour maintenir l'accès à votre compte.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Stealth:IAMUser/LoggingConfigurationModified

Un principal a invoqué une API couramment utilisée pour arrêter la journalisation CloudTrail, supprimer des journaux existants et éliminer par d'autres méthodes les traces d'activité dans votre compte AWS.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat est déclenché lorsque la configuration de la journalisation dans le compte AWS répertorié au sein de votre environnement est modifiée dans des circonstances suspectes. Ce résultat vous informe qu'un principal spécifique de votre environnement AWS présente un comportement différent de celui de la référence établie ; par exemple, si un principal (Utilisateur racine d'un compte AWS, rôle IAM ou utilisateur IAM) a invoqué l'API `StopLogging` alors qu'il ne l'a jamais fait auparavant. Cela peut indiquer qu'un pirate tente de recouvrir ses traces toute trace de ses activités.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

UnauthorizedAccess:IAMUser/ConsoleLogin

Une connexion inhabituelle à une console par un principal dans votre compte AWS a été observée.

Gravité par défaut : moyenne*

> **Note**
>
> La gravité par défaut de ce résultat est moyenne. Toutefois, si l'API est invoquée à l'aide d'informations d'identification AWS temporaires créées sur une instance, la gravité du résultat est élevée.

Ce résultat est déclenchée lorsqu'une connexion à une console est détectée dans des circonstances suspectes. Par exemple, si un principal a appelé pour la première fois l'API ConsoleLogin API depuis un client jamais utilisé auparavant ou un emplacement inhabituel. Ceci peut indiquer que des informations d'identification volées sont utilisées pour accéder à votre compte AWS ou qu'un utilisateur valide accède au compte d'une manière invalide ou peu sécurisée (par exemple sans passer par un VPN approuvé).

Ce résultat vous informe qu'un principal spécifique de votre environnement AWS présente un comportement différent de la référence établie. Ce principal n'a jamais eu d'activité de connexion à l'aide de cette application client et depuis cet emplacement spécifique auparavant.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

UnauthorizedAccess:EC2/TorIPCaller

Votre instance EC2 reçoit des connexions entrantes d'un nœud d'exit Tor.

Gravité par défaut : moyenne

Ce résultat vous informe qu'une instance EC2 dans votre environnement AWS reçoit des connexions entrantes à partir d'un nœud d'exit Tor. Tor est un logiciel permettant d'activer les communications

anonymes. Il crypte et retourne des communications de façon aléatoire à l'expéditeur via des relais entre une série de nœuds du réseau. Le dernier nœud Tor est appelé nœud de sortie. Ce résultat peut être le signe d'un accès non autorisé à vos ressources AWS dans le but de masquer la véritable identité du pirate.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

Backdoor:EC2/XORDDOS

Une instance EC2 tente communiquer avec une adresse IP associée au programme malveillant XOR DDos.

Gravité par défaut : élevée

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS tente de communiquer avec une adresse IP associée au programme malveillant XOR DDos. Cette instance EC2 pourrait être compromise. XOR DDoS est un cheval de Troie qui pirate les systèmes Linux. Pour accéder au système, il lance une attaque en force afin de découvrir le mot de passe d'accès aux services Secure Shell (SSH) sur Linux. Une fois les informations d'identification SSH obtenues et la connexion réussie, il utilise les privilèges d'utilisateur root pour exécuter un script qui télécharge et installe XOR DDoS. Ce logiciel malveillant est ensuite utilisé dans le cadre d'un botnet pour lancer des attaques par déni de service (DDoS) distribué à l'encontre d'autres cibles.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

Behavior:IAMUser/InstanceLaunchUnusual

Un utilisateur a lancé une instance EC2 d'un type inhabituel.

Gravité par défaut : élevée

Ce résultat vous informe qu'un utilisateur spécifique de votre environnement AWS présente un comportement différent de la référence établie. Cet utilisateur n'a jamais lancé d'instances EC2 de ce type auparavant. Vos informations d'identification de connexion pourraient être compromises.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

CryptoCurrency:EC2/BitcoinTool.A

Une instance EC2 communique avec des groupes de minage de bitcoins.

Gravité par défaut : élevée

Ce résultat vous informe qu'une instance EC2 de votre environnement AWS communique avec des groupes de minage de bitcoins. Dans le domaine du minage de monnaies cryptographiques, un groupe de minage désigné le regroupement des ressources des mineurs, qui partagent leur puissance de traitement sur un réseau pour répartir les gains en fonction de leur contribution à la résolution d'un bloc. A moins que vous ne l'utilisiez à des fins de minage de bitcoins, votre instance EC2 pourrait être compromise.

Recommandations de correction :

Si cette activité est imprévue, il se peut que votre instance soit compromise. Pour de plus amples informations, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Une API a été invoquée depuis une adresse IP d'un réseau inhabituel.

Gravité par défaut : élevée

Ce résultat vous informe qu'une activité a été appelée depuis une adresse IP d'un réseau inhabituel. Ce réseau n'a jamais été observé dans l'historique d'utilisation d'AWS de l'utilisateur spécifié. Cette activité peut inclure une connexion à la console, ou une tentative de lancement d'une instance EC2, de création d'un utilisateur IAM ou de modification de vos privilèges AWS, etc. Cela peut être signe d'un accès non autorisé à vos ressources AWS.

Recommandations de correction :

Si cette activité est inattendue, vos informations d'identification peuvent être compromises. Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.

Résultats par type de ressource

Les pages suivantes sont classées par type de ressource associé à une GuardDuty constatation :

- Types de résultat EC2
- IAMtypes de recherche
- Types de résultat S3
- EKStypes de recherche de journaux d'audit
- Types de recherche liés à la surveillance du temps
- Protection contre les programmes malveillants pour les types de détection EC2
- Protection contre les programmes malveillants pour le type de recherche S3
- Types de résultat de la protection RDS
- Types de résultat de la protection Lambda

Tableau des résultats

Le tableau suivant présente tous les types de résultat actifs triés par source de données ou fonctionnalité de base, le cas échéant. Certains des types de résultat suivants peuvent avoir une gravité variable, indiquée par un astérisque (*). Pour plus d'informations sur la gravité variable d'un type de résultat, veuillez consulter la description détaillée qui s'y rapporte.

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Discovery :S3/Anoma lousBehavior	Amazon S3	CloudTrail événements de données pour S3	Faible
Discovery:S3/ MaliciousIPCal ler	Amazon S3	CloudTrail événements de données pour S3	Élevée
Discovery:S3/ MaliciousIPCal ler.Custom	Amazon S3	CloudTrail événements de données pour S3	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail événements de données pour S3	Medium
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail événements de données pour S3	Élevée
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail événements de données pour S3	Élevée
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail événements de données pour S3	Élevée
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail événements de données pour S3	Élevée
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail événements de données pour S3	Medium
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail événements de données pour S3	Élevée
PenTest:S3/KaliLinux	Amazon S3	CloudTrail événements de données pour S3	Medium
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail événements de données pour S3	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
PenTest:S3/PentooLinux	Amazon S3	CloudTrail événements de données pour S3	Medium
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail événements de données pour S3	Élevée
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail événements de données pour S3	Élevée
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Medium
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Medium
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Faible
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Élevée
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Medium
PenTest:IAMUser/KaliLinux	IAM	CloudTrail événement de gestion	Medium
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail événement de gestion	Medium
PenTest:IAMUser/PentooLinux	IAM	CloudTrail événement de gestion	Medium
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Medium
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail événement de gestion	Faible*

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail événement de gestion	Élevée*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail événement de gestion	Faible
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail événement de gestion	Élevée
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail événement de gestion	Faible
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail événement de gestion	Élevée
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail événement de gestion	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail événement de gestion	Medium
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail événement de gestion	Medium
Recon:IAMUser/TorIPCaller	IAM	CloudTrail événement de gestion	Medium
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail événement de gestion	Faible
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail événement de gestion	Faible
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail événement de gestion	Medium
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail événement de gestion	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail événement de gestion	Medium
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail événement de gestion	Medium
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail événements de gestion ou événements de CloudTrail données pour S3	Faible
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail événements de gestion ou événements de CloudTrail données pour S3	Élevée
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNSjournaux	Élevée
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNSjournaux	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNSjournaux	Medium
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNSjournaux	Élevée
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNSjournaux	Élevée
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNSjournaux	Faible
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNSjournaux	Medium
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNSjournaux	Élevée
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNSjournaux	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNSjournaux	Élevée
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNSjournaux	Élevée
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNSjournaux	Medium
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNSjournaux	Élevée
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNSjournaux	Élevée
Execution:Container/MaliciousFile	Conteneur	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée
Execution:Container/SuspiciousFile	Conteneur	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée
Execution:EC2/MaliciousFile	EC2	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Execution:EC2/SuspiciousFile	EC2	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée
Execution:ECS/MaliciousFile	ECS	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée
Execution:ECS/SuspiciousFile	ECS	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée
Execution:Kubernetes/MaliciousFile	Kubernetes	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBSProtection contre les logiciels malveillants	Varie en fonction de la menace détectée
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKSjournaux d'audit	Medium
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKSjournaux d'audit	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSjournaux d'audit	Élevée
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSjournaux d'audit	Élevée
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKSjournaux d'audit	Élevée
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKSjournaux d'audit	Élevée
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSjournaux d'audit	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSjournaux d'audit	Élevée
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKSjournaux d'audit	Élevée
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKSjournaux d'audit	Faible
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKSjournaux d'audit	Medium
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSjournaux d'audit	Medium
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSjournaux d'audit	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKSjournaux d'audit	Medium
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKSjournaux d'audit	Medium
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKSjournaux d'audit	Medium
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKSjournaux d'audit	Faible
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKSjournaux d'audit	Élevée
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSjournaux d'audit	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSjournaux d'audit	Élevée
Impact:Kubernetes/TorIPCaller	Kubernetes	EKSjournaux d'audit	Élevée
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKSjournaux d'audit	Medium
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKSjournaux d'audit	Medium
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSjournaux d'audit	Medium
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSjournaux d'audit	Élevée
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKSjournaux d'audit	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKSjournaux d'audit	Élevée
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKSjournaux d'audit	Élevée
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKSjournaux d'audit	Medium
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKSjournaux d'audit	Medium
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKSjournaux d'audit	Moyenne*

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKSjournaux d'audit	Faible
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKSjournaux d'audit	Élevée
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKSjournaux d'audit	Élevée
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	EKSjournaux d'audit	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Backdoor:Lambda/C&CActivity.B	Lambda	Surveillance de l'activité du réseau Lambda	Élevée
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Surveillance de l'activité du réseau Lambda	Élevée
Trojan:Lambda/BlackholeTraffic	Lambda	Surveillance de l'activité du réseau Lambda	Medium
Trojan:Lambda/DropPoint	Lambda	Surveillance de l'activité du réseau Lambda	Medium
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Surveillance de l'activité du réseau Lambda	Medium
UnauthorizedAccess:Lambda/TorClient	Lambda	Surveillance de l'activité du réseau Lambda	Élevée
UnauthorizedAccess:Lambda/TorRelay	Lambda	Surveillance de l'activité du réseau Lambda	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Faible
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Élevée
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Variable*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Medium
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
CredentialAccess:RDS/TorIPCaller.FailedLogin	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Medium
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Élevée
Discovery:RDS/MaliciousIPCaller	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Medium
Discovery:RDS/TorIPCaller	RDSBases de données Amazon Aurora et Amazon prises en charge	RDSSurveillance de l'activité de connexion	Medium
Backdoor:Runtime/C&CActivity.B	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Backdoor:Runtime/C&CActivity.B!DNS	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
CryptoCurrency:Runtime/BitcoinTool.B	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/FilelessExecution	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
DefenseEvasion:Runtime/ProcessInjection.Proc	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/PtraceAntiDebugging	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Faible

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
DefenseEvasion:Runtime/SuspiciousCommand	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Execution:Runtime/MaliciousFileExecuted	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Execution:Runtime/NewBinaryExecuted	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Execution:Runtime/NewLibraryLoaded	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Execution:Runtime/SuspiciousCommand	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Variable
Execution:Runtime/SuspiciousShellCreated	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Faible
Execution:Runtime/SuspiciousTool	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Variable

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Execution:Runtime/ReverseShell	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Impact:Runtime/AbusedDomainRequest.Reputation	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Impact:Runtime/BitcoinDomainRequest.Reputation	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Impact:Runtime/CryptoMinerExecuted	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Impact:Runtime/MaliciousDomainRequest.Reputation	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Faible

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
PrivilegeEscalation:Runtime/ElevationToRoot	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
PrivilegeEscalation:Runtime/RuncContainerEscape	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Privilege Escalation:Runtime/UserfaultfdUsage	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Object:S3/MaliciousFile	S3Object	Protection contre les logiciels malveillants pour S3	Élevée
Trojan:Runtime/BlackholeTraffic	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Trojan:Runtime/BlackholeTraffic!DNS	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Trojan:Runtime/DropPoint	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Trojan:Runtime/DGADomainRequest.C!DNS	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Trojan:Runtime/DriveBySourceTraffic!DNS	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Trojan:Runtime/DropPoint!DNS	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Medium
Trojan:Runtime/PhishingDomainRequest!DNS	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/TorClient	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/TorRelay	Instance, EKS ECS cluster, cluster ou conteneur	Surveillance d'exécution	Élevée
Backdoor:EC2/C&CActivity.B	EC2	Journaux de flux VPC	Élevée
Backdoor:EC2/DenialOfService.Dns	EC2	Journaux de flux VPC	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Backdoor:EC2/DenialOfService.Tcp	EC2	Journaux de flux VPC	Élevée
Backdoor:EC2/DenialOfService.Udp	EC2	Journaux de flux VPC	Élevée
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	Journaux de flux VPC	Élevée
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	Journaux de flux VPC	Élevée
Backdoor:EC2/Spambot	EC2	Journaux de flux VPC	Medium
Behavior:EC2/NetworkPortUnusual	EC2	Journaux de flux VPC	Medium
Behavior:EC2/TrafficVolumeUnusual	EC2	Journaux de flux VPC	Medium
CryptoCurrency:EC2/BitcoinTool.B	EC2	Journaux de flux VPC	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
DefenseEvasion:EC2/UnusualDNSResolver	EC2	Journaux de flux VPC	Medium
DefenseEvasion:EC2/UnusualDoHActivity	EC2	Journaux de flux VPC	Medium
DefenseEvasion:EC2/UnusualDoTActivity	EC2	Journaux de flux VPC	Medium
Impact:EC2/PortSweep	EC2	Journaux de flux VPC	Élevée
Impact:EC2/WinRMBruteForce	EC2	Journaux de flux VPC	Faible*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	Journaux de flux VPC	Élevée
Recon:EC2/PortProbeUnprotectedPort	EC2	Journaux de flux VPC	Faible*
Recon:EC2/Portscan	EC2	Journaux de flux VPC	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Trojan:EC2/BlackholeTraffic	EC2	Journaux de flux VPC	Medium
Trojan:EC2/DropPoint	EC2	Journaux de flux VPC	Medium
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	Journaux de flux VPC	Medium
UnauthorizedAccess:EC2/RDPBruteForce	EC2	Journaux de flux VPC	Faible*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	Journaux de flux VPC	Faible*
UnauthorizedAccess:EC2/TorClient	EC2	Journaux de flux VPC	Élevée
UnauthorizedAccess:EC2/TorRelay	EC2	Journaux de flux VPC	Élevée

Gérer les GuardDuty résultats d'Amazon

GuardDuty propose plusieurs fonctionnalités importantes pour vous aider à trier, stocker et gérer vos résultats. Ces fonctionnalités vous aident à adapter les résultats à votre environnement spécifique, à réduire le bruit des résultats de faible valeur et de vous aider à vous concentrer sur les menaces propres à votre environnement AWS . Consultez les rubriques de cette page pour comprendre comment vous pouvez utiliser ces fonctionnalités pour augmenter la valeur des résultats GuardDuty de votre recherche.

Rubriques :

Tableau de bord récapitulatif

Découvrez les composants du tableau de bord récapitulatif disponible dans la GuardDuty console.

Filtrage des résultats

Découvrez comment filtrer les GuardDuty résultats en fonction des critères que vous spécifiez.

Règles de suppression

Découvrez comment filtrer automatiquement les résultats qui vous sont GuardDuty signalés par le biais de règles de suppression. Les règles de suppression archivent automatiquement les résultats en fonction de filtres.

Utilisation de listes d'adresses IP approuvées et de listes de menaces

Personnalisez le périmètre GuardDuty de surveillance à l'aide de listes d'adresses IP et de listes de menaces basées sur des adresses IP routables publiquement. DNSLes listes d'adresses IP fiables empêchent de générer des informations erronées à partir d'adresses IP que vous considérez comme fiables, tandis que les listes d'informations sur les menaces vous alerteront en cas d'activité définie par l'utilisateurIPs. GuardDuty

Exportation des résultats

Exportez les résultats générés vers un compartiment Amazon S3 afin de pouvoir conserver les dossiers au-delà de la période de conservation de 90 jours prévue GuardDuty pour. Utilisez ces données historiques pour suivre les activités suspectes potentielles sur votre compte et évaluer si les mesures correctives recommandées ont été efficaces.

Création de réponses personnalisées aux GuardDuty résultats avec Amazon CloudWatch Events

Configurez des notifications automatiques pour les GuardDuty résultats obtenus par le biais d' CloudWatch événements Amazon. Vous pouvez également automatiser d'autres tâches par le biais CloudWatch des événements pour vous aider à répondre aux résultats.

Comprendre CloudWatch les journaux et les raisons du manque de ressources lors de l'analyse Malware Protection for EC2

Découvrez comment auditer les CloudWatch journaux pour détecter la protection contre les GuardDuty programmes malveillants EC2 et quelles sont les raisons pour lesquelles votre EC2 instance Amazon ou vos EBS volumes Amazon concernés peuvent avoir été ignorés pendant le processus de numérisation.

Signalement des faux positifs dans GuardDuty Malware Protection for EC2

Découvrez comment signaler les détections potentielles de fausses menaces positives dans Malware Protection for S3.

Tableau de bord récapitulatif

Le tableau de bord récapitulatif fournit une vue agrégée des GuardDuty résultats générés Compte AWS dans votre région actuelle. À l'heure actuelle, le tableau de bord prend en charge un volume allant jusqu'à 5 000 résultats. Toutefois, vous pouvez consulter le détail de tous les résultats en utilisant soit la page Résultats de la GuardDuty console, GetFindingssoit ListFindings.

> **Note**
>
> Le résumé des résultats est uniquement disponible via la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

Les sections suivantes vous aideront à accéder au tableau de bord et à comprendre ses composants.

Table des matières

Accès au tableau de bord récapitulatif

Sur la GuardDuty console, le tableau de bord récapitulatif affiche une vue consolidée des 5 000 derniers GuardDuty résultats générés dans la région actuelle.

Pour accéder au tableau de bord récapitulatif

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Résumé. Lorsque vous ouvrez la console, le tableau de bord récapitulatif s' GuardDuty affiche.
3. Par défaut, le résumé est affiché pour le jour même, c'est-à-dire aujourd'hui. La GuardDuty console propose une option permettant d'afficher le résumé des 2 derniers jours, des 7 derniers jours et des 30 derniers jours. Pour modifier la plage de temps par défaut, choisissez l'une des options dans le menu déroulant au-dessus du volet Présentation.
4. Filtrer les données

   - Les widgets Comptes contenant le plus de résultats, Ressources contenant le plus de résultats et Résultats les moins fréquents vous aident à filtrer les données en fonction du niveau de gravité des résultats.
   - Le widget Ressources contenant le plus de résultats vous permet également de filtrer les données en fonction du type de ressource potentiellement concerné.

     Un compte membre peut consulter les détails de la ressource potentiellement concernée qui appartient à son propre compte. Si vous êtes GuardDuty administrateur et que vous souhaitez consulter les détails de la ressource potentiellement affectée, ouvrez la GuardDuty console à l'aide des informations d'identification du compte membre associé.
5. Couverture des plans de protection

   La couverture des plans de protection indique le nombre de comptes membres qui ont été activés GuardDuty dans votre organisation. Les statistiques ne sont visibles que par l' GuardDuty administrateur délégué.

Présentation du tableau de bord de récapitulatif

Le tableau de bord récapitulatif affiche les données agrégées dans les sections suivantes. Avant de consulter et de comprendre le résumé, assurez-vous de choisir l' Région AWS souhaitée dans le sélecteur de région en haut de la console. Assurez-vous également de choisir la plage horaire

souhaitée dans le menu déroulant situé au-dessus du volet Présentation. Si aucun résultat n'a été généré pour les paramètres choisis, aucune donnée ne sera disponible dans aucun des widgets.

Sur un volume contenant jusqu'à 5 000 GuardDuty résultats, le tableau de bord récapitulatif contenant les comptes contenant le plus de résultats, les ressources contenant le plus de résultats et les résultats les moins récents affiche les données basées sur les 5 meilleurs résultats. Pour une analyse plus approfondie, consultez la page Résultats de la GuardDuty console.

Présentation

Cette section fournit les données suivantes :

- Total des résultats : indique le nombre total de résultats générés sur votre compte dans la région actuelle.
- Constatations de gravité élevée : indique le nombre de GuardDuty constatations présentant un niveau de gravité élevé dans la région actuelle.
- Ressources contenant des résultats : indique le nombre de ressources associées à un résultat et potentiellement compromises.
- Comptes contenant des résultats : indique le nombre de comptes dans lesquels au moins un résultat a été généré. Si vous êtes un compte autonome, la valeur de ce champ est 1.

Pour les plages de temps Les 7 derniers jours et Les 30 derniers jours, le volet Présentation peut afficher la différence en pourcentage entre les résultats générés semaine après semaine (WoW) ou mois par mois (MoM), respectivement. Si aucun résultat n'a été généré au cours de la semaine ou du mois précédent, en l'absence de données à comparer, il se peut que la différence en pourcentage ne soit pas disponible.

Si vous êtes un compte GuardDuty administrateur, tous ces champs fournissent les données résumées de tous les comptes membres de votre organisation.

Résultats par gravité

Cette section affiche un graphique à barres indiquant le nombre total de résultats par rapport à la plage de temps choisie. Vous pouvez consulter le nombre de résultats de gravité faible, moyenne ou élevée, générés à une date précise dans la plage de temps choisie.

Types de résultat les plus courants

Cette section fournit une illustration sous forme de diagramme circulaire des cinq principaux types de résultats courants observés à partir d'un volume allant jusqu'à 5 000 GuardDuty résultats générés

dans la région actuelle. Ce graphique circulaire affiche les données suivantes lorsque vous survolez chaque secteur avec le pointeur de la souris :

- Nombre de résultats : indique le nombre de fois que ce résultat a été généré dans la plage de temps choisie.
- Gravité : indique le niveau de gravité du résultat, comme moyen ou élevé.
- Pourcentage : indique la part de ce type de résultat dans le graphique circulaire.
- Dernière génération : indique le temps écoulé depuis la dernière génération de ce type de résultat.

Comptes contenant le plus de résultats

Cette section fournit les données suivantes :

- Compte : indique l' Compte AWS identifiant dans lequel le résultat a été généré.
- Nombre de résultats : indique le nombre de fois qu'un résultat a été généré pour cet ID de compte.
- Dernière génération : indique le temps écoulé depuis la dernière génération de ce type de résultat pour cet ID de compte.
- Gravité élevée : par défaut, les données sont affichées pour les types de résultat de gravité élevée. Les options possibles pour ce champ sont Gravité élevée, Gravité moyenne et Toutes les formes de gravité.

Ressources contenant des résultats

Cette section fournit les données suivantes :

- Ressource : indique le type de ressource potentiellement concerné et si cette ressource appartient à votre compte, vous pouvez accéder au lien rapide pour afficher les détails de la ressource. Si vous êtes GuardDuty administrateur, vous pouvez consulter les détails de la ressource potentiellement affectée en accédant à la GuardDuty console avec les informations d'identification du compte membre auquel appartient cette ressource.
- Compte : indique l' Compte AWS ID auquel appartient cette ressource.
- Nombre de résultats : indique le nombre de fois que cette ressource a été associée à un résultat.
- Dernière génération : indique le temps écoulé depuis la dernière génération d'un type de résultat associé à cette ressource.

- Tous types de ressource : par défaut, les données sont affichées pour tous les types de ressource. À l'aide de la liste déroulante, vous pouvez afficher les données d'un type de ressource spécifique, tel que Instance AccessKey, Lambda, etc.
- Gravité élevée : par défaut, les données sont affichées pour les types de résultat de gravité élevée. À l'aide de la liste déroulante, vous pouvez consulter les données relatives aux autres niveaux de gravité. Les options possibles sont Gravité élevée, Gravité moyenne et Toutes les formes de gravité.

Résultats les moins fréquents

Cette section fournit des informations détaillées sur les types de recherche qui ne sont pas souvent générés dans votre AWS environnement. Ces informations peuvent vous aider à analyser un modèle de menace émergent dans votre environnement et à prendre des mesures pour y remédier. Le tableau présente les données suivantes :

- Type de résultat : indique le nom du type de résultat.
- Nombre de résultats : indique le nombre de fois que ce type de résultat a été généré dans la plage de temps choisie.
- Dernière génération : indique le temps écoulé depuis la dernière génération de ce type de résultat.
- Gravité élevée : par défaut, les données sont affichées pour les types de résultat de gravité élevée. Les options possibles pour ce champ sont Gravité élevée, Gravité moyenne et Toutes les formes de gravité.

Couverture des plans de protection

Cette section indique le nombre de comptes de membres actifs appartenant à votre organisation et ayant activé une ou plusieurs fonctionnalités ainsi que la configuration de fonctionnalités supplémentaires (le cas échéant) dans la configuration actuelle Région AWS.

Seul un GuardDuty administrateur délégué peut consulter les statistiques des comptes des membres au sein de son organisation. Si aucune fonctionnalité n'est configurée, choisissez Configurer dans la colonne Actions.

Lorsque vous créez une nouvelle AWS organisation, la génération des statistiques pour l'ensemble de l'organisation peut prendre jusqu'à 24 heures.

Fourniture de commentaires sur le tableau de bord récapitulatif

GuardDuty vous encourage à fournir des commentaires sur la convivialité, les fonctionnalités et les performances du tableau de bord récapitulatif. Cela nous aidera à améliorer le tableau de bord.

Pour fournir des commentaires sur le tableau de bord récapitulatif

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le volet de navigation, choisissez Résumé. Lorsque vous ouvrez la GuardDuty console, le tableau de bord récapitulatif s'affiche.
3. Choisissez Commentaire dans le coin supérieur droit du tableau de bord. Cela permet d'ouvrir un formulaire. Après avoir fourni les commentaires, choisissez Soumettre.

Filtrage des résultats

Un filtre de recherche vous permet de visualiser les résultats correspondant aux critères que vous spécifiez et de filtrer les résultats non concordants. Vous pouvez facilement créer des filtres de recherche à l'aide de la GuardDuty console Amazon, ou vous pouvez les créer à l'CreateFilterAPIaide deJSON. Consultez les sections suivantes pour comprendre comment créer un filtre dans la console. Pour utiliser ces filtres afin d'archiver automatiquement les résultats entrants, veuillez consulter Règles de suppression.

Création de filtres dans la GuardDuty console

Les filtres de recherche peuvent être créés et testés via la GuardDuty console. Vous pouvez enregistrer les filtres créés via la console pour les utiliser dans les règles de suppression ou les futures opérations de filtrage. Un filtre est composé d'au moins un critère de filtre, qui consiste en un attribut de filtre associé à au moins une valeur.

Lorsque vous créez des filtres, soyez conscient de ce qui suit :

- Les filtres n'acceptent pas les caractères génériques.
- Vous pouvez spécifier un minimum d'un attribut et un maximum de 50 attributs comme critères pour un filtre particulier.
- Lorsque vous utilisez la condition equal to ou not equal to pour filtrer sur une valeur d'attribut telle que l'ID de compte, vous pouvez spécifier 50 valeurs au maximum.

- Chaque attribut de critères de filtre est évalué en tant qu'opérateur AND. Plusieurs valeurs pour le même attribut sont évaluées comme AND/OR.

Pour filtrer des résultats (console)

1. Sous Filtrer par attribut, choisissez Ajouter des critères de filtre. Cela vous montrera une liste étendue d'attributs de filtre.
2. Dans la liste étendue des attributs, sélectionnez l'attribut que vous souhaitez spécifier comme critère pour votre filtre, tel que l'ID de compte ou le type d'action.

   Pour obtenir la liste complète des attributs, voirAttributs du filtre.
3. Dans le champ de texte affiché, spécifiez une valeur pour l'attribut sélectionné, puis choisissez Appliquer.
4. Pour ajouter plusieurs critères de filtre, répétez les étapes 1 à 3.
5. Par défaut, la liste affiche les résultats correspondant au filtre appliqué. Si vous souhaitez afficher les résultats qui ne correspondent pas à l'attribut du filtre, choisissez Exclure à côté du filtre.

6. Enregistrez les attributs et valeurs spécifiés sous forme de filtres

   a. Pour enregistrer les attributs spécifiés et leurs valeurs (critères de filtre) sous forme de filtre, sélectionnez Enregistrer/Modifier.

   b. Entrez le nom et la description de la règle de filtrage.

   c. Choisissez Save (Enregistrer).

Attributs du filtre

Lorsque vous créez des filtres ou que vous triez des résultats à l'aide API des opérations, vous devez spécifier des critères de filtre dansJSON. Ces critères de filtrage sont en corrélation avec les détails JSON d'un résultat. Le tableau suivant contient la liste des noms d'affichage de la console pour les attributs de filtre et leurs noms de JSON champs équivalents.

Nom de champ de console	Nom de champ JSON
ID de compte	accountId
ID de résultat	id
Région	region
Sévérité	severity Vous pouvez filtrer les types de résultats en fonction de leur niveau de gravité. Pour plus d'informations sur les valeurs de gravité, consultezNiveaux de gravité des GuardDuty résultats. Si vous utilisez `severity` avec API AWS CLI, ou AWS CloudFormation, une valeur numérique lui est attribuée. Pour plus d'informations, consultez findingCriteriale Amazon GuardDuty API Reference.
Type de résultat	type
Mis à jour le	updatedAt
ID de clé d'accès	ressource. accessKeyDetails. accessKeyId
ID principal	ressource. accessKeyDetails. principalId
Nom d'utilisateur	ressource. accessKeyDetails. userName
Type utilisateur	ressource. accessKeyDetails. userType
IAMID de profil d'instance	ressource. instanceDetails. iamInstanceProfile .id
ID d'instance	ressource. instanceDetails. instanceId
ID d'image d'instance	ressource. instanceDetails. imageId
Clé de balise d'instance	ressource. instanceDetails.tags .key

Nom de champ de console	Nom de champ JSON
Valeur de balise d'instance	ressource. instanceDetails.tags .valeur
IPv6adresse	ressource. instanceDetails. networkInterfaces. Adresses IPv6
IPv4Adresse privée	ressource. instanceDetails. networkInterfaces. privateIpAddresses. privateIpAddress
DNSNom public	ressource. instanceDetails. networkInterfaces. publicDnsName
IP publique	ressource. instanceDetails. networkInterfaces. publicIp
ID du groupe de sécurité	ressource. instanceDetails. networkInterfaces. securityGroups. groupId
Nom du groupe de sécurité	ressource. instanceDetails. networkInterfaces. securityGroups. groupName
ID de sous-réseau (subnet)	ressource. instanceDetails. networkInterfaces. subnetId
VPCID	ressource. instanceDetails. networkInterfaces. vpcId
Avant-poste ARN	ressource. instanceDetails.avant-poste ARN
Type de ressource	ressource. resourceType
Autorisations du compartiment	ressource.s3. BucketDetails publicAccess. effectivePermission
Nom du compartiment	resource.s3 .name BucketDetails
Clé de balise du compartiment	ressource.s3 .tags .key BucketDetails
Valeur de balise de compartiment	ressource.s3 .tags .value BucketDetails

Nom de champ de console	Nom de champ JSON
Type de compartiment	ressource.s3 .type BucketDetails
Type d'action	service.action. actionType
APIappelé	service.action. awsApiCallAPI d'action
APItype d'appelant	service.action. awsApiCallAction. callerType
APICode d'erreur	service.action. awsApiCallAction. errorCode
APIville de l'appelant	service.action. awsApiCallAction. remoteIpDetails.ville. cityName
APIpays de l'appelant	service.action. awsApiCallAction. remoteIpDetails.pays. countryName
APIadresse de l'appelant IPv4	service.action. awsApiCallAction. remoteIpDetails. ipAddressV4
APIadresse de l'appelant IPv6	service.action. awsApiCallAction. remoteIpDetails. ipAddressV6
APIidentification de l'appelant ASN	service.action. awsApiCallAction. remoteIpDetails.organisation.asn
APInom de l'appelant ASN	service.action. awsApiCallAction. remoteIpDetails.organisation. asnOrg
APInom du service de l'appelant	service.action. awsApiCallAction. serviceName
DNSdomaine de demande	service.action. dnsRequestAction.domaine
DNSdemander un suffixe de domaine	service.action. dnsRequestAction. domainWithSuffix
Connexion réseau bloquée	service.action. networkConnectionAction.bloqué

Nom de champ de console	Nom de champ JSON
Direction de la connexion réseau	service.action. networkConnectionAction. connectionDirection
Port local de la connexion réseau	service.action. networkConnectionAction. localPortDetails.port
Protocole de la connexion réseau	service.action. networkConnectionAction.pro tocole
Ville de la connexion réseau	service.action. networkConnectionAction. remoteIpDetails.ville. cityName
Pays de la connexion réseau	service.action. networkConnectionAction. remoteIpDetails.pays. countryName
IPv4Adresse distante de connexion réseau	service.action. networkConnectionAction. remoteIpDetails. ipAddressV4
IPv6Adresse distante de connexion réseau	service.action. networkConnectionAction. remoteIpDetails. ipAddressV6
ASNID IP distant de connexion réseau	service.action. networkConnectionAction. remoteIpDetails.organisation.asn
ASNNom IP distant de la connexion réseau	service.action. networkConnectionAction. remoteIpDetails.organisation. asnOrg
Port distant de la connexion réseau	service.action. networkConnectionAction. remotePortDetails.port
Compte distant affilié	service.action. awsApiCallAction. remoteAcc ountDetails.affilié
Adresse de l'appelant Kubernetes API IPv4	service.action. kubernetesApiCallAction. remoteIpDetails. ipAddressV4
Adresse de l'appelant Kubernetes API IPv6	service.action. kubernetesApiCallAction. remoteIpDetails. ipAddressV6

Nom de champ de console	Nom de champ JSON
Espace de noms Kubernetes	service.action. kubernetesApiCallAction.Namespace
Identifiant de l'appelant Kubernetes API ASN	service.action. kubernetesApiCallAction. remoteIpDetails.organisation.asn
Demande d'appel Kubernetes API URI	service.action. kubernetesApiCallAction. requestUri
Code d'état de Kubernetes API	service.action. kubernetesApiCallAction. statusCode
IPv4Adresse locale de connexion réseau	service.action. networkConnectionAction. localIpDetails. ipAddressV4
IPv6Adresse locale de connexion réseau	service.action. networkConnectionAction. localIpDetails. ipAddressV6
Protocole	service.action. networkConnectionAction.protocole
APInom du service d'appel	service.action. awsApiCallAction. serviceName
APIID du compte de l'appelant	service.action. awsApiCallAction. remoteAccountDetails. accountId
Nom de la liste des menaces	service. additionalInfo. threatListName
Rôle de ressource	service. resourceRole
EKSnom du cluster	ressource. eksClusterDetails.nom
Nom de charge de travail Kubernetes	ressource. kubernetesDetails. kubernetesWorkloadDetails.nom
Espace de noms de charge de travail Kubernetes	ressource. kubernetesDetails. kubernetesWorkloadDetails.namespace

Nom de champ de console	Nom de champ JSON
Nom d'utilisateur Kubernetes	ressource. kubernetesDetails. kubernetesUserDetails.nom d'utilisateur
Image de conteneur Kubernetes	ressource. kubernetesDetails. kubernetesWorkloadDetails.conteneurs.image
Préfixe de l'image de conteneur Kubernetes	ressource. kubernetesDetails. kubernetesWorkloadDetails.conteneurs. imagePrefix
ID de numérisation	service. ebsVolumeScanDétails. scanId
EBSnom de la menace d'analyse des volumes	service. ebsVolumeScanDétails. scanDetections. threatDetectedByNom. threatNames.nom
Nom de la menace de scan d'objets S3	service. malwareScanDetails.threats .name
Gravité de la menace	service. ebsVolumeScanDétails. scanDetections. threatDetectedByNom. threatNames.gravité
Dossier SHA	service. ebsVolumeScanDétails. scanDetections. threatDetectedByNom. threatNames. filePaths.hachage
ECSnom du cluster	ressource. ecsClusterDetails.nom
ECSimage du conteneur	ressource. ecsClusterDetails. taskDetails.conteneurs.image
ECSdéfinition de la tâche ARN	ressource. ecsClusterDetails. taskDetails. definitionArn
Image de conteneur autonome	ressource. containerDetails.image
ID d'instance de base de données	ressource. rdsDbInstanceDétails. dbInstanceIdentifier

Nom de champ de console	Nom de champ JSON
ID de cluster de base de données	ressource. rdsDbInstanceDétails. dbCluster Identifier
Moteur de base de données	ressource. rdsDbInstanceDétails. Moteur
Utilisateur de la base de donnée	ressource. rdsDbUserDetails.user
Clé de balise d'instance de base de données	ressource. rdsDbInstanceDetails.tags.key
Valeur de balise d'instance de base de données	ressource. rdsDbInstanceDetails.tags.value
Exécutable SHA -256	service. runtimeDetails.processus. executabl eSha256
Nom du processus	service. runtimeDetails.process.name
Chemin exécutable	service. runtimeDetails.processus. executabl ePath
Nom de fonction Lambda	ressource. lambdaDetails. functionName
Fonction Lambda ARN	ressource. lambdaDetails. functionArn
Clé de balise de fonction Lambda	ressource. lambdaDetails.tags .key
Valeur de balise de fonction Lambda	ressource. lambdaDetails.tags .valeur
DNSdomaine de demande	service.action. dnsRequestAction. domainWit hSuffix

Règles de suppression

Une règle de suppression est un ensemble de critères, composés d'un attribut de filtre associé à une valeur, utilisés pour filtrer les résultats en archivant automatiquement les nouveaux résultats qui correspondent aux critères spécifiés. Les règles de suppression peuvent être utilisées pour filtrer les résultats de faible valeur, les faux positifs ou les menaces sur lesquelles vous n'avez pas l'intention

d'agir. Cela facilite la reconnaissance des menaces de sécurité ayant le plus d'impact sur votre environnement.

Après avoir créé une règle de suppression, les nouveaux résultats qui correspondent aux critères définis dans la règle sont automatiquement archivés tant que la règle de suppression est active. Vous pouvez utiliser un filtre existant pour créer une règle de suppression ou créer une règle de suppression à partir d'un nouveau filtre que vous définissez. Vous pouvez configurer des règles de suppression pour supprimer des types de recherche entiers ou définir des critères de filtre plus précis afin de supprimer uniquement des instances spécifiques d'un type de résultat particulier. Vous pouvez modifier les règles de suppression à tout moment.

Les résultats supprimés ne sont pas envoyés à AWS Security Hub Amazon Simple Storage Service, Amazon Detective ou Amazon EventBridge, ce qui réduit le niveau de bruit si vous consultez GuardDuty les résultats via Security Hub, un tiers SIEM ou d'autres applications d'alerte et de billetterie. Si vous l'avez activéProtection contre les logiciels malveillants pour EC2, les GuardDuty résultats supprimés ne lanceront pas d'analyse des logiciels malveillants.

GuardDuty continue de générer des résultats même s'ils correspondent à vos règles de suppression, mais ces résultats sont automatiquement marqués comme archivés. Les résultats archivés sont conservés GuardDuty pendant 90 jours et peuvent être consultés à tout moment pendant cette période. Vous pouvez afficher les résultats supprimés dans la GuardDuty console en sélectionnant Archivé dans le tableau des résultats ou GuardDuty API en utilisant le ListFindingsAPI`findingCriteria`critère `service.archived` égal à vrai.

> **Note**
>
> Dans un environnement multi-comptes, seul l' GuardDuty administrateur peut créer des règles de suppression.

Cas d'utilisation courants des règles de suppression et exemples

Les types de recherche suivants présentent des cas d'utilisation courants pour appliquer des règles de suppression. Sélectionnez le nom du résultat pour en savoir plus sur ce résultat. Consultez la description du cas d'utilisation pour décider si vous souhaitez créer une règle de suppression pour ce type de recherche.

> **Important**
>
> GuardDuty recommande de créer des règles de suppression de manière réactive et uniquement pour les résultats pour lesquels vous avez identifié à plusieurs reprises des faux positifs dans votre environnement.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS— Utilisez une règle de suppression pour archiver automatiquement les résultats générés lorsque le VPC réseau est configuré pour acheminer le trafic Internet de manière à ce qu'il sorte d'une passerelle locale plutôt que d'une passerelle VPC Internet.

  Ce résultat est généré lorsque le réseau est configuré pour acheminer le trafic Internet de manière à ce qu'il sorte d'une passerelle locale plutôt que d'une passerelle VPC Internet ()IGW. Les configurations courantes, telles que l'utilisation AWS Outpostsou VPC VPN les connexions, peuvent entraîner le routage du trafic de cette façon. Si ce comportement est attendu, il est recommandé d'utiliser des règles de suppression et de créer une règle composée de deux critères de filtre. Le premier critère est le type de résultat, qui devrait être `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Le deuxième critère de filtre est l'IPv4adresse de l'APIappelant avec l'adresse IP ou la CIDR plage de votre passerelle Internet locale. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de recherche en fonction de l'adresse IP de l'APIappelant.

  ```
  Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
   API caller IPv4 address: 198.51.100.6
  ```

  > **Note**
  >
  > Pour inclure plusieurs API appelants, IPs vous pouvez ajouter un nouveau filtre d'IPv4adresse d'APIappelant pour chacun d'entre eux.

- Recon:EC2/Portscan : utilisez une règle de suppression pour archiver automatiquement les résultats lors de l'utilisation d'une application d'évaluation des vulnérabilités.

  La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `Recon:EC2/Portscan`. Le second critère de filtre doit correspondre à l'instance ou aux instances qui hébergent ces outils d'évaluation de vulnérabilité. Vous pouvez utiliser l'attribut ID d'image d'instance ou Valeur de balise en fonction

des critères identifiables avec les instances qui hébergent ces outils. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de recherche en fonction des instances présentant un certain type de rechercheAMI.

```
Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
```

- UnauthorizedAccess:EC2/SSHBruteForce : utilisez une règle de suppression pour archiver automatiquement les résultats lorsque la règle est ciblée sur des instances de bastion.

  Si la cible de la tentative de force brute est un hôte bastion, cela peut représenter le comportement attendu de votre AWS environnement. Dans ce cas, nous vous recommandons de configurer une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `UnauthorizedAccess:EC2/SSHBruteForce`. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui hébergent ces outils. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de résultat en fonction des instances avec une certaine valeur de balise d'instance.

  ```
  Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
  ```

- Recon:EC2/PortProbeUnprotectedPort : utilisez une règle de suppression pour archiver automatiquement les résultats lorsque la règle est ciblée sur des instances exposées intentionnellement.

  Dans certains cas, les instances peuvent être intentionnellement exposées, par exemple si elles hébergent des serveurs Web. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce résultat. La règle de suppression doit comprendre deux critères de filtre. Le premier critère doit utiliser l'attribut Finding type (Type de résultat) avec la valeur `Recon:EC2/PortProbeUnprotectedPort`. Le second critère de filtre doit correspondre à l'instance ou aux instances qui servent d'hôte bastion. Vous pouvez utiliser l'attribut ID d'image d'instance ou l'attribut de valeur Balise en fonction du critère identifiable avec les instances qui hébergent ces outils. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de résultat en fonction des instances avec une certaine clé de balise d'instance dans la console.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Règles de suppression recommandées pour les résultats de la surveillance du temps d'exécution

- PrivilegeEscalation:Runtime/DockerSocketAccessed est généré lorsqu'un processus à l'intérieur d'un conteneur communique avec le socket Docker. Certains conteneurs de votre environnement peuvent avoir besoin d'accéder au socket Docker pour des raisons légitimes. L'accès à partir de tels conteneurs générera un résultat PrivilegeEscalation:Runtime/DockerSocketAccessed. Si tel est le cas dans votre AWS environnement, nous vous recommandons de définir une règle de suppression pour ce type de recherche. Le premier critère doit utiliser l'attribut Type de résultat avec la valeur `PrivilegeEscalation:Runtime/DockerSocketAccessed`. Le deuxième critère de filtre est le champ Chemin exécutable dont la valeur est égale à celle du `executablePath` du processus dans le résultat généré. Le deuxième critère de filtre peut également utiliser le champ exécutable SHA -256 avec une valeur égale à celle du processus `executableSha256` dans le résultat généré.
- Les clusters Kubernetes exécutent leurs propres DNS serveurs sous forme de pods, tels que. `coredns` Par conséquent, pour chaque DNS recherche à partir d'un module, GuardDuty capture deux DNS événements : l'un provenant du module et l'autre du module du serveur. Cela peut générer des doublons pour les résultats suivants : DNS
  - Backdoor:Runtime/C&CActivity.B!DNS
  - CryptoCurrency:Runtime/BitcoinTool.B!DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation
  - Impact:Runtime/BitcoinDomainRequest.Reputation
  - Impact:Runtime/MaliciousDomainRequest.Reputation
  - Impact:Runtime/SuspiciousDomainRequest.Reputation
  - Trojan:Runtime/BlackholeTraffic!DNS
  - Trojan:Runtime/DGADomainRequest.C!DNS
  - Trojan:Runtime/DriveBySourceTraffic!DNS
  - Trojan:Runtime/DropPoint!DNS
  - Trojan:Runtime/PhishingDomainRequest!DNS

  Les résultats dupliqués incluront les détails du pod, du conteneur et du processus correspondant à votre pod de DNS serveur. Vous pouvez définir une règle de suppression pour supprimer ces résultats en double à l'aide de ces champs. Les premiers critères de filtre doivent utiliser le champ Type de recherche dont la valeur est égale à un type de DNS recherche figurant dans la liste

des résultats fournie plus haut dans cette section. Le deuxième critère de filtre peut être soit le chemin exécutable avec une valeur égale à celle de votre DNS serveur, `executablePath` soit l'exécutable SHA -256 avec une valeur égale à celle de votre DNS serveur `executableSHA256` dans le résultat généré. En tant que troisième critère de filtre facultatif, vous pouvez utiliser le champ d'image de conteneur Kubernetes avec une valeur égale à l'image de conteneur de votre pod de DNS serveur dans le résultat généré.

Création de règles de suppression

Choisissez votre méthode d'accès préférée pour créer une règle de suppression permettant de GuardDuty rechercher des types.

Console

Vous pouvez visualiser, créer et gérer des règles de suppression à l'aide de la GuardDuty console. Les règles de suppression sont générées de la même manière que les filtres, et les filtres enregistrés existants peuvent être utilisés comme règles de suppression. Pour plus d'informations sur la création de filtres, veuillez consulter Filtrage des résultats.

Pour créer une règle de suppression à l'aide de la console :

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Sur la page Résultats, choisissez Supprimer les résultats pour ouvrir le panneau des règles de suppression.
3. Pour ouvrir le menu des critères de filtre, entrez le **`filter criteria`** dans le champ Ajouter des critères de filtre. Vous pouvez choisir un critère dans la liste. Entrez une valeur valide pour le critère choisi.

> **Note**
>
> Pour déterminer la valeur valide, consultez le tableau des résultats et choisissez le résultat que vous souhaitez supprimer. Passez en revue ses détails dans le panneau des résultats.

Vous pouvez ajouter plusieurs critères de filtre et vous assurer que seuls les résultats que vous souhaitez supprimer apparaissent dans le tableau.

4. Entrez un nom et une description pour la règle de suppression. Les caractères valides sont le point (.), le trait de soulignement (_), le tiret (-) et les caractères alphanumériques.
5. Choisissez Enregistrer.

Vous pouvez également créer une règle de suppression à partir d'un filtre enregistré existant. Pour plus d'informations sur la création de filtres, veuillez consulter Filtrage des résultats.

Pour créer une règle de suppression à partir d'un filtre enregistré :

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Sur la page Résultats, choisissez Supprimer les résultats pour ouvrir le panneau des règles de suppression.
3. Dans le menu déroulant Règles enregistrées, choisissez un filtre enregistré.
4. Vous pouvez également ajouter de nouveaux critères de filtre. Si vous n'avez pas besoin de critères de filtre supplémentaires, ignorez cette étape.

   Pour ouvrir le menu des critères de filtre, entrez le **`filter criteria`** dans le champ Ajouter des critères de filtre. Vous pouvez choisir un critère dans la liste. Entrez une valeur valide pour le critère choisi.

   > **Note**
   >
   > Pour déterminer la valeur valide, consultez le tableau des résultats et choisissez le résultat que vous souhaitez supprimer. Passez en revue ses détails dans le panneau des résultats.

5. Entrez un nom et une description pour la règle de suppression. Les caractères valides sont le point (.), le trait de soulignement (_), le tiret (-) et les caractères alphanumériques.
6. Choisissez Enregistrer.

API/CLI

Pour créer une règle de suppression à l'aide de API :

1. Vous pouvez créer des règles de suppression par le biais du CreateFilterAPI. Pour ce faire, spécifiez les critères de filtre dans un JSON fichier au format de l'exemple détaillé ci-dessous. L'exemple ci-dessous supprimera tous les résultats de faible gravité non archivés contenant

une DNS demande adressée au domaine test.example.com. Pour les résultats de gravité moyenne, la liste d'entrée sera `["4", "5", "7"]`. Pour les résultats de gravité élevée, la liste d'entrée sera `["6", "7", "8"]`. Vous pouvez également filtrer en fonction de n'importe quelle valeur de la liste.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Pour une liste des noms de JSON champs et de leur équivalent sur console, voirAttributs du filtre.

Pour tester les critères de votre filtre, utilisez le même JSON critère dans le ListFindingsAPIet vérifiez que les bons résultats ont été sélectionnés. Pour tester vos critères de filtre, AWS CLI suivez l'exemple en utilisant votre propre fichier detectorId et un fichier .json.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Téléchargez votre filtre à utiliser comme règle de suppression avec CreateFilterAPIou en utilisant l' AWS CLIexemple ci-dessous avec votre propre identifiant de détecteur, un nom pour la règle de suppression et un fichier .json.

   Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

   ```
   aws guardduty create-filter --action ARCHIVE --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
    file://criteria.json
   ```

Vous pouvez afficher la liste de vos filtres par programmation à l'aide du. ListFilterAPI Vous pouvez consulter les détails d'un filtre individuel en fournissant le nom du filtre au GetFilterAPI. Mettez à jour les filtres en utilisant UpdateFilterou supprimez-les à l'aide du DeleteFilterAPI.

Suppression de règles de suppression

Choisissez votre méthode d'accès préférée pour supprimer une règle de suppression permettant de GuardDuty rechercher des types.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Sur la page Résultats, choisissez Supprimer les résultats pour ouvrir le panneau des règles de suppression.
3. Dans le menu déroulant Règles enregistrées, choisissez un filtre enregistré.
4. Choisissez Delete rule (Supprimer la règle).

API/CLI

Exécutez le DeleteFilterAPI. Spécifiez le nom du filtre et l'ID du détecteur associé pour la région en question.

Vous pouvez également utiliser l' AWS CLI exemple suivant en remplaçant les valeurs formatées dans *red*:

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

Utilisation de listes d'adresses IP approuvées et de listes de menaces

Amazon GuardDuty surveille la sécurité de votre AWS environnement en analysant et en traitant les journaux de VPC flux, les journaux d' AWS CloudTrail événements et DNS les journaux. Vous pouvez personnaliser cette étendue de surveillance en la configurant de manière GuardDuty à arrêter les alertes relatives aux personnes fiables à IPs partir de vos propres listes d'adresses IP fiables et à émettre des alertes en cas IPs de maliciel connu à partir de vos propres listes de menaces.

Les listes d'adresses IP approuvées et les listes de menaces s'appliquent uniquement au trafic destiné aux adresses IP publiquement routables. Les effets d'une liste s'appliquent à tous les journaux de VPC flux et à tous CloudTrail les résultats, mais pas aux DNS résultats.

GuardDuty peut être configuré pour utiliser les types de listes suivants.

Liste d'adresses IP approuvées

Les listes d'adresses IP fiables sont des adresses IP auxquelles vous avez fait confiance pour sécuriser les communications avec votre AWS infrastructure et vos applications. GuardDuty ne génère pas de journal de VPC flux ni de CloudTrail résultats pour les adresses IP figurant sur des listes d'adresses IP fiables. Vous pouvez inclure un maximum de 2 000 adresses IP et CIDR plages dans une seule liste d'adresses IP fiables. À tout moment, vous pouvez avoir seulement une liste d'adresses IP approuvées chargée par compte AWS et par région.

Liste d'adresses IP de menaces

Les listes de menaces répertorient les adresses IP malveillantes connues. Cette liste peut être fournie par des renseignements tiers sur les menaces ou créée spécifiquement pour votre organisation. En plus de générer des résultats en raison d'une activité potentiellement suspecte, il génère GuardDuty également des résultats basés sur ces listes de menaces. Vous pouvez inclure un maximum de 250 000 adresses IP et CIDR plages dans une seule liste de menaces.

GuardDuty génère uniquement des résultats basés sur une activité impliquant des adresses IP et des CIDR plages dans vos listes de menaces ; les résultats ne sont pas générés sur la base des noms de domaine. À tout moment, vous pouvez télécharger jusqu'à six listes de menaces Compte AWS par région.

> **Note**
>
> Si vous incluez la même adresse IP à la fois dans une liste d'adresses IP approuvées et dans une liste de menaces, elle sera d'abord traitée par la liste d'adresses IP approuvées et ne générera aucun résultat.

Dans les environnements multicomptes, seuls les utilisateurs GuardDuty disposant de comptes d'administrateur peuvent ajouter et gérer des listes d'adresses IP fiables et des listes de menaces. Les listes d'adresses IP fiables et les listes de menaces téléchargées par le compte administrateur sont imposées aux GuardDuty fonctionnalités de ses comptes membres. En d'autres termes, les comptes membres GuardDuty génèrent des résultats basés sur des activités impliquant des adresses IP malveillantes connues figurant dans les listes de menaces du compte administrateur, mais ne génère pas de résultats basés sur des activités impliquant des adresses IP figurant dans les listes d'adresses IP fiables du compte administrateur. Pour de plus amples informations, veuillez consulter Gestion de plusieurs comptes sur Amazon GuardDuty.

Formats de liste

GuardDuty accepte les listes dans les formats suivants.

La taille maximale de chaque fichier hébergeant votre liste d'adresses IP autorisées ou liste d'adresses IP de menaces est de 35 Mo. Dans vos listes d'adresses IP fiables et de menaces, les adresses IP et les CIDR plages d'adresses IP doivent apparaître une par ligne. Seules IPv4 les adresses sont acceptées.

- Texte brut () TXT

  Ce format prend en charge à la fois les adresses IP par CIDR blocs et les adresses IP individuelles. La liste d'exemples suivante utilise le format Plaintext (TXT).

```
192.0.2.0/24
198.51.100.1
```

```
203.0.113.1
```

- Expression structurée des informations sur les menaces (STIX)

  Ce format prend en charge à la fois les adresses IP par CIDR blocs et les adresses IP individuelles. La liste d'exemples suivante utilise ce STIX format.

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
```

```
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- Ouvrez Threat Exchange (OTX) ™ CSV

  Ce format prend en charge à la fois les adresses IP par CIDR blocs et les adresses IP individuelles. La liste d'exemples suivante utilise ce `OTX`™ CSV format.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ est le renseignement SIGHT sur les menaces CSV

  Ce format prend en charge à la fois les adresses IP par CIDR blocs et les adresses IP individuelles. La liste d'exemples suivante utilise un `FireEye`™ CSV format.

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
```

```
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- Fil d'information Proofpoint ™ ET CSV

  Ce format ne prend en charge que les adresses IP individuelles. La liste d'exemples suivante utilise ce `Proofpoint` CSV format. Le paramètre `ports` est facultatif. Si vous ignorez le port, veillez à laisser une virgule (,) à la fin.

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVaultFil de réputation ™

  Ce format ne prend en charge que les adresses IP individuelles. La liste d'exemples suivante utilise le format `AlienVault`.

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Autorisations requises pour charger les listes d'adresses IP approuvées et les listes de menaces

Les différentes IAM identités nécessitent des autorisations spéciales pour pouvoir utiliser des listes d'adresses IP fiables et des listes de menaces GuardDuty. Une identité avec la stratégie gérée AmazonGuardDutyFullAccess attachée peut uniquement renommer et désactiver les listes d'adresses IP approuvées et les listes des menaces chargées .

Pour accorder à différentes identités un accès complet à la gestion des listes d'adresses IP approuvées et des listes des menaces (en plus de renommer et de désactiver, cela inclut l'ajout, l'activation, la suppression et la mise à jour de l'emplacement ou du nom des listes), assurez-vous que les actions suivantes sont présentes dans la stratégie d'autorisations attachée à un utilisateur, un groupe ou un rôle :

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Ces actions ne sont pas incluses dans la politique gérée `AmazonGuardDutyFullAccess`.

Utilisation du chiffrement côté serveur pour les listes d'adresses IP approuvées et les listes de menaces

GuardDuty prend en charge les types de chiffrement suivants pour les listes : SSE - AES256 et SSE - KMS. SSE-C n'est pas pris en charge. Pour de plus amples informations sur les types de chiffrement pour S3, veuillez consulter Protection des données à l'aide du chiffrement côté serveur.

Si votre liste est chiffrée à l'aide du chiffrement SSE côté serveur, KMS vous devez accorder au rôle GuardDuty lié au service l'AWSServiceRoleForAmazonGuardDutyautorisation de déchiffrer le fichier

afin d'activer la liste. Ajoutez la déclaration suivante à la politique KMS clé et remplacez l'identifiant du compte par le vôtre :

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Ajouter et activer une liste d'adresses IP approuvées ou une liste d'adresses IP de menaces

Choisissez l'une des méthodes d'accès suivantes pour ajouter et activer une liste d'adresses IP approuvées ou une liste d'adresses IP de menaces.

Console

(Facultatif) Étape 1 : Récupération de URL l'emplacement de votre liste

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le nom du compartiment Amazon S3 contenant la liste spécifique que vous souhaitez ajouter.
4. Choisissez le nom de l'objet (liste) pour en afficher les détails.
5. Sous l'onglet Propriétés, copiez le S3 URI de cet objet.

Étape 2 : ajout d'une liste d'adresses IP approuvées ou d'une liste de menaces

> **Important**
>
> Par défaut, à tout moment, vous pouvez avoir seulement une liste d'adresses IP approuvées. De même, vous pouvez avoir jusqu'à six listes de menaces.

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page List management, choisissez Add a trusted IP list ou Add a threat list.
4. En fonction de votre sélection, une boîte de dialogue s'affiche. Procédez comme suit :

   a. Pour Nom de la liste, saisissez un nom pour votre liste.

      Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, des tirets (-) et des traits de soulignement (_).

   b. Pour Emplacement, indiquez l'emplacement où vous avez chargé votre liste. Si vous ne l'avez pas encore fait, veuillez consulter Step 1: Fetching location URL of your list.

      Format de localisation URL

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3-aws-region.amazonaws.com/file.txt
      - s3://bucket.name/file.txt

   c. Cochez la case I agree.

   d. Choisissez Ajouter une liste. Par défaut, l'état de la liste ajoutée est Inactif. Pour que la liste soit effective, vous devez l'activer.

Étape 3 : activation d'une liste d'adresses IP approuvées ou d'une liste de menaces

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Gestion de la liste, sélectionnez la liste que vous souhaitez activer.
4. Choisissez Actions, puis Activer. L'entrée en vigueur de la liste peut prendre jusqu'à 15 minutes.

API/CLI

Pour les listes d'adresses IP approuvées

- Exécutez reateIPSetC. Assurez-vous de fournir l'`detectorId` compte membre pour lequel vous souhaitez créer cette liste d'adresses IP approuvées.

  Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, des tirets (-) et des traits de soulignement (_).

  - Vous pouvez également procéder en exécutant la commande AWS Command Line Interface suivante et en vous assurant de remplacer l'`detector-id` par l'ID de détecteur du compte membre pour lequel vous allez mettre à jour la liste d'adresses IP approuvées.

    ```
    aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
     --name AnyOrganization List --format Plaintext --location https://
    s3.amazonaws.com/amzn-s3-demo-bucket2/DOC-EXAMPLE-SOURCE-FILE.format --
    activate
    ```

Pour les listes de menaces

- Courez CreateThreatIntelSet. Assurez-vous de fournir l'`detectorId` compte membre pour lequel vous souhaitez créer cette liste de menaces.
  - Vous pouvez également le faire en exécutant la AWS Command Line Interface commande suivante. Assurez-vous de fournir l'`detectorId` compte membre pour lequel vous souhaitez créer une liste de menaces.

    ```
    aws guardduty create-threat-intel-set --detector-
    id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
    format Plaintext --location https://s3.amazonaws.com/amzn-s3-demo-bucket2/
    DOC-EXAMPLE-SOURCE-FILE.format --activate
    ```

> **Note**
>
> Après avoir activé ou mis à jour une liste d'adresses IP, la synchronisation de la liste GuardDuty peut prendre jusqu'à 15 minutes.

Mise à jour des listes d'adresses IP approuvées et des listes de menaces

Vous pouvez mettre à jour le nom d'une liste ou les adresses IP ajoutées à une liste déjà ajoutée et activée. Si vous mettez à jour une liste, vous devez la réactiver GuardDuty pour pouvoir utiliser la dernière version de la liste.

Choisissez l'une des méthodes d'accès pour mettre à jour une liste d'adresses IP approuvées ou une liste de menaces.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Gestion de la liste, sélectionnez l'ensemble d'adresses IP approuvées ou une liste de menaces que vous souhaitez mettre à jour.
4. Sélectionnez Actions, puis Edit (Modifier).
5. Dans la boîte de dialogue Mettre à jour la liste, mettez à jour les informations selon vos besoins.

   Contraintes de dénomination des listes : le nom de votre liste peut inclure des lettres minuscules, des lettres majuscules, des chiffres, des tirets (-) et des traits de soulignement (_).
6. Cochez la case J'accepte, puis sélectionnez Mettre à jour la liste. La valeur de la colonne État deviendra Inactif.
7. Réactivation de la liste mise à jour

   a. Sur la page Gestion de la liste, sélectionnez la liste que vous souhaitez réactiver.

   b. Choisissez Actions, puis Activer.

API/CLI

1. Exécutez UpdateIPSet pour mettre à jour une liste d'adresses IP approuvées.
   - Vous pouvez également exécuter la commande AWS CLI suivante pour mettre à jour une liste d'adresses IP approuvées et vous assurer de remplacer l'`detector-id` par l'ID de détecteur du compte membre pour lequel vous allez mettre à jour la liste d'adresses IP approuvées.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

2. Exécuter UpdateThreatIntelSet pour mettre à jour une liste de menaces
   - Vous pouvez également exécuter la commande AWS CLI suivante pour mettre à jour une liste de menaces et vous assurer de remplacer le `detector-id` par l'ID de détecteur du compte membre pour lequel vous allez mettre à jour la liste de menaces.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

Désactivation ou suppression d'une liste d'adresses IP approuvées ou d'une liste de menaces

Choisissez l'une des méthodes d'accès pour supprimer (à l'aide de la console) ou désactiver (en utilisantAPI/CLI) une liste d'adresses IP fiables ou une liste de menaces.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Listes.
3. Sur la page Gestion de la liste, sélectionnez la liste que vous souhaitez supprimer.
4. Choisissez Actions, puis Supprimer.
5. Confirmez l'action et sélectionnez Supprimer. La liste spécifique ne sera plus disponible dans le tableau.

API/CLI

1. Pour une liste d'adresses IP approuvées

   Exécutez UpdateIPSet pour mettre à jour une liste d'adresses IP approuvées.

   - Vous pouvez également exécuter la commande AWS CLI suivante pour mettre à jour une liste d'adresses IP approuvées et vous assurer de remplacer l'`detector-id` par l'ID de détecteur du compte membre pour lequel vous allez mettre à jour la liste d'adresses IP approuvées.

     Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     no-activate
     ```

2. Pour une liste de menaces

   Exécuter UpdateThreatIntelSet pour mettre à jour une liste de menaces

   - Vous pouvez également exécuter la commande AWS CLI suivante pour mettre à jour une liste d'adresses IP approuvées et vous assurer de remplacer l'`detector-id` par l'ID de détecteur du compte membre pour lequel vous allez mettre à jour la liste de menaces.

     ```
     aws guardduty update-threatintel-set --detector-
     id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
     intel-set-id d4b94fc952d6912b8f3060768example --no-activate
     ```

Exportation des résultats

GuardDuty conserve les résultats générés pendant une période de 90 jours. GuardDuty exporte les résultats actifs vers Amazon EventBridge (EventBridge). Vous pouvez éventuellement exporter les résultats générés vers un bucket Amazon Simple Storage Service (Amazon S3). Cela vous aidera à suivre les données historiques relatives aux activités potentiellement suspectes de votre compte et à évaluer si les mesures correctives recommandées ont été efficaces.

Tous les nouveaux résultats actifs GuardDuty générés sont automatiquement exportés environ 5 minutes après leur génération. Vous pouvez définir la fréquence à laquelle les mises à jour des résultats actifs sont exportées EventBridge. La fréquence que vous sélectionnez s'applique à l'exportation de nouvelles occurrences de résultats existants vers EventBridge votre compartiment S3 (lorsqu'il est configuré) et Detective (lorsqu'il est intégré). Pour plus d'informations sur la manière dont GuardDuty agrège plusieurs occurrences de résultats existants, voirGuardDuty recherche d'une agrégation.

Lorsque vous configurez les paramètres pour exporter les résultats vers un compartiment Amazon S3, GuardDuty utilise AWS Key Management Service (AWS KMS) pour chiffrer les données des résultats dans votre compartiment S3. Cela nécessite que vous ajoutiez des autorisations à votre compartiment S3 et à la AWS KMS clé afin que GuardDuty vous puissiez les utiliser pour exporter les résultats dans votre compte.

Table des matières

Considérations

Avant de passer aux prérequis et aux étapes nécessaires à l'exportation des résultats, tenez compte des concepts clés suivants :

- Les paramètres d'exportation sont régionaux : vous devez configurer les options d'exportation dans chaque région que vous utilisez GuardDuty.
- Exportation des résultats vers des compartiments Amazon S3 situés dans différents compartiments Régions AWS (entre régions) : GuardDuty prend en charge les paramètres d'exportation suivants :
  - Votre compartiment ou objet Amazon S3 et votre AWS KMS clé doivent appartenir au même Région AWS.
  - Pour les résultats générés dans une région commerciale, vous pouvez choisir d'exporter ces résultats vers un compartiment S3 dans n'importe quelle région commerciale. Toutefois, vous ne pouvez pas exporter ces résultats vers un compartiment S3 dans une région optionnelle.

  - Pour les résultats générés dans une région optionnelle, vous pouvez choisir d'exporter ces résultats vers la même région optionnelle où ils ont été générés ou vers n'importe quelle région commerciale. Toutefois, vous ne pouvez pas exporter les résultats d'une région optionnelle vers une autre région optionnelle.
- Autorisations d'exportation des résultats : pour configurer les paramètres d'exportation des résultats actifs, votre compartiment S3 doit disposer des autorisations GuardDuty permettant de télécharger des objets. Vous devez également disposer d'une AWS KMS clé qui GuardDuty peut être utilisée pour chiffrer les résultats.
- Les résultats archivés ne sont pas exportés : le comportement par défaut est que les résultats archivés, y compris les nouvelles instances de résultats supprimés, ne sont pas exportés.

  Lorsqu'une GuardDuty découverte est générée en tant qu'archive, vous devez la désarchiver. Cela fait passer le statut de recherche du filtre à Actif. GuardDuty exporte les mises à jour des résultats non archivés existants en fonction de votre configurationÉtape 5 — Fréquence d'exportation des résultats.
- GuardDuty le compte administrateur peut exporter les résultats générés dans les comptes membres associés — Lorsque vous configurez les résultats d'exportation dans un compte administrateur, tous les résultats des comptes membres associés générés dans la même région sont également exportés vers le même emplacement que celui que vous avez configuré pour le compte administrateur. Pour de plus amples informations, veuillez consulter Comprendre la relation entre le compte GuardDuty administrateur et les comptes membres.

Étape 1 — Autorisations requises pour exporter les résultats

Lorsque vous configurez les paramètres d'exportation des résultats, vous sélectionnez un compartiment Amazon S3 dans lequel vous pouvez stocker les résultats et une AWS KMS clé à utiliser pour le chiffrement des données. Outre les autorisations relatives aux GuardDuty actions, vous devez également être autorisé à effectuer les actions suivantes pour configurer correctement les paramètres d'exportation des résultats :

- `s3:GetBucketLocation`
- `s3:PutObject`
- `s3:ListBucket`

Étape 2 — Attacher une politique à votre KMS clé

GuardDuty chiffre les données de résultats de votre compartiment en utilisant AWS Key Management Service. Pour configurer correctement les paramètres, vous devez d'abord GuardDuty autoriser l'utilisation d'une KMS clé. Vous pouvez accorder les autorisations en attachant la politique à votre KMS clé.

Lorsque vous utilisez une KMS clé d'un autre compte, vous devez appliquer la politique en matière de clés en vous connectant au Compte AWS propriétaire de la clé. Lorsque vous configurez les paramètres pour exporter les résultats, vous aurez également besoin ARN de la clé du compte propriétaire de la clé.

Pour modifier la politique KMS clé permettant GuardDuty de chiffrer vos résultats exportés

1. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Sélectionnez une KMS clé existante ou suivez les étapes du guide du AWS Key Management Service développeur pour créer une nouvelle clé, que vous utiliserez pour chiffrer les résultats exportés.

   > **Note**
   >
   > Votre KMS clé et le compartiment Amazon S3 doivent être identiques. Région AWS

   Vous pouvez utiliser le même compartiment S3 et la même paire de KMS clés pour exporter les résultats depuis n'importe quelle région applicable. Pour plus d'informations, voir Considérations pour exporter les résultats d'une région à l'autre.
4. Dans la section Key policy (Politique de clé), choisissez Edit (Modifier).

   Si Basculer vers l'affichage des politiques est affiché, choisissez-le pour afficher la politique clé, puis choisissez Modifier.
5. Copiez le bloc de politique suivant dans votre politique de KMS clé, pour GuardDuty autoriser l'utilisation de votre clé.

```
{
    "Sid": "AllowGuardDutyKey",
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. Modifiez la politique en remplaçant les valeurs suivantes mises en forme dans *red*dans l'exemple de politique :

   1. Remplacez *KMS key ARN* avec le Amazon Resource Name (ARN) de la KMS clé. Pour localiser la cléARN, reportez-vous à la section Trouver l'identifiant de la clé et ARN au manuel du AWS Key Management Service développeur.
   2. Remplacez *123456789012* avec l' Compte AWS identifiant propriétaire du GuardDuty compte exportant les résultats.
   3. Remplacez *Region2* avec l' Région AWS endroit où les GuardDuty résultats sont générés.
   4. Remplacez *SourceDetectorID* avec le GuardDuty compte `detectorID` de la région spécifique où les résultats ont été générés.

      Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

> **Note**
>
> Si vous l'utilisez GuardDuty dans une région optionnelle, remplacez la valeur du « Service » par le point de terminaison régional de cette région. Par exemple, si vous utilisez GuardDuty dans la région Moyen-Orient (Bahreïn) (me-south-1), remplacez par. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Pour plus d'informations sur les points de terminaison

pour chaque région optionnelle, consultez la section GuardDuty Points de terminaison et quotas.

7. Si vous avez ajouté la déclaration de politique avant la déclaration finale, ajoutez une virgule avant d'ajouter cette déclaration. Assurez-vous que la JSON syntaxe de votre politique KMS clé est valide.

   Choisissez Save (Enregistrer).

8. (Facultatif) copiez la clé ARN dans un bloc-notes pour l'utiliser dans les étapes ultérieures.

Étape 3 — Attacher une politique au compartiment Amazon S3

Ajoutez des autorisations au compartiment Amazon S3 vers lequel vous allez exporter les résultats afin de GuardDuty pouvoir télécharger des objets dans ce compartiment S3. Indépendamment de l'utilisation d'un compartiment Amazon S3 appartenant à votre compte ou à un autre Compte AWS, vous devez ajouter ces autorisations.

Si, à un moment donné, vous décidez d'exporter les résultats vers un autre compartiment S3, pour continuer à exporter les résultats, vous devez ajouter des autorisations à ce compartiment S3 et reconfigurer les paramètres d'exportation des résultats.

Si vous ne possédez pas encore de compartiment Amazon S3 dans lequel vous souhaitez exporter ces résultats, consultez la section Création d'un compartiment dans le guide de l'utilisateur Amazon S3.

Pour associer des autorisations à votre politique de compartiment S3

1. Effectuez les étapes décrites dans la section Pour créer ou modifier une politique de compartiment dans le guide de l'utilisateur d'Amazon S3, jusqu'à ce que la page Modifier la politique de compartiment apparaisse.
2. L'exemple de politique montre comment accorder GuardDuty l'autorisation d'exporter les résultats vers votre compartiment Amazon S3. Si vous modifiez le chemin après avoir configuré les résultats de l'exportation, vous devez modifier la politique pour autoriser le nouvel emplacement.

   Copiez l'exemple de politique suivant et collez-le dans l'éditeur de politique Bucket.

Si vous avez ajouté la déclaration de politique avant la déclaration finale, ajoutez une virgule avant d'ajouter cette déclaration. Assurez-vous que la JSON syntaxe de votre politique KMS clé est valide.

Exemple de stratégie de compartiment S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
```

```
            }
        }
    },
    {
        "Sid": "DenyUnencryptedUploadsThis is optional",
        "Effect": "Deny",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": "aws:kms"
            }
        }
    },
    {
        "Sid": "DenyIncorrectHeaderThis is optional",
        "Effect": "Deny",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
            }
        }
    },
    {
        "Sid": "DenyNon-HTTPS",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        }
    }
```

```
    ]
}
```

3. Modifiez la politique en remplaçant les valeurs suivantes mises en forme dans *red*dans l'exemple de politique :

   1. Remplacez *Amazon S3 bucket ARN* avec le nom de ressource Amazon (ARN) du compartiment Amazon S3. Vous pouvez trouver le bucket ARN sur la page Modifier la politique du bucket de la https://console.aws.amazon.com/s3/console.
   2. Remplacez *123456789012* avec l' Compte AWS identifiant propriétaire du GuardDuty compte exportant les résultats.
   3. Remplacez *Region2* avec l' Région AWS endroit où les GuardDuty résultats sont générés.
   4. Remplacez *SourceDetectorID* avec le GuardDuty compte `detectorID` de la région spécifique où les résultats ont été générés.

      Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.
   5. Remplacez *[optional prefix]* partie du *S3 bucket ARN/[optional prefix]* valeur d'espace réservé avec un emplacement de dossier facultatif vers lequel vous souhaitez exporter les résultats. Pour plus d'informations sur l'utilisation des préfixes, consultez la section Organisation des objets à l'aide de préfixes dans le guide de l'utilisateur Amazon S3.

      Lorsque vous fournissez un emplacement de dossier facultatif qui n'existe pas encore, vous ne GuardDuty créerez cet emplacement que si le compte associé au compartiment S3 est le même que le compte exportant les résultats. Lorsque vous exportez des résultats vers un compartiment S3 appartenant à un autre compte, l'emplacement du dossier doit déjà exister.
   6. Remplacez *KMS key ARN* avec le Amazon Resource Name (ARN) de la KMS clé associée au chiffrement des résultats exportés vers le compartiment S3. Pour localiser la cléARN, reportez-vous à la section Trouver l'identifiant de la clé et ARN au manuel du AWS Key Management Service développeur.

   > **Note**
   >
   > Si vous l'utilisez GuardDuty dans une région optionnelle, remplacez la valeur du « Service » par le point de terminaison régional de cette région. Par exemple, si vous utilisez GuardDuty dans la région Moyen-Orient (Bahreïn) (me-south-1), remplacez par.

`"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Pour plus d'informations sur les points de terminaison pour chaque région optionnelle, consultez la section GuardDuty Points de terminaison et quotas.

4. Choisissez Save (Enregistrer).

Étape 4 - Exportation des résultats vers un compartiment S3 (console)

GuardDuty vous permet d'exporter les résultats vers un compartiment existant dans un autre Compte AWS.

Lorsque vous créez un nouveau compartiment S3 ou que vous choisissez un compartiment existant dans votre compte, vous pouvez ajouter un préfixe facultatif. Lors de la configuration des résultats d'exportation, GuardDuty crée un nouveau dossier dans le compartiment S3 pour vos résultats. Le préfixe sera ajouté à la structure de dossiers par défaut créée. GuardDuty Par exemple, le format du préfixe `/AWSLogs/123456789012/GuardDuty/Region` facultatif.

Le chemin complet de l'objet S3 sera`amzn-s3-demo-bucket/prefix-name/UUID.jsonl.gz`. Le `UUID` est généré de manière aléatoire et ne représente pas l'ID du détecteur ou l'ID de recherche.

> **Important**
>
> La KMS clé et le compartiment S3 doivent se trouver dans la même région.

Avant de terminer ces étapes, assurez-vous d'avoir attaché les politiques correspondantes à votre KMS clé et à votre compartiment S3 existant.

Pour configurer les résultats de l'exportation

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Paramètres, sous Options d'exportation des résultats, pour le compartiment S3, choisissez Configurer maintenant (ou Modifier, selon les besoins).
4. Pour le compartiment S3 ARN, entrez le**`bucket ARN`**. Pour trouver le compartimentARN, consultez la section Affichage des propriétés d'un compartiment S3 dans le guide de l'utilisateur

Amazon S3. Dans l'onglet Autorisations de la page Propriétés du bucket associé dans la https://console.aws.amazon.com/guardduty/console.

5. Pour KMSla clé ARN, entrez le **`key ARN`**. Pour localiser la cléARN, reportez-vous à la section Trouver l'identifiant de la clé et ARN au manuel du AWS Key Management Service développeur.
6. Joindre des politiques

   - Procédez comme suit pour associer la politique du compartiment S3. Pour de plus amples informations, veuillez consulter Étape 3 — Attacher une politique au compartiment Amazon S3.

   - Procédez comme suit pour joindre la politique KMS clé. Pour de plus amples informations, veuillez consulter Étape 2 — Attacher une politique à votre KMS clé.
7. Choisissez Save (Enregistrer).

Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour

Configurez la fréquence d'exportation des résultats actifs mis à jour en fonction de votre environnement. Par défaut, les conclusions mises à jour sont exportées toutes les 6 heures. Cela signifie que tous les résultats mis à jour après l'exportation la plus récente sont inclus dans la nouvelle exportation. Si les résultats mis à jour sont exportés toutes les 6 heures et que l'exportation se produit à 12 h, tout résultat mis à jour après 12 h est exporté à 18 h.

Pour définir la fréquence

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Sélectionnez Settings (Paramètres).
3. Dans la section Options d'exportation des résultats choisissez Fréquence des résultats mis à jour. Cela définit la fréquence d'exportation des résultats actifs mis à jour à la fois vers Amazon S3 EventBridge et vers Amazon S3. Sélectionnez parmi les éléments suivants :

   - Mise à jour EventBridge et S3 toutes les 15 minutes
   - Mise à jour EventBridge et S3 toutes les 1 heure
   - Mise à jour CWE et S3 toutes les 6 heures (par défaut)
4. Sélectionnez Enregistrer les modifications.

Création de réponses personnalisées aux GuardDuty résultats avec Amazon CloudWatch Events

GuardDuty crée un événement pour Amazon CloudWatch Events en cas de modification des résultats. Les modifications susceptibles de créer un CloudWatch événement incluent des résultats récemment générés ou des résultats récemment agrégés. Les événements sont générés dans la mesure du possible.

Un identifiant de GuardDuty recherche est attribué à chaque découverte. GuardDuty crée un CloudWatch événement pour chaque découverte avec un identifiant de recherche unique. Toutes les occurrences ultérieures d'une constatation existante sont regroupées avec les conclusions initiales. Pour plus d’informations, consultez GuardDuty recherche d'une agrégation.

> **Note**
>
> Si votre compte est un administrateur GuardDuty délégué, les CloudWatch événements sont publiés sur votre compte ainsi que sur le compte du membre où le résultat a été généré.

En utilisant CloudWatch des événements avec GuardDuty, vous pouvez automatiser les tâches pour vous aider à répondre aux problèmes de sécurité révélés par GuardDuty les résultats.

Pour recevoir des notifications concernant les GuardDuty résultats basés sur les CloudWatch événements, vous devez créer une règle d' CloudWatch événements et une cible pour GuardDuty. Cette règle permet CloudWatch d'envoyer des notifications pour les résultats GuardDuty générés à la cible spécifiée dans la règle. Pour plus d’informations, consultez Création d'une règle d' CloudWatch événements et d'une cible pour GuardDuty (CLI).

Rubriques

- CloudWatch Fréquence de notification des événements pour GuardDuty
- CloudWatch format d'événement pour GuardDuty
- Création d'une règle d' CloudWatch événements pour vous informer des GuardDuty résultats (console)
- Création d'une règle d' CloudWatch événements et d'une cible pour GuardDuty (CLI)
- CloudWatch Événements pour les GuardDuty environnements multi-comptes

CloudWatch Fréquence de notification des événements pour GuardDuty

Notifications pour les résultats nouvellement générés avec un ID de résultat unique

GuardDuty envoie une notification en fonction de son CloudWatch événement dans les 5 minutes suivant la découverte. Cet événement (et cette notification) inclut également toutes les occurrences ultérieures de ce résultat qui surviennent dans les 5 minutes suivant la génération de ce résultat avec un ID unique.

> **Note**
>
> Par défaut, la fréquence des notifications concernant les nouveaux résultats est de 5 minutes. Cette fréquence ne peut pas être mise à jour.

Notifications pour les occurrences de résultat ultérieures

Par défaut, pour chaque résultat doté d'un identifiant de recherche unique, GuardDuty regroupe en un seul événement toutes les occurrences ultérieures d'un type de recherche particulier qui se produisent dans les intervalles de 6 heures. GuardDuty envoie ensuite une notification concernant ces occurrences ultérieures en fonction de cet événement. Par défaut, pour les occurrences ultérieures des résultats existants, GuardDuty envoie des notifications en fonction des CloudWatch événements toutes les 6 heures.

Seul un compte administrateur peut personnaliser la fréquence par défaut des notifications envoyées concernant les occurrences ou les CloudWatch événements de recherche ultérieurs. Les utilisateurs de comptes membres ne peuvent pas personnaliser cette fréquence. La valeur de fréquence définie par le compte administrateur dans son propre compte est imposée aux GuardDuty fonctionnalités de tous ses comptes membres. Si un utilisateur d'un compte administrateur définit cette valeur de fréquence sur 1 heure, tous les comptes membres auront également la fréquence d'une heure pour recevoir des notifications concernant les occurrences de recherche ultérieures. Pour plus d’informations, consultez Gestion de plusieurs comptes sur Amazon GuardDuty.

> **Note**
>
> En tant que compte administrateur, vous pouvez personnaliser la fréquence par défaut des notifications concernant les occurrences de recherche ultérieures. Les valeurs

possibles sont 15 minutes, 1 heure ou, par défaut, 6 heures. Pour plus d'informations sur la configuration de la fréquence de ces notifications, veuillez consulter Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour.

Surveillance des GuardDuty résultats archivés grâce aux CloudWatch événements

Pour les résultats archivés manuellement, les occurrences initiales et suivantes de ces résultats (générées une fois l'archivage terminé) sont envoyées à CloudWatch Events selon la fréquence décrite ci-dessus.

Pour les résultats archivés automatiquement, les occurrences initiales et suivantes de ces résultats (générées une fois l'archivage terminé) ne sont pas envoyées à CloudWatch Events.

CloudWatch format d'événement pour GuardDuty

L' CloudWatch événement pour GuardDuty a le format suivant.

```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

Note

La valeur de détail renvoie les détails JSON d'un seul résultat sous forme d'objet, au lieu de renvoyer la valeur « résultats » qui peut prendre en charge plusieurs résultats au sein d'une matrice.

Pour obtenir la liste complète de tous les paramètres inclus dans `GUARDDUTY_FINDING_JSON_OBJECT`, consultez GetFindings. Le paramètre `id` qui apparaît dans `GUARDDUTY_FINDING_JSON_OBJECT` est l'ID du résultat décrit précédemment.

Création d'une règle d' CloudWatch événements pour vous informer des GuardDuty résultats (console)

Vous pouvez utiliser CloudWatch Events with GuardDuty pour configurer des alertes de recherche automatisées en envoyant les événements de GuardDuty recherche à un hub de messagerie afin d'accroître la visibilité des GuardDuty résultats. Cette rubrique explique comment envoyer des alertes de résultats par e-mail, Slack ou Amazon Chime en configurant une rubrique SNS, puis en connectant cette rubrique à CloudWatch une règle d'événement d'événements.

Configurer une rubrique Amazon SNS et un point de terminaison

Pour commencer, vous devez d'abord configurer une rubrique dans Amazon Simple Notification Service et ajouter un point de terminaison. Pour en savoir plus, veuillez consulter Mise en route dans le Guide du développeur Amazon Simple Notification Service.

Cette procédure définit l'endroit où vous souhaitez envoyer les données de GuardDuty recherche. Le sujet SNS peut être ajouté à une règle d' CloudWatch événement pendant ou après la création de la règle d'événement.

Email setup

Création d'une rubrique SNS

1. Connectez-vous à la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Sélectionnez Rubriques dans le panneau de navigation, puis Créer une rubrique.
3. Dans la section Créer une rubrique, sélectionnez Standard. Ensuite, saisissez un nom de rubrique, comme **`GuardDuty_to_Email`**. D'autres détails sont facultatifs.
4. Choisissez Créer la rubrique. Les détails de la rubrique pour votre nouvelle rubrique s'ouvrent.
5. Dans la section Abonnements, choisissez Créer un abonnement.
6. a. Dans le menu Protocole sélectionnez E-mail.
   b. Dans le champ Point de terminaison, ajoutez l'adresse e-mail à laquelle vous souhaitez recevoir les notifications.

> **Note**
>
> Vous devrez confirmer votre abonnement par l'intermédiaire de votre client de messagerie après l'avoir créé.

c. Choisissez Créer un abonnement.

7. Recherchez un message d'abonnement dans votre boîte de réception et choisissez Confirmer l'abonnement.

Slack setup

Création d'une rubrique SNS

1. Connectez-vous à la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Sélectionnez Rubriques dans le panneau de navigation, puis Créer une rubrique.
3. Dans la section Créer une rubrique, sélectionnez Standard. Ensuite, saisissez un nom de rubrique, comme **`GuardDuty_to_Slack`**. D'autres détails sont facultatifs. Choisissez Créer une rubrique pour finaliser.

Configuration d'un client AWS Chatbot

1. Accédez à la console AWS Chatbot.
2. Dans le panneau Clients configurés, sélectionnez Configurer un nouveau client.
3. Choisissez Slack et confirmez avec « Configurer ».

> **Note**
>
> Lorsque vous choisissez Slack, vous devez confirmer les autorisations permettant à AWS Chatbot d'accéder à votre canal en sélectionnant « Autoriser ».

4. Sélectionnez Configurer un nouveau canal pour ouvrir le volet des détails de configuration.

   a. Saisissez un nom pour le canal.

   b. Pour le canal Slack, choisissez le canal que vous souhaitez utiliser. Pour utiliser un canal privé Slack avec AWS Chatbot, choisissez Canal privé.

c. Dans Slack, copiez l'identifiant du canal privé en cliquant avec le bouton droit sur le nom du canal et en sélectionnant Copier le lien.

d. Sur la Console de gestion AWS, dans la fenêtre AWS Chatbot, collez l'ID que vous avez copié depuis Slack dans le champ ID de canal privé.

e. Dans Autorisations, choisissez de créer un rôle IAM à l'aide d'un modèle, si vous n'en avez pas déjà un.

f. Dans les modèles Stratégie, choisissez Autorisations de notification. Il s'agit du modèle de politique IAM pour AWS Chatbot. Il fournit les autorisations de lecture et de liste nécessaires pour les CloudWatch alarmes, les événements et les journaux, ainsi que pour les rubriques Amazon SNS.

g. Choisissez la région dans laquelle vous avez précédemment créé votre rubrique SNS, puis sélectionnez la rubrique Amazon SNS que vous avez créée pour envoyer des notifications au canal Slack.

5. Sélectionnez Configure (Configurer).

Chime setup

Création d'une rubrique SNS

1. Connectez-vous à la console Amazon SNS à l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Sélectionnez Rubriques dans le panneau de navigation, puis Créer une rubrique.
3. Dans la section Créer une rubrique, sélectionnez Standard. Ensuite, saisissez un nom de rubrique, comme **`GuardDuty_to_Chime`**. D'autres détails sont facultatifs. Choisissez Créer une rubrique pour finaliser.

Configuration d'un client AWS Chatbot

1. Accédez à la console AWS Chatbot.
2. Dans le panneau Clients configurés, sélectionnez Configurer un nouveau client.
3. Choisissez Chime et confirmez avec « Configurer ».
4. Dans le volet Détails de configuration, saisissez le nom du canal.
5. Dans Chime, ouvrez le salon de discussion souhaité.

a. Choisissez l'icône d'engrenage dans le coin supérieur droit, puis sélectionnez Manage webhooks (Gérer les webhooks) .

b. Sélectionnez Copier l'URL pour copier l'URL du webhook dans votre presse-papiers.

6. Sur la Console de gestion AWS, dans la fenêtre AWS Chatbot, collez l'URL que vous avez copiée dans le champ URL de Webhook.
7. Dans Autorisations, choisissez de créer un rôle IAM à l'aide d'un modèle, si vous n'en avez pas déjà un.
8. Dans les modèles Stratégie, choisissez Autorisations de notification. Il s'agit du modèle de politique IAM pour AWS Chatbot. Il fournit les autorisations de lecture et de liste nécessaires pour les CloudWatch alarmes, les événements et les journaux, ainsi que pour les rubriques Amazon SNS.
9. Choisissez la région dans laquelle vous avez précédemment créé votre rubrique SNS, puis sélectionnez la rubrique Amazon SNS que vous avez créée pour envoyer des notifications à la salle Chime.
10. Sélectionnez Configure (Configurer).

Configurez un CloudWatch événement pour les GuardDuty résultats

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Sélectionnez Règles dans le panneau de navigation, puis Créer une règle.
3. Dans le menu Nom du service, choisissez GuardDuty.
4. Dans le menu Type d'événement, choisissez GuardDutyRechercher.
5. En regard de Aperçu du modèle d'événement, choisissez Modifier.
6. Collez le code JSON ci-dessous dans l'Aperçu du modèle d'événement, puis choisissez Enregistrer.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
```

```
        4,
        4.0,
        4.1,
        4.2,
        4.3,
        4.4,
        4.5,
        4.6,
        4.7,
        4.8,
        4.9,
        5,
        5.0,
        5.1,
        5.2,
        5.3,
        5.4,
        5.5,
        5.6,
        5.7,
        5.8,
        5.9,
        6,
        6.0,
        6.1,
        6.2,
        6.3,
        6.4,
        6.5,
        6.6,
        6.7,
        6.8,
        6.9,
        7,
        7.0,
        7.1,
        7.2,
        7.3,
        7.4,
        7.5,
        7.6,
        7.7,
        7.8,
        7.9,
```

```
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9
    ]
  }
}
```

> **Note**
>
> Le code ci-dessus alertera pour toute recherche de Moyenne à Élevée.

7. Dans la section Cibles, cliquez sur Ajouter une cible.
8. Dans le menu Sélectionner des cibles, choisissez Rubrique SNS.
9. Pour Sélectionner une rubrique, sélectionnez le nom de la rubrique SNS que vous avez créée à l'étape 1.
10. Configurez l'entrée pour l'événement.

    - Si vous configurez les notifications pour Chime ou Slack, passez à l'étape 11, le type de saisie passe par défaut à Événement correspondant.
    - Si vous configurez les notifications par e-mail via SNS, suivez les étapes ci-dessous pour personnaliser le message envoyé dans votre boîte de réception en procédant comme suit :

    a. Développez Configurer l'entrée, puis choisissez Transformateur d'entrée.

    b. Copiez le code suivant et collez-le dans le champ Chemin d'entrée.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
```

```
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

c. Copiez le code suivant et collez-le dans le champ Modèle d'entrée pour formater l'e-mail.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. Cliquez sur Configurer les détails.
12. Sur la page Configurer les détails de la règle, entrez un nom et une description pour la règle, puis choisissez Créer une règle.

Création d'une règle d' CloudWatch événements et d'une cible pour GuardDuty (CLI)

La procédure suivante montre comment utiliser des AWS CLI commandes pour créer une règle d' CloudWatch événements et une cible pour GuardDuty. Plus précisément, la procédure vous montre comment créer une règle qui permet d' CloudWatch envoyer des événements pour tous les résultats qui GuardDuty génèrent et d'ajouter une AWS Lambda fonction en tant que cible pour la règle.

> **Note**
>
> Outre les fonctions Lambda, elles prennent en CloudWatch charge GuardDuty les types de cibles suivants : les instances Amazon EC2, les flux Amazon Kinesis, les tâches Amazon ECS, les machines d'étatAWS Step Functions, la commande et `run` les cibles intégrées.

Vous pouvez également créer une règle et une cible d' CloudWatch événements GuardDuty par le biais de la console CloudWatch Événements. Pour plus d'informations et des étapes détaillées, voir Création d'une règle d' CloudWatch événements qui déclenche un événement. Dans la section Event Source, sélectionnez **`GuardDuty`** pour Service name et **`GuardDuty Finding`** pour Event Type.

Pour créer une règle et une cible

1. Pour créer une règle permettant d' CloudWatch envoyer des événements pour tous les résultats GuardDuty générés, exécutez la commande CloudWatch CLI suivante.

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > Vous pouvez personnaliser davantage votre règle afin qu'elle indique d' CloudWatch envoyer des événements uniquement pour un sous-ensemble des GuardDuty résultats générés. Ce sous-ensemble est basé sur le ou les attributs de résultat qui sont spécifiés dans la règle. Par exemple, utilisez la commande CLI suivante pour créer une règle qui permet CloudWatch d'envoyer des événements uniquement pour les GuardDuty résultats présentant une gravité de 5 ou 8 :
   > `AWS events put-rule --name Test --event-pattern "{\"source\": [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"], \"detail\":{\"severity\":[5,8]}}"`
   > À cette fin, vous pouvez utiliser n'importe quelle valeur de propriété disponible dans le JSON pour les GuardDuty résultats.

2. Pour associer une fonction Lambda comme cible à la règle que vous avez créée à l'étape 1, exécutez la commande CloudWatch CLI suivante.

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > Assurez-vous de remplacer <your_function>la commande ci-dessus par votre fonction Lambda réelle pour les GuardDuty événements.

3. Pour ajouter les autorisations requises pour invoquer la cible, exécutez la commande d'interface de ligne de commande Lambda suivante.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

> **Note**
>
> Assurez-vous de remplacer <your_function>la commande ci-dessus par votre fonction Lambda réelle pour les GuardDuty événements.

> **Note**
>
> Dans la procédure ci-dessus, nous utilisons une fonction Lambda comme cible pour la règle qui déclenche CloudWatch les événements. Vous pouvez également configurer d'autres AWS ressources en tant que cibles pour déclencher CloudWatch des événements. Pour plus d'informations, consultez PutTargets.

CloudWatch Événements pour les GuardDuty environnements multi-comptes

En tant qu' GuardDuty administrateur, les règles relatives aux CloudWatch événements de votre compte seront déclenchées en fonction des résultats applicables de vos comptes de membre. Cela signifie que si vous configurez une notification de recherche par le biais d' CloudWatch événements dans votre compte administrateur, comme indiqué dans la section précédente, vous serez informé des résultats de gravité élevée ou moyenne générés par vos comptes de membre en plus des vôtres.

Vous pouvez identifier le compte membre à l'origine de la GuardDuty recherche à l'aide du `accountId` champ contenant les détails JSON de la recherche.

Pour commencer à écrire une règle d'événement personnalisée pour un compte membre spécifique de votre environnement dans la console, créez une règle et collez le modèle suivant dans Aperçu du modèle d'événement, en ajoutant l'ID de compte du compte membre avec lequel vous souhaitez déclencher l'événement.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
```

```
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Cet exemple se déclenchera en cas de résultat de l'ID de compte indiqué. Plusieurs ID peuvent être ajoutés, séparés par une virgule conformément à la syntaxe JSON.

Comprendre CloudWatch les journaux et les raisons du manque de ressources lors de l'analyse Malware Protection for EC2

GuardDuty Malware Protection for EC2 publie des événements dans votre groupe de CloudWatch journaux Amazon /aws/guardduty/ malware-scan-events. Pour chacun des événements liés à l'analyse des programmes malveillants, vous pouvez surveiller l'état et le résultat de l'analyse de vos ressources concernées. Certaines ressources Amazon EC2 et certains volumes Amazon EBS ont peut-être été ignorés lors de l'analyse Malware Protection for EC2.

CloudWatch Journaux d'audit dans GuardDuty Malware Protection for EC2

Trois types d'événements de scan sont pris en charge dans le groupe de journaux malware-scan-events CloudWatch /aws/guardduty/.

Nom de l'événement de scan de protection contre les programmes malveillants pour EC2	Explication
`EC2_SCAN_STARTED`	Créé lorsqu'une protection contre les GuardDuty programmes malveillants pour EC2 lance le processus d'analyse des programmes malveillants, par exemple en préparant la prise d'un instantané d'un volume EBS.

Nom de l'événement de scan de protection contre les programmes malveillants pour EC2	Explication
`EC2_SCAN_COMPLETED`	Créé lorsque l'analyse GuardDuty Malware Protection for EC2 est terminée pour au moins un des volumes EBS de la ressource concernée. Cet événement inclut également l'`snapshotId` qui appartient au volume EBS analysé. Une fois l'analyse terminée, son résultat de l'analyse sera `CLEAN`, `THREATS_FOUND` ou `NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Créé lorsque le scan GuardDuty Malware Protection for EC2 ignore tous les volumes EBS de la ressource affectée. Pour identifier le motif de l'omission, sélectionnez l'événement correspondant et consultez les détails. Pour plus d'informations sur les motifs de l'omission, veuillez consulter Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants ci-dessous.

> **Note**
>
> Si vous utilisez un AWS Organizations, CloudWatch les événements enregistrés depuis les comptes des membres dans Organizations sont publiés à la fois dans le compte administrateur et dans le groupe de journaux du compte membre.

Choisissez votre méthode d'accès préférée pour consulter et interroger CloudWatch les événements.

Console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.

2. Dans le panneau de navigation, choisissez Journaux, Groupes de journaux. Choisissez le groupe de malware-scan-events journaux /aws/guardduty/ pour afficher les événements d'analyse relatifs à Malware Protection for EC2. GuardDuty

   Pour exécuter une requête, choisissez Log Insights.

   Pour plus d'informations sur l'exécution d'une requête, consultez Analyser les données des CloudWatch journaux avec Logs Insights dans le guide de CloudWatch l'utilisateur Amazon.

3. Choisissez Analyser l'ID pour surveiller les détails de la ressource concernée et les résultats de logiciels malveillants. Par exemple, vous pouvez exécuter la requête suivante pour filtrer les événements du CloudWatch journal en utilisant`scanId`. Assurez-vous d'utiliser votre propre valeur *`scan-id`* valide.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Pour travailler avec des groupes de journaux, consultez la section Rechercher dans les entrées de journal AWS CLIà l'aide du guide de CloudWatch l'utilisateur Amazon.

  Choisissez le groupe de malware-scan-events journaux /aws/guardduty/ pour afficher les événements d'analyse relatifs à Malware Protection for EC2. GuardDuty
- Pour afficher et filtrer les événements du journal, consultez GetLogEventset FilterLogEvents, respectivement, dans le Amazon CloudWatch API Reference.

GuardDuty Protection contre les logiciels malveillants pour la conservation des journaux EC2

La période de conservation des journaux par défaut pour le groupe de journaux /aws/guardduty/ est de 90 jours, après quoi les événements du malware-scan-events journal sont automatiquement supprimés. Pour modifier la politique de conservation des journaux de votre groupe de CloudWatch journaux, consultez la section Conservation des données des CloudWatch journaux des modifications dans Logs du guide de CloudWatch l'utilisateur Amazon ou PutRetentionPolicydans le manuel Amazon CloudWatch API Reference.

Motifs de l'omission des ressources lors de l'analyse des logiciels malveillants

Lors des événements liés à l'analyse des programmes malveillants, certaines ressources EC2 et certains volumes EBS peuvent avoir été ignorés pendant le processus d'analyse. Le tableau suivant répertorie les raisons pour lesquelles GuardDuty Malware Protection for EC2 peut ne pas analyser les ressources. Le cas échéant, suivez les étapes proposées pour résoudre ces problèmes et analysez ces ressources la prochaine fois que GuardDuty Malware Protection for EC2 lancera une analyse des programmes malveillants. Les autres problèmes sont utilisés pour vous informer sur le cours des événements et ne sont pas exploitables.

Motifs de l'omission	Explication	Étapes proposées
`RESOURCE_NOT_FOUND`	Le `resourceArn` code fourni pour lancer l'analyse des programmes malveillants à la demande est introuvable dans votre AWS environnement.	Validez l'`resourceArn` de votre instance ou charge de travail de conteneur Amazon EC2, puis réessayez.
`ACCOUNT_INELIGIBLE`	L'identifiant du AWS compte à partir duquel vous avez essayé de lancer une analyse des programmes malveillants à la demande n'est pas activé GuardDuty.	Vérifiez que GuardDuty c'est activé pour ce AWS compte. Lorsque vous GuardDuty en activez une nouvelle Région AWS , la synchronisation peut prendre jusqu'à 20 minutes.
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Malware Protection for EC2 prend en charge les volumes à la	Remplacez votre clé de chiffrement par une clé gérée par le client. Pour

Motifs de l'omission	Explication	Étapes proposées	
	fois non chiffrés et chiffrés avec une clé gérée par le client. Il ne prend pas en charge l'analyse des volumes EBS chiffrés à l'aide du chiffrement Amazon EBS. À l'heure actuelle, il existe une différenc e régionale selon laquelle cette raison d'omission ne s'applique pas. Pour plus d'informations à ce sujet Régions AWS, consultez Disponibilité des fonctionnalités propres à la région.	plus d'informations sur les types de chiffrement pris GuardDuty en charge, consultezEBSVolume s Amazon pris en charge pour l'analyse des programmes malveillants.	

Motifs de l'omission	Explication	Étapes proposées	
`EXCLUDED_BY_SCAN_SETTINGS`	L'instance EC2 ou le volume EBS a été exclu lors de l'analyse des programmes malveillants. Il existe deux possibilités : soit la balise a été ajoutée à la liste d'inclusion, mais la ressource n'est pas associée à cette balise, soit la balise a été ajoutée à la liste d'exclusion et la ressource est associée à cette balise, soit la balise `GuardDuty Excluded` est définie sur `true` pour cette ressource.	Mettez à jour vos options d'analyse ou les balises associées à votre ressource Amazon EC2. Pour plus d'informations, consultez Options d'analyse avec balises définies par l'utilisateur.	
`UNSUPPORTED_VOLUME_SIZE`	Le volume est supérieur à 2 048 Go.	Non exploitable.	
`NO_VOLUMES_ATTACHED`	GuardDuty Malware Protection for EC2 a détecté l'instance dans votre compte, mais aucun volume EBS n'a été attaché à cette instance pour procéder à l'analyse.	Non exploitable.	
`UNABLE_TO_SCAN`	Il s'agit d'une erreur de service interne.	Non exploitable.	

Motifs de l'omission	Explication	Étapes proposées	
SNAPSHOT_NOT_FOUND	Les instantanés créés à partir des volumes EBS et partagés avec le compte de service sont introuvables, et GuardDuty Malware Protection for EC2 n'a pas pu poursuivre l'analyse.	Vérifiez que CloudTrail les instantanés n'ont pas été supprimés intentionnellement.	
SNAPSHOT_QUOTA_REACHED	Vous avez atteint le volume maximum autorisé d'instantanés pour chaque région. Cela empêche non seulement de retenir, mais également de créer d'autres instantanés.	Vous pouvez soit supprimer les anciens instantanés, soit demander une augmentation du quota. Vous pouvez consulter la limite par défaut pour les instantanés par région et la procédure à suivre pour demander une augmentation de quota sous Service Quotas dans le Guide de référence général AWS .	

Motifs de l'omission	Explication	Étapes proposées	
`MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED`	Plus de 11 volumes EBS ont été attachés à une instance EC2. GuardDuty Malware Protection for EC2 a analysé les 11 premiers volumes EBS, obtenus en les triant par ordre alphabétique. `deviceName`	Non exploitable.	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty ne prend pas en charge l'analyse des instances avec `productCode` as`marketplace` . Pour plus d'informations, consultez la section AMI payantes dans le guide de l'utilisateur Amazon EC2. Pour plus d'informations sur `productCode` , veuillez consulter ProductCode dans la Référence API d'Amazon EC2.	Non exploitable.	

Signalement des faux positifs dans GuardDuty Malware Protection for EC2

GuardDuty La protection contre les programmes malveillants pour les scans EC2 peut identifier un fichier inoffensif de votre instance Amazon EC2 ou de votre charge de travail de conteneur comme étant malveillant ou dangereux. Pour améliorer votre expérience avec Malware Protection for EC2 et le GuardDuty service, vous pouvez signaler des résultats faussement positifs si vous pensez qu'un fichier identifié comme étant malveillant ou dangereux lors d'une analyse ne contient pas réellement de logiciel malveillant.

Soumission de fichier faussement positive

1. Connectez-vous à la console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Lorsque vous identifiez ce qui semble être un résultat faussement positif, contactez-nous AWS Support pour lancer le processus de soumission de fichier faussement positif.
3. Choisissez Analyses des logiciels malveillants.
4. Choisissez une analyse pour voir son ID de résultat.
5. Communiquez l'ID de résultat. Vous devez également fournir le hachage SHA-256 du fichier. Cela est nécessaire pour garantir que GuardDuty Malware Protection for EC2 a reçu le bon fichier.
6. L' AWS Support équipe vous fournira une URL Amazon Simple Storage Service (S3) que vous pourrez utiliser pour télécharger le fichier et le hachage SHA-256. Informez l' AWS Support équipe une fois que vous avez chargé le fichier avec succès.

   > **Warning**
   >
   > Ne communiquez pas directement le fichier ou le hachage SHA-256 à AWS Support. Vous devez uniquement charger le fichier et le hachage sur Amazon S3 par le biais de l'URL fournie. Si vous ne parvenez pas à charger le fichier et le hachage dans les sept jours suivant la réception de l'URL, elle perdra sa validité. Si l'URL n'est plus valide, vous devrez nous contacter AWS Support pour recevoir une nouvelle URL.

   GuardDuty conserve votre dossier pendant 30 jours maximum. GuardDuty les membres de l'équipe analyseront votre soumission et prendront les mesures appropriées pour améliorer votre expérience avec Malware Protection for EC2 et le GuardDuty service.

Corriger les problèmes de sécurité découverts par GuardDuty

Amazon GuardDuty génère des résultats qui indiquent des problèmes de sécurité potentiels. Dans cette version de GuardDuty, les problèmes de sécurité potentiels indiquent soit une charge de travail d'EC2instance ou de conteneur compromise, soit un ensemble d'informations d'identification compromises dans votre AWS environnement. Les sections suivantes décrivent les étapes de correction recommandées pour ces scénarios. S'il existe d'autres scénarios de correction, ils seront décrits dans l'entrée correspondant à ce type de résultat spécifique. Vous pouvez accéder aux informations complètes sur un type de résultat en le sélectionnant dans le tableau des types de résultat actifs.

Table des matières

Corriger une instance Amazon EC2 potentiellement compromise

Suivez ces étapes recommandées pour corriger une EC2 instance potentiellement compromise dans votre AWS environnement :

1. Identifiez l'EC2instance Amazon potentiellement compromise

   Recherchez dans l'instance potentiellement compromise des programmes malveillants et supprimez ceux qui sont détectés. Vous pouvez l'utiliser Analyse des logiciels malveillants à la

demande pour identifier les logiciels malveillants dans l'EC2instance potentiellement compromise ou AWS Marketplacevérifier s'il existe des produits partenaires utiles pour identifier et supprimer les logiciels malveillants.

2. Isolez l'EC2instance Amazon potentiellement compromise

   Si possible, procédez comme suit pour isoler l'instance potentiellement compromise :

   1. Créez un groupe de sécurité dédié à l'isolation. Un groupe de sécurité d'isolation ne doit avoir un accès entrant et sortant qu'à partir d'adresses IP spécifiques. Assurez-vous qu'aucune règle entrante ou sortante n'autorise le trafic pour. `0.0.0.0/0 (0-65535)`
   2. Associez le groupe de sécurité Isolation à cette instance.
   3. Supprimez toutes les associations de groupes de sécurité autres que le nouveau groupe de sécurité Isolation de l'instance potentiellement compromise.

   > **Note**
   >
   > Les connexions suivies existantes ne seront pas interrompues suite à un changement de groupe de sécurité. Seul le trafic futur sera effectivement bloqué par le nouveau groupe de sécurité.
   > Pour plus d'informations sur les connexions suivies et non suivies, consultez la section Suivi des connexions des groupes de EC2 sécurité Amazon dans le guide de EC2 l'utilisateur Amazon.
   > Pour plus d'informations sur le blocage du trafic provenant de connexions existantes suspectes, voir Appliquer NACLs en fonction du réseau IoCs pour empêcher tout trafic supplémentaire dans le manuel de réponse aux incidents.

3. Identifiez la source de l'activité suspecte.

   Si un logiciel malveillant est détecté, identifiez et arrêtez les activités potentiellement non autorisées sur votre EC2 instance en fonction du type de détection détecté dans votre compte. Cela peut nécessiter des actions telles que la fermeture de tous les ports ouverts, la modification des stratégies d'accès et la mise à niveau des applications pour corriger les vulnérabilités.

   Si vous ne parvenez pas à identifier et à arrêter toute activité non autorisée sur votre EC2 instance potentiellement compromise, nous vous recommandons de mettre fin à l'EC2instance compromise et de la remplacer par une nouvelle instance si nécessaire. Vous trouverez ci-dessous des ressources supplémentaires pour sécuriser vos EC2 instances :

- Sections relatives à la sécurité et à la mise en réseau dans Meilleures pratiques pour Amazon EC2
- Groupes EC2 de sécurité Amazon pour les instances Linux et groupes EC2 de sécurité Amazon pour les instances Windows
- Sécurité sur Amazon EC2
- Conseils pour sécuriser vos EC2 instances (Linux).
- AWS meilleures pratiques en matière de sécurité
- Incidents du domaine de l'infrastructure sur AWS

4. Parcourir AWS re:Post

   Naviguez AWS re:Postpour obtenir de l'aide supplémentaire.

5. Soumission d'une demande de support technique

   Si vous êtes abonné à un package Premium Support, vous pouvez soumettre une demande de support technique.

Corriger un compartiment S3 potentiellement compromis

Suivez ces étapes recommandées pour corriger un compartiment Amazon S3 potentiellement compromis dans votre AWS environnement :

1. Identifiez la ressource S3 potentiellement compromise.

   Une GuardDuty recherche pour S3 indiquera le compartiment S3 associé, son Amazon Resource Name (ARN) et son propriétaire dans les détails de la recherche.

2. Identifiez la source de l'activité suspecte et l'APIappel utilisé.

   L'APIappel utilisé sera répertorié comme indiqué `API` dans les détails de la recherche. La source sera un IAM mandant (IAMrôle, utilisateur ou compte) et les informations d'identification seront répertoriées dans le résultat. Selon le type de source, l'adresse IP distante ou les informations sur le domaine source seront disponibles et peuvent vous aider à déterminer si la source était autorisée. Si la recherche impliquait des informations d'identification provenant d'une EC2 instance Amazon, les détails de cette ressource seront également inclus.

3. Déterminez si la source de l'appel était autorisée à accéder à la ressource identifiée.

   Prenons l'exemple suivant :

- Si un IAM utilisateur était impliqué, est-il possible que ses informations d'identification aient été potentiellement compromises ? Pour de plus amples informations, veuillez consulter Corriger les informations d'identification potentiellement compromises AWS.
- Si un API a été invoqué par un principal qui n'a jamais invoqué ce type deAPI, cette source a-t-elle besoin d'autorisations d'accès pour cette opération ? Les autorisations du compartiment peuvent-elles être davantage restreintes ?
- Si l'accès a été détecté à partir du nom d'utilisateur `ANONYMOUS_PRINCIPAL` avec le type d'utilisateur de `AWSAccount`, cela indique que le compartiment est public et qu'il a été consulté. Ce compartiment doit-il être public ? Si ce n'est pas le cas, veuillez consulter les recommandations de sécurité ci-dessous pour découvrir des solutions alternatives au partage des ressources S3.
- Si l'accès a eu lieu par le biais d'un `PreflightRequest` appel réussi, vu à partir du nom d'utilisateur **`ANONYMOUS_PRINCIPAL`** avec le type d'utilisateur, `AWSAccount` cela indique que le bucket dispose d'une politique de partage de ressources (CORS) inter-origines définie. Ce compartiment doit-il être assorti d'une CORS politique ? Dans le cas contraire, assurez-vous que le compartiment n'a pas été rendu public par inadvertance et veuillez consulter les recommandations de sécurité ci-dessous pour trouver des solutions alternatives au partage des ressources S3. Pour plus d'informations sur l'CORSutilisation du partage de ressources entre origines multiples (CORS) dans le guide de l'utilisateur de S3.

4. Déterminez si le compartiment S3 contient des données sensibles.

   Utilisez Amazon Macie pour déterminer si le compartiment S3 contient des données sensibles, telles que des informations personnellement identifiables (PII), des données financières ou des informations d'identification. Si la découverte automatique des données sensibles est activée pour votre compte Macie, examinez les détails du compartiment S3 pour mieux comprendre son contenu. Si cette fonctionnalité est désactivée pour votre compte Macie, nous vous recommandons de l'activer pour accélérer votre évaluation. Vous pouvez également créer et exécuter une tâche de découverte de données sensibles pour inspecter les objets du compartiment S3 afin de détecter des données sensibles. Pour plus d'informations, veuillez consulter Découverte de données sensibles avec Macie (langue française non garantie).

Si l'accès a été autorisé, vous pouvez ignorer le résultat. La https://console.aws.amazon.com/guardduty/console vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour de plus amples informations, veuillez consulter Règles de suppression.

Si vous déterminez que vos données S3 ont été exposées ou consultées par un tiers non autorisé, consultez les recommandations de sécurité S3 suivantes pour renforcer les autorisations et restreindre l'accès. Les solutions de correction appropriées dépendent des besoins de votre environnement spécifique.

Recommandations basées sur les besoins spécifiques d'accès aux compartiments S3

La liste suivante fournit des recommandations basées sur les besoins spécifiques d'accès aux compartiments Amazon S3 :

- Pour limiter de manière centralisée l'accès public à l'utilisation de vos données S3, S3 bloque l'accès public. Les paramètres de blocage de l'accès public peuvent être activés pour les points d'accès, les compartiments et les AWS comptes via quatre paramètres différents afin de contrôler la granularité de l'accès. Pour plus d'informations, veuillez consulter Blocage de l'accès public à votre stockage Amazon S3.
- AWS Les politiques d'accès peuvent être utilisées pour contrôler la manière dont IAM les utilisateurs peuvent accéder à vos ressources ou à vos compartiments. Pour plus d'informations, veuillez consulter Utilisation de stratégies de compartiment et de stratégies utilisateur.

  En outre, vous pouvez utiliser des points de terminaison Virtual Private Cloud (VPC) avec des politiques de compartiment S3 pour restreindre l'accès à des points de VPC terminaison spécifiques. Pour plus d'informations, consultez Exemples de politiques de compartiment pour les VPC points de terminaison pour Amazon S3
- Pour autoriser temporairement l'accès à vos objets S3 à des entités de confiance extérieures à votre compte, vous pouvez créer un pré-signé URL via S3. Cet accès est créé à l'aide des informations d'identification de votre compte et, selon les informations d'identification utilisées, peut durer de 6 heures à 7 jours. Pour plus d'informations, consultez la section Génération de documents présignés URLs avec S3.
- Pour les cas d'utilisation nécessitant le partage d'objets S3 entre différentes sources, vous pouvez utiliser les points d'accès S3 pour créer des ensembles d'autorisations qui limitent l'accès aux seuls utilisateurs de votre réseau privé. Pour plus d'informations, veuillez consulter Gestion de l'accès aux données avec les points d'accès Amazon S3.
- Pour accorder en toute sécurité l'accès à vos ressources S3 à d'autres AWS comptes, vous pouvez utiliser une liste de contrôle d'accès (ACL). Pour plus d'informations, consultez Gérer l'accès S3 avec ACLs.

Pour plus d'informations sur les options de sécurité S3, consultez les meilleures pratiques de sécurité S3.

Corriger un objet S3 potentiellement malveillant

Lorsqu'un Protection contre les programmes malveillants pour le type de recherche S3 est généré dans votre Compte AWS, le type de ressource potentiellement malveillant est un S3Object.

Suivez les étapes recommandées ci-dessous pour éventuellement corriger le résultat généré :

1. Identifiez l'objet S3 potentiellement malveillant en vérifiant le S3 ObjectDetails associé à la découverte.
2. Isolez l'objet S3 concerné. Si vous aviez activé le balisage au moment de l'activation de Malware Protection for S3 pour le compartiment Amazon S3 associé, vous GuardDuty devez avoir attribué un tag Malicious à cet objet. Utilisez le contrôle d'accès basé sur des balises (TBAC) pour restreindre l'accès à cet objet S3. Pour de plus amples informations, veuillez consulter Utilisation du contrôle d'accès basé sur des balises () TBAC.

   Si vous n'avez plus besoin de cet objet, vous pouvez également choisir de le supprimer ou de le déplacer vers un compartiment S3 isolé. Pour plus d'informations sur les considérations relatives à la suppression d'un objet S3, consultez Supprimer des objets dans le guide de l'utilisateur Amazon S3.

Corriger un cluster potentiellement compromis ECS

Suivez ces étapes recommandées pour corriger un ECS cluster Amazon potentiellement compromis dans votre AWS environnement :

1. Identifiez le ECS cluster potentiellement compromis.

   La protection contre les GuardDuty programmes malveillants pour la EC2 recherche ECS fournit les détails du ECS cluster dans le panneau des détails de la recherche.
2. Évaluation de la source des logiciels malveillants

   Évaluez si le logiciel malveillant détecté se trouvait dans l'image du conteneur. Si un logiciel malveillant se trouvait dans l'image, identifiez toutes les autres tâches en cours d'exécution à l'aide de cette image. Pour plus d'informations sur l'exécution de tâches, consultez ListTasks.
3. Isolez les tâches potentiellement touchées

Isolez les tâches concernées en refusant tout trafic entrant et sortant vers la tâche. Une règle interdisant tout trafic peut vous aider à stopper une attaque déjà en cours, en coupant toutes les connexions à la tâche.

Si l'accès a été autorisé, vous pouvez ignorer le résultat. La https://console.aws.amazon.com/guardduty/console vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour de plus amples informations, veuillez consulter Règles de suppression.

Corriger les informations d'identification potentiellement compromises AWS

Suivez ces étapes recommandées pour corriger les informations d'identification potentiellement compromises dans votre AWS environnement :

1. Identifiez l'IAMentité potentiellement compromise et l'APIappel utilisé.

   L'APIappel utilisé sera répertorié comme indiqué `API` dans les détails de la recherche. L'IAMentité (IAMrôle ou utilisateur) et ses informations d'identification seront répertoriées dans la section Ressource des détails de la recherche. Le type d'IAMentité impliqué peut être déterminé par le champ Type d'utilisateur, le nom de l'IAMentité figurera dans le champ Nom d'utilisateur. Le type d'IAMentité impliqué dans la recherche peut également être déterminé par l'ID de clé d'accès utilisé.

   Pour les clés commençant par `AKIA` :

   Ce type de clé est un identifiant géré à long terme par le client associé à un IAM utilisateur ou. Utilisateur racine d'un compte AWS Pour plus d'informations sur la gestion des clés d'accès pour IAM les utilisateurs, consultez la section Gestion des clés d'accès pour IAM les utilisateurs.

   Pour les clés commençant par `ASIA` :

   Ce type de clé est une information d'identification temporaire à court terme générée par AWS Security Token Service. Ces clés n'existent que pour une courte période et ne peuvent être ni affichées ni gérées dans la console AWS de gestion. IAMles rôles utiliseront toujours des AWS STS informations d'identification, mais elles peuvent également être générées pour IAM

les utilisateurs. Pour plus d'informations, AWS STS voir IAM: Informations d'identification de sécurité temporaires.

Si un rôle a été utilisé, le champ Nom d'utilisateur contient des informations sur le nom du rôle utilisé. Vous pouvez déterminer comment la clé a été demandée AWS CloudTrail en examinant l'`sessionIssuer`élément de l'entrée du CloudTrail journal. Pour plus d'informations, voir IAMet AWS STS informations dans CloudTrail.

2. Vérifiez les autorisations accordées à l'IAMentité.

   Ouvrez la IAM console. Selon le type d'entité utilisé, choisissez l'onglet Utilisateurs ou Rôles, puis localisez l'entité affectée en saisissant le nom identifié dans le champ de recherche. Utilisez les onglets Permission et Access Advisor pour vérifier les autorisations effectives pour cette entité.

3. Déterminez si les informations d'identification de IAM l'entité ont été utilisées de manière légitime.

   Contactez l'utilisateur des informations d'identification pour déterminer si l'activité était intentionnelle.

   Recherchez par exemple si l'utilisateur a effectué les actions suivantes :

   - A invoqué l'APIopération répertoriée dans le GuardDuty résultat
   - A invoqué l'APIopération à l'heure indiquée dans le GuardDuty résultat
   - A appelé l'APIopération à partir de l'adresse IP répertoriée dans le GuardDuty résultat

Si cette activité constitue une utilisation légitime des AWS informations d'identification, vous pouvez ignorer le GuardDuty résultat. La https://console.aws.amazon.com/guardduty/console vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour de plus amples informations, veuillez consulter Règles de suppression.

Si vous ne pouvez pas confirmer si cette activité constitue une utilisation légitime, elle peut être le résultat d'une compromission de la clé d'accès en question, c'est-à-dire des informations de connexion de l'IAMutilisateur, ou peut-être de l'intégralité Compte AWS. Si vous pensez que vos informations d'identification ont été compromises, consultez les informations contenues dans l'article Mon compte Compte AWS peut être compromis pour résoudre ce problème.

Corriger un conteneur autonome potentiellement compromis

1. Isolez le contenant potentiellement compromis

Les étapes suivantes vous aideront à identifier la charge de travail de conteneur potentiellement malveillante :

- Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
- Sur la page Résultats, choisissez le résultat correspondant pour afficher le panneau des résultats.
- Dans le panneau des résultats, sous la section Ressource concernée, vous pouvez voir l'ID et le nom du conteneur.

Isolez ce conteneur des autres charges de travail de conteneur.

2. Mise en pause du conteneur

   Suspendez tous les processus dans votre conteneur.

   Pour plus d'informations sur la congélation de votre contenant, voir Suspendre un contenant.

   Arrêt du conteneur

   Si l'étape ci-dessus échoue et que le conteneur ne se suspend pas, arrêtez son exécution. Si vous avez activé cette Conservation des instantanés GuardDuty fonctionnalité, les instantanés de vos EBS volumes contenant des logiciels malveillants seront conservés.

   Pour plus d'informations sur l'arrêt du conteneur, voir Arrêter un conteneur.

3. Évaluation de la présence de logiciels malveillants

   Évaluez si un logiciel malveillant se trouvait dans l'image du conteneur.

Si l'accès a été autorisé, vous pouvez ignorer le résultat. La https://console.aws.amazon.com/guardduty/console vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. La GuardDuty console vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour de plus amples informations, veuillez consulter Règles de suppression.

Correction des résultats de la surveillance des journaux d'audit EKS

Amazon GuardDuty génère des résultats qui indiquent les problèmes de sécurité potentiels liés à Kubernetes lorsque la surveillance du journal d'audit EKS est activée pour votre compte. Pour de plus amples informations, veuillez consulter EKSSurveillance du journal d'audit. Les sections suivantes décrivent les étapes de correction recommandées pour ces scénarios. Les mesures correctives spécifiques sont décrites dans l'entrée correspondant à ce type de résultat spécifique. Vous pouvez accéder aux informations complètes sur un type de résultat en le sélectionnant dans le tableau des types de résultat actifs.

Si l'un des types de résultat de surveillance des journaux d'audit EKS a été généré comme prévu, vous pouvez envisager d'ajouter une Règles de suppression pour éviter de futures alertes.

Différents types d'attaques et de problèmes de configuration peuvent déclencher les découvertes de GuardDuty Kubernetes. Ce guide vous aide à identifier les causes profondes des GuardDuty découvertes concernant votre cluster et présente des conseils de correction appropriés. Les principales causes à l'origine des découvertes de GuardDuty Kubernetes sont les suivantes :

- Problèmes de configuration potentiels
- Corriger les utilisateurs Kubernetes potentiellement compromis
- Corriger les pods Kubernetes potentiellement compromis
- Corriger les nœuds Kubernetes potentiellement compromis
- Corriger les images de conteneurs potentiellement compromises

> **Note**
>
> Avant la version 1.14 de Kubernetes, le `system:unauthenticated` groupe était associé à `system:discovery` et par défaut. `system:basic-user` ClusterRoles Cela peut autoriser un accès involontaire de la part d'utilisateurs anonymes. Les mises à jour de cluster ne révoquent pas ces autorisations, ce qui signifie que même si vous avez mis à jour votre cluster vers la version 1.14 ou ultérieure, elles peuvent toujours être en place. Nous vous recommandons de dissocier ces autorisations du groupe `system:unauthenticated`. Pour plus d'informations sur la suppression de ces autorisations, consultez les meilleures pratiques de sécurité pour Amazon EKS dans le guide de l'utilisateur Amazon EKS.

Problèmes de configuration potentiels

Si un résultat indique un problème de configuration, veuillez consulter la section sur la correction de ce résultat pour obtenir des conseils sur la résolution de ce problème particulier. Pour de plus amples informations, veuillez consulter les types de résultat suivants qui indiquent des problèmes de configuration :

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Toute découverte qui se termine par SuccessfulAnonymousAccess

Corriger les utilisateurs Kubernetes potentiellement compromis

Un GuardDuty résultat peut indiquer un utilisateur Kubernetes compromis lorsqu'un utilisateur identifié dans le résultat a effectué une action d'API inattendue. Vous pouvez identifier l'utilisateur dans la section Détails de l'utilisateur Kubernetes des détails d'un résultat dans la console, ou dans les `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` des résultats JSON. Ces détails de l'utilisateur incluent `user name`, `uid` et les groupes Kubernetes auxquels l'utilisateur appartient.

Si l'utilisateur accédait à la charge de travail via une entité IAM, vous pouvez utiliser la section `Access Key details` pour identifier les détails d'un utilisateur ou d'un rôle IAM. Consultez les types d'utilisateur suivants et leurs conseils en matière de correction.

> **Note**
>
> Vous pouvez utiliser Amazon Detective pour étudier plus en détail l'utilisateur ou le rôle IAM identifié dans le résultat. Lorsque vous consultez les détails de la recherche dans GuardDuty la console, choisissez Investigate in Detective. Sélectionnez ensuite un AWS utilisateur ou un rôle parmi les éléments répertoriés pour l'étudier dans Detective.

Administrateur Kubernetes intégré : utilisateur par défaut attribué par Amazon EKS à l'identité IAM qui a créé le cluster. Ce type d'utilisateur est identifié par le nom d'utilisateur `kubernetes-admin`.

Pour révoquer l'accès d'un administrateur Kubernetes intégré :

- Identifiez le `userType` dans la section `Access Key details`.
  - Si le `userType` est Rôle et que le rôle appartient à un rôle d'instance EC2 :
    - Identifiez cette instance, puis suivez les instructions fournies dans Corriger une instance Amazon EC2 potentiellement compromise.
  - Si le `userType` est Utilisateur ou un rôle assumé par un utilisateur :
    1. Effectuez une rotation de la clé d'accès de cet utilisateur.
    2. Effectuez une rotation de tous les secrets auxquels l'utilisateur avait accès.
    3. Consultez les informations dans Mon AWS compte peut être compromis pour plus de détails.

Utilisateur authentifié OIDC : utilisateur auquel l'accès a été accordé par un fournisseur OIDC. Généralement, le nom d'utilisateur OIDC est une adresse e-mail. Vous pouvez vérifier si votre cluster utilise OIDC avec la commande suivante : `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`* .

Pour révoquer l'accès d'un utilisateur authentifié OIDC :

1. Effectuez une rotation des informations d'identification de cet utilisateur dans le fournisseur OIDC.
2. Effectuez une rotation de tous les secrets auxquels l'utilisateur avait accès.

AWS-Utilisateur ConfigMap défini par -Auth : utilisateur IAM auquel l'accès a été accordé par le biais d'un -auth. AWSConfigMap Pour plus d'informations, veuillez consulter Autorisation d'un principal IAM à accéder à votre cluster dans le guide de l'utilisateur &EKS ;. Vous pouvez consulter les autorisations à l'aide de la commande suivante : `kubectl edit configmaps aws-auth --namespace kube-system`

Pour révoquer l'accès d'un AWS ConfigMap utilisateur :

1. Utilisez la commande suivante pour ouvrir le ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifiez le rôle ou l'entrée utilisateur dans la section MapRoles ou MapUsers avec le même nom d'utilisateur que celui indiqué dans la section des informations utilisateur Kubernetes de votre recherche. GuardDuty Consultez l'exemple suivant, où l'utilisateur administrateur a été identifié dans un résultat.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Supprimez cet utilisateur du ConfigMap. Consultez l'exemple suivant où l'utilisateur administrateur a été supprimé.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. Si le `userType` est Utilisateur ou un rôle assumé par un utilisateur :
   a. Effectuez une rotation de la clé d'accès de cet utilisateur.
   b. Effectuez une rotation de tous les secrets auxquels l'utilisateur avait accès.
   c. Consultez les informations dans Mon AWS compte peut être compromis pour plus de détails.

Si le résultat ne comporte pas de section `resource.accessKeyDetails`, l'utilisateur est un compte de service Kubernetes.

Compte de service : le compte de service fournit une identité aux pods et peut être identifié par un nom d'utilisateur au format suivant : `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Pour révoquer l'accès à un compte de service :

1. Effectuez une rotation des informations d'identification du compte de service.
2. Consultez les instructions relatives à la compromission du pod dans la section suivante.

Corriger les pods Kubernetes potentiellement compromis

Lorsque vous GuardDuty spécifiez les détails d'un pod ou d'une ressource de charge de travail dans la `resource.kubernetesDetails.kubernetesWorkloadDetails` section, cet espace ou cette ressource de charge de travail a été potentiellement compromis. Une GuardDuty découverte peut indiquer qu'un seul pod a été compromis ou que plusieurs pods ont été compromis par le biais d'une ressource de niveau supérieur. Consultez les scénarios de compromission suivants pour savoir comment identifier le ou les pods compromis.

Pods compromis individuels

Si le champ `type` dans la section `resource.kubernetesDetails.kubernetesWorkloadDetails` est pods, le résultat identifie un seul pod. Le champ de nom est le `name` des pods et le champ `namespace` est son espace de noms.

Pour plus d'informations sur l'identification du nœud de travail exécutant les modules, voir Identifier les modules et le nœud de travail incriminés.

Pods compromis par le biais d'une ressource de charge de travail

Si le champ `type` de la section `resource.kubernetesDetails.kubernetesWorkloadDetails` identifie une ressource de charge de travail, comme un `Deployment`, il est probable que tous les pods de cette ressource de charge de travail aient été compromis.

Pour plus d'informations sur l'identification de tous les pods de la ressource de charge de travail et des nœuds sur lesquels ils s'exécutent, voir Identifier les pods et nœuds de travail incriminés à l'aide du nom de la charge de travail.

Pods compromis par le biais d'un compte de service

Si un GuardDuty résultat identifie un compte de service dans la `resource.kubernetesDetails.kubernetesUserDetails` section, il est probable que les pods utilisant le compte de service identifié soient compromis. Le nom d'utilisateur indiqué par un résultat est un compte de service s'il a le format suivant : `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Pour plus d'informations sur l'identification de tous les pods à l'aide du compte de service et des nœuds sur lesquels ils s'exécutent, voir Identifier les pods et nœuds de travail incriminés à l'aide du nom du compte de service.

Une fois que vous avez identifié tous les pods compromis et les nœuds sur lesquels ils s'exécutent, consultez le guide des meilleures pratiques d'Amazon EKS pour isoler le pod, modifier ses informations d'identification et collecter des données à des fins d'analyse médico-légale.

Pour réparer un pod potentiellement compromis :

1. Identifiez la vulnérabilité qui a compromis les pods.
2. Mettez en œuvre le correctif pour cette vulnérabilité et démarrez de nouveaux pods de remplacement.
3. Supprimez les pods vulnérables.

   Pour plus d'informations, consultez la section Redéploiement d'un pod ou d'une ressource de charge de travail compromise.

Si un rôle IAM a été attribué au nœud de travail qui permet aux Pods d'accéder à d'autres AWS ressources, supprimez ces rôles de l'instance pour éviter que l'attaque ne cause de nouveaux

dommages. De même, si un rôle IAM a été attribué au pod, déterminez si vous pouvez supprimer les politiques IAM du rôle en toute sécurité sans affecter les autres charges de travail.

Corriger les images de conteneurs potentiellement compromises

Lorsqu'un GuardDuty résultat indique une compromission du pod, l'image utilisée pour lancer le pod peut être potentiellement malveillante ou compromise. GuardDuty les résultats identifient l'image du conteneur `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` sur le terrain. Vous pouvez déterminer si l'image est malveillante en l'analysant afin de détecter des logiciels malveillants.

Pour corriger une image de conteneur potentiellement compromise, procédez comme suit :

1. Arrêtez immédiatement d'utiliser l'image et supprimez-la de votre référentiel d'images.
2. Identifiez tous les pods à l'aide de l'image potentiellement compromise.

   Pour plus d'informations, voir Identifier les pods dont les images de conteneur et les nœuds de travail sont potentiellement vulnérables ou compromis.
3. Isolez les modules potentiellement compromis, alternez les informations d'identification et collectez des données à des fins d'analyse. Pour plus d'informations, consultez le guide des meilleures pratiques Amazon EKS.
4. Supprimez tous les modules utilisant l'image potentiellement compromise.

Corriger les nœuds Kubernetes potentiellement compromis

Une GuardDuty découverte peut indiquer une compromission d'un nœud si l'utilisateur identifié dans la découverte représente une identité de nœud ou si la découverte indique l'utilisation d'un conteneur privilégié.

L'identité de l'utilisateur est un composant master si le champ username a le format suivant : `system:node:node name`. Par exemple, `system:node:ip-192-168-3-201.ec2.internal`. Cela indique que l'adversaire a obtenu l'accès au nœud et qu'il utilise les informations d'identification du nœud pour communiquer avec le point de terminaison de l'API Kubernetes.

Un résultat indique l'utilisation d'un conteneur privilégié si un ou plusieurs conteneurs répertoriés dans le résultat a le champ de résultat

`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` défini sur `True`.

Pour remédier à un nœud potentiellement compromis, procédez comme suit :

1. Isolez le module, modifiez ses informations d'identification et collectez des données pour une analyse médico-légale.

   Pour plus d'informations, consultez le guide des meilleures pratiques Amazon EKS.
2. Identifiez les comptes de service utilisés par tous les pods exécutés sur le nœud potentiellement compromis. Vérifiez leurs autorisations et effectuez une rotation des comptes de service, si nécessaire.
3. Mettez fin au nœud potentiellement compromis.

Corriger les résultats de la surveillance de l'exécution

Lorsque vous activez la surveillance du temps d'exécution pour votre compte, Amazon GuardDuty peut générer des informations Types de recherche liés à la surveillance du temps indiquant des problèmes de sécurité potentiels dans votre AWS environnement. Les problèmes de sécurité potentiels indiquent soit une instance Amazon EC2 compromise, soit une charge de travail de conteneur, soit un cluster Amazon EKS, soit un ensemble d'informations d'identification compromises dans votre AWS environnement. L'agent de sécurité surveille les événements d'exécution provenant de plusieurs types de ressources. Pour identifier la ressource potentiellement compromise, consultez le type de ressource dans les informations de recherche générées dans la GuardDuty console. La section suivante décrit les étapes de correction recommandées pour chaque type de ressource.

Instance

Si le type de ressource indiqué dans les détails du résultat est Instance, cela indique qu'une instance EC2 ou un nœud EKS est potentiellement compromis.

- Pour corriger un nœud EKS compromis, veuillez consulter Corriger les nœuds Kubernetes potentiellement compromis.
- Pour corriger une instance EC2 compromise, veuillez consulter Corriger une instance Amazon EC2 potentiellement compromise.

EKSCluster

Si le type de ressource indiqué dans les détails du résultat est EKSCluster, cela indique qu'un pod ou un conteneur dans un cluster EKS est potentiellement compromis.

- Pour corriger un pod compromis, veuillez consulter Corriger les pods Kubernetes potentiellement compromis.
- Pour corriger une image de conteneur compromise, veuillez consulter Corriger les images de conteneurs potentiellement compromises.

ECSCluster

Si le type de ressource indiqué dans les détails de la recherche est ECSCluster, cela indique qu'une tâche ECS ou un conteneur à l'intérieur d'une tâche ECS est potentiellement compromis.

1. Identifiez le cluster ECS concerné

   La constatation GuardDuty Runtime Monitoring fournit les détails du cluster ECS dans le panneau de détails de la découverte ou dans la `resource.ecsClusterDetails` section du JSON de recherche.

2. Identifiez la tâche ECS affectée

   La constatation GuardDuty Runtime Monitoring fournit les détails de la tâche ECS dans le panneau de détails de la recherche ou dans la `resource.ecsClusterDetails.taskDetails` section du JSON de recherche.

3. Isolez la tâche affectée

   Isolez la tâche affectée en refusant tout trafic entrant et sortant vers la tâche. Une règle interdisant tout trafic peut aider à stopper une attaque déjà en cours, en coupant toutes les connexions à la tâche.

4. Corriger la tâche compromise

   a. Identifiez la vulnérabilité qui a compromis la tâche.

   b. Mettez en œuvre le correctif pour cette vulnérabilité et lancez une nouvelle tâche de remplacement.

   c. Arrêtez cette tâche vulnérable.

Container

Si le type de ressource indiqué dans les détails du résultat est Conteneur, cela indique qu'un conteneur autonome est potentiellement compromis.

- Pour remédier à cette situation, veuillez consulter Corriger un conteneur autonome potentiellement compromis.
- Si le résultat est généré sur plusieurs conteneurs à l'aide de la même image de conteneur, veuillez consulter Corriger les images de conteneurs potentiellement compromises.
- Si le conteneur a accédé à l'hôte EC2 sous-jacent, ses informations d'identification d'instance associées ont peut-être été compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.
- Si un acteur potentiellement malveillant a accédé au nœud EKS ou à une instance EC2 sous-jacent, veuillez consulter la correction recommandée sous les onglets EKSCluster et Instance.

Correction des images de conteneur compromises

Lorsqu'un GuardDuty résultat indique la compromission d'une tâche, l'image utilisée pour lancer la tâche peut être malveillante ou compromise. GuardDuty les résultats identifient l'image du conteneur `resource.ecsClusterDetails.taskDetails.containers.image` sur le terrain. Vous pouvez déterminer si l'image est malveillante ou non en la scannant à la recherche de logiciels malveillants.

Pour corriger une image de conteneur compromise

1. Arrêtez immédiatement d'utiliser l'image et supprimez-la de votre référentiel d'images.
2. Identifiez toutes les tâches qui utilisent cette image.
3. Arrêtez toutes les tâches utilisant l'image compromise. Mettez à jour leurs définitions de tâches afin qu'ils cessent d'utiliser l'image compromise.

Corriger une base de données potentiellement compromise

GuardDuty génère Types de résultat de la protection RDS qui indiquent un comportement de connexion potentiellement suspect et anormal chez vous une Bases de données prises en charge fois que vous l'avez activéRDSProtection. L'activité de connexion RDS permet d' GuardDuty analyser et de profiler les menaces en identifiant les modèles inhabituels lors des tentatives de connexion.

> **Note**
>
> Vous pouvez accéder aux informations complètes sur un type de résultat en le sélectionnant dans la Tableau des résultats.

Suivez ces étapes recommandées pour corriger une base de données Amazon Aurora potentiellement compromise dans votre AWS environnement.

Rubriques

- Correction d'une base de données potentiellement compromise avec des événements de connexion réussie
- Correction d'une base de données potentiellement compromise avec des événements de connexion échouée
- Correction d'informations d'identification compromises
- Retreindre l'accès au réseau

Correction d'une base de données potentiellement compromise avec des événements de connexion réussie

Les étapes recommandées ci-dessous peuvent vous aider à corriger une base de données Aurora potentiellement compromise qui présente un comportement inhabituel lié à des événements de connexion réussie.

1. Identifiez la base de données et l'utilisateur concernés.

   Le GuardDuty résultat généré fournit le nom de la base de données affectée et les informations utilisateur correspondantes. Pour de plus amples informations, veuillez consulter Détails d’un résultat.
2. Vérifiez si ce comportement est attendu ou inattendu.

   La liste suivante indique les scénarios potentiels susceptibles d'avoir entraîné GuardDuty la génération d'un résultat :
   - Un utilisateur qui se connecte à sa base de données après une longue période.
   - Un utilisateur qui se connecte à sa base de données de façon occasionnelle, par exemple un analyste financier qui se connecte chaque trimestre.

- Un acteur potentiellement suspect impliqué dans une tentative de connexion réussie peut compromettre la base de données.

3. Commencez cette étape si le comportement est inattendu.

   1. Restreindre l'accès à la base de données

      Limitez l'accès à la base de données pour les comptes suspects et la source de cette activité de connexion. Pour plus d'informations, consultez Correction d'informations d'identification compromises et Retreindre l'accès au réseau.

   2. Évaluez l'impact et déterminez quelles informations ont été consultées.

      - Le cas échéant, veuillez consulter les journaux d'audit pour identifier les informations susceptibles d'avoir été consultées. Pour de plus amples informations, veuillez consulter Surveillance des événements, des journaux et des flux dans un cluster de base de données Amazon Aurora dans le Guide de l'utilisateur Amazon Aurora.
      - Déterminez si des informations sensibles ou protégées ont été consultées ou modifiées.

Correction d'une base de données potentiellement compromise avec des événements de connexion échouée

Les étapes recommandées ci-dessous peuvent vous aider à corriger une base de données Aurora potentiellement compromise qui présente un comportement inhabituel lié à des événements de connexion échouée.

1. Identifiez la base de données et l'utilisateur concernés.

   Le GuardDuty résultat généré fournit le nom de la base de données affectée et les informations utilisateur correspondantes. Pour de plus amples informations, veuillez consulter Détails d'un résultat.

2. Identifiez la source des tentatives de connexion infructueuses.

   Le GuardDuty résultat généré fournit l'adresse IP et l'organisation ASN (s'il s'agissait d'une connexion publique) dans la section Acteur du panneau de recherche.

   Un système autonome est un groupe d'un ou de plusieurs préfixes IP (listes d'adresses IP accessibles sur un réseau) gérés par un ou plusieurs opérateurs réseau qui appliquent une stratégie de routage unique et clairement définie. Les opérateurs réseau ont besoin de numéros

de système autonomes (ASN) pour contrôler le routage au sein de leurs réseaux et pour échanger des informations de routage avec d'autres fournisseurs de services Internet (FSI).

3. Vérifiez que ce comportement est inattendu.

   Vérifiez si cette activité représente une tentative d'obtenir un accès non autorisé supplémentaire à la base de données comme suit :

   - Si la source est interne, vérifiez si une application est mal configurée et tente de se connecter à plusieurs reprises.
   - S'il s'agit d'un acteur externe, vérifiez si la base de données correspondante est accessible au public ou si elle est mal configurée, ce qui permet à des acteurs malveillants potentiels de recourir à une attaque en force visant à obtenir les noms d'utilisateur courants.

4. Commencez cette étape si le comportement est inattendu.

   1. Restreindre l'accès à la base de données

      Limitez l'accès à la base de données pour les comptes suspects et la source de cette activité de connexion. Pour plus d'informations, consultez Correction d'informations d'identification compromises et Retreindre l'accès au réseau.

   2. Effectuez une analyse des causes profondes et déterminez les étapes qui ont potentiellement donné lieu à cette activité.

      Configurez une alerte pour être averti lorsqu'une activité modifie une stratégie réseau et crée un état non sécurisé. Pour plus d'informations, veuillez consulter Politiques de pare-feu dans AWS Network Firewall dans le Guide du développeurAWS Network Firewall (langue française non garantie).

Correction d'informations d'identification compromises

Une GuardDuty découverte peut indiquer que les informations d'identification d'utilisateur d'une base de données affectée ont été compromises lorsque l'utilisateur identifié dans la recherche a effectué une opération de base de données inattendue. Vous pouvez identifier l'utilisateur dans la section Détails de l'utilisateur de la base de données RDS dans le panneau de résultat de la console, ou dans les `resource.rdsDbUserDetails` des résultats JSON. Ces informations utilisateur incluent le nom d'utilisateur, l'application utilisée, la base de données consultée, la version SSL et la méthode d'authentification.

- Pour révoquer l'accès ou modifier les mots de passe pour des utilisateurs spécifiques impliqués dans le résultat, veuillez consulter Sécurité avec Amazon Aurora MySQL ou Sécurité avec Amazon Aurora PostgreSQL dans le Guide de l'utilisateur Amazon Aurora.
- AWS Secrets Manager À utiliser pour stocker en toute sécurité et transférer automatiquement les secrets des bases de données Amazon Relational Database Service (RDS). Pour plus d'informations, veuillez consulter la rubrique DidacticielsAWS Secrets Manager dans le Guide de l'utilisateurAWS Secrets Manager .
- Utilisez l'authentification de base de données IAM pour gérer l'accès des utilisateurs de base de données sans avoir besoin de mots de passe. Pour de plus amples informations, veuillez consulter Authentification de base de données IAM dans le Guide de l'utilisateur Amazon Aurora.

  Pour de plus amples informations, veuillez consulter Bonnes pratiques en matière de sécurité pour Amazon Relational Database Service dans le Guide de l'utilisateur Amazon RDS.

Retreindre l'accès au réseau

Une GuardDuty découverte peut indiquer qu'une base de données est accessible au-delà de vos applications ou du Virtual Private Cloud (VPC). Si l'adresse IP distante indiquée dans le résultat est une source de connexion inattendue, vérifiez les groupes de sécurité. La liste des groupes de sécurité attachés à la base de données est disponible sous Groupes de sécurité dans la console https://console.aws.amazon.com/rds/ ou dans les `resource.rdsDbInstanceDetails.dbSecurityGroups` du fichier JSON des résultats. Pour de plus amples informations sur la configuration des groupes de sécurité, veuillez consulter Contrôle d'accès par groupes de sécurité dans le Guide de l'utilisateur Amazon RDS.

Si vous utilisez un pare-feu, limitez l'accès réseau à la base de données en reconfigurant les listes de contrôle d'accès réseau (NACL). Pour plus d'informations, veuillez consulter Pare-feux dans AWS Network Firewall dans le Guide du développeurAWS Network Firewall .

Corriger une fonction Lambda potentiellement compromise

Lorsque vous GuardDuty générez un résultat de protection Lambda et que l'activité est inattendue, votre fonction Lambda peut être compromise. Nous vous recommandons de procéder comme suit pour corriger une fonction Lambda compromise.

Pour corriger les résultats de la protection Lambda

1. Identifiez la version de la fonction Lambda potentiellement compromise.

   Une GuardDuty recherche pour Lambda Protection fournit le nom, le nom de ressource Amazon (ARN), la version de la fonction et l'ID de révision associés à la fonction Lambda répertoriés dans les détails de la recherche.
2. Identifiez la source de l'activité potentiellement suspecte.

   a. Examinez le code associé à la version de la fonction Lambda impliquée dans le résultat.
   b. Examinez les bibliothèques et les couches importées de la version de la fonction Lambda impliquée dans le résultat.
   c. Si vous avez activé AWS Lambda les fonctions de numérisation avec Amazon Inspector, consultez les résultats Amazon Inspector associés à la fonction Lambda impliquée dans le résultat.
   d. Passez en revue les AWS CloudTrail journaux pour identifier le principal responsable de la mise à jour de la fonction et assurez-vous que l'activité était autorisée ou attendue.
3. Corrigez la fonction Lambda potentiellement compromise.

   a. Désactivez les déclencheurs d'exécution de la fonction Lambda impliqués dans le résultat. Pour plus d'informations, consultez DeleteFunctionEventInvokeConfig.
   b. Examinez le code Lambda et mettez à jour les importations de bibliothèques et les couches de fonctions Lambda afin de supprimer les bibliothèques et les couches potentiellement suspectes.
   c. Atténuez les résultats Amazon Inspector liés à la fonction Lambda impliquée dans le résultat.

Estimation des GuardDuty coûts

Au cours de l'essai gratuit de 30 jours, vous pouvez utiliser la GuardDuty console ou les API opérations pour estimer les coûts d'utilisation moyens quotidiens de. GuardDuty L'estimation des coûts prévoit quels seront vos coûts estimés après la période d'essai. Toutefois, pour obtenir une estimation précise des coûts pendant l'essai gratuit, nous vous recommandons d' GuardDuty utiliser l' AWS Billing adresse suivante : https://console.aws.amazon.com/billing/.

Lorsque vous opérez dans un environnement à comptes multiples, le compte GuardDuty administrateur peut surveiller les indicateurs de coûts pour tous les comptes membres.

> **Remarque sur le coût d'utilisation de la protection contre les programmes malveillants pour S3**
>
> Le coût d'utilisation de Malware Protection for S3 n'est pas inclus dans la section Utilisation de la GuardDuty console. Pour de plus amples informations, veuillez consulter Affichage de l'utilisation et du coût de Malware Protection for S3.

Vous pouvez consulter l'estimation des coûts en fonction des métriques suivantes :

- Numéro de compte : indique le coût estimé pour votre compte, ou pour vos comptes de membre si vous utilisez un compte GuardDuty administrateur.
- Sources de données : répertorie le coût estimé pour chaque source de données de base (événements de AWS CloudTrail gestion, journaux de VPC flux et journaux de requêtes Route53 DNS Resolver).
- Fonctionnalités — Répertorie le coût estimé des GuardDuty fonctionnalités (événements de CloudTrail données pour S3, surveillance du journal EKS d'audit, données de EBS volume, activité de RDS connexion, surveillance du temps EKS d'exécution, surveillance du temps d'exécution Fargate, surveillance du temps d'exécution ou surveillance EC2 de l'activité réseau Lambda).
- Compartiments S3 : indique le coût estimé des événements de données S3 sur un compartiment spécifié ou les compartiments les plus chers pour les comptes de votre environnement. Cette statistique n'est disponible que lorsque vous activez Protection S3 un Compte AWS.

Comprendre comment GuardDuty calculer les coûts d'utilisation

Les estimations affichées dans la GuardDuty console peuvent être légèrement différentes de celles affichées dans votre AWS Billing and Cost Management console. La liste suivante explique comment GuardDuty estimer les coûts d'utilisation :

- L'estimation GuardDuty d'utilisation concerne uniquement la région actuelle.
- Le coût GuardDuty d'utilisation est basé sur les 30 derniers jours d'utilisation.
- L'estimation du coût d'utilisation de l'essai inclut l'estimation des sources de données de base et des fonctionnalités actuellement comprises dans la période d'essai. Chaque fonctionnalité et source de données qu'elle GuardDuty contient possède sa propre période d'essai, mais celle-ci peut chevaucher la période d'essai GuardDuty ou une autre fonctionnalité activée en même temps.
- L'estimation GuardDuty d'utilisation inclut les remises sur le prix en GuardDuty volume par région, comme indiqué sur la page de GuardDuty tarification d'Amazon, mais uniquement pour les comptes individuels respectant les niveaux de tarification en volume. Les remises sur volume ne sont pas incluses dans les estimations de l'utilisation totale combinée entre les comptes d'une organisation. Pour plus d'informations sur les tarifs relatifs à la réduction sur volume pour l'utilisation combinée, veuillez consulter Facturation AWS : remises sur volume (langue française non garantie).
- La somme des coûts d'utilisation pour chaque élément Compte AWS de votre organisation n'est pas toujours identique au coût estimé des 30 derniers jours pour la source de données sélectionnée. Le niveau de tarification peut changer à mesure que GuardDuty davantage d'événements ou de données sont traités. Pour plus d'informations, consultez la section Niveaux de tarification dans le guide de AWS Billing l'utilisateur.

Ce scénario explique que pour ne plus générer de coûts d'utilisation liés à la surveillance du temps d'exécution, les fonctionnalités de surveillance du temps d'exécution et de surveillance du temps d'EKSexécution doivent être désactivées.

GuardDuty a consolidé l'expérience de console pour la surveillance du EKS temps d'exécution dans la surveillance du temps d'exécution. GuardDuty recommande Vérifier l'état de configuration de EKS Runtime Monitoring etMigration de la surveillance du temps EKS d'exécution vers la surveillance du temps d'exécution.

Dans le cadre de la migration vers Runtime Monitoring, assurez-vous deDésactiver la surveillance de l'EKSexécution. Ceci est important car si vous choisissez ultérieurement de désactiver la surveillance du temps d'exécution et que vous ne le désactivez EKS pas, vous continuerez de devoir payer des frais d'utilisation pour EKS ce type de surveillance.

Surveillance du temps d'exécution : impact des journaux de VPC flux provenant EC2 des instances sur les coûts d'utilisation

Lorsque vous gérez l'agent de sécurité (manuellement ou via GuardDuty) dans EKS Runtime Monitoring ou Runtime Monitoring for EC2 instances, et qu'GuardDuty il est actuellement déployé sur une EC2 instance Amazon et que vous le recevez Types d'événement d'exécution collectés de cette instance, l'analyse Compte AWS des journaux de VPC flux provenant de cette EC2 instance Amazon ne vous GuardDuty sera pas facturée. Cela permet GuardDuty d'éviter le double coût d'utilisation sur le compte.

Comment GuardDuty estimer le coût d'utilisation des CloudTrail événements

Lorsque vous l'activez GuardDuty, il commence automatiquement à consommer les journaux d' AWS CloudTrail événements enregistrés pour votre compte dans le fichier sélectionné Région AWS. GuardDuty réplique les journaux des événements de service mondiaux, puis traite ces événements indépendamment dans chaque région où vous les avez GuardDuty activés. Cela permet de GuardDuty maintenir les profils des utilisateurs et des rôles dans chaque région afin d'identifier les anomalies.

Votre CloudTrail configuration n'a aucun impact sur les coûts GuardDuty d'utilisation ni sur le GuardDuty traitement de vos journaux d'événements. Vos frais GuardDuty d'utilisation dépendent de l'utilisation que vous AWS APIs faites de votre connexion CloudTrail. Pour de plus amples informations, veuillez consulter AWS CloudTrail événements de gestion.

Consulter les statistiques GuardDuty d'utilisation

Choisissez votre méthode d'accès préférée pour consulter les statistiques d'utilisation de votre GuardDuty compte. Si vous êtes un compte GuardDuty administrateur, les méthodes suivantes vous aideront à consulter les statistiques d'utilisation de tous les membres.

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

   Assurez-vous d'utiliser le compte GuardDuty administrateur.
2. Dans le panneau de navigation, choisissez Utilisateurs.
3. Sur la page Utilisation, un compte GuardDuty administrateur doté de comptes membres peut consulter le coût d'organisation estimé pour les 30 derniers jours. Il s'agit d'une estimation du coût d'utilisation total pour votre organisation.
4. GuardDuty les comptes d'administrateur avec des membres peuvent consulter la répartition des coûts d'utilisation par source de données ou par compte. Les comptes individuels ou autonomes peuvent consulter la répartition par source de données.

   Si vous avez des comptes membres, vous pouvez consulter les statistiques d'un compte individuel en sélectionnant ce compte dans le tableau Comptes.

   Dans l'onglet Par sources de données, lorsque vous sélectionnez une source de données associée à un coût d'utilisation, la somme correspondante de la répartition des coûts au niveau des comptes peut ne pas toujours être la même.

API/CLI

Exécutez l'GetUsageStatisticsAPIopération en utilisant les informations d'identification du compte GuardDuty administrateur. Fournissez les informations suivantes pour exécuter la commande :

- (Obligatoire) Indiquez l'ID du GuardDuty détecteur régional du compte pour lequel vous souhaitez récupérer les statistiques.
- (Obligatoire) L'un des types de statistique à récupérer : `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

  Actuellement, `TOP_ACCOUNTS_BY_FEATURE` ne prend pas en charge la récupération des statistiques d'utilisation pour`RDS_LOGIN_EVENTS`.
- (Obligatoire) fournissez une ou plusieurs sources de données ou fonctionnalités pour consulter vos statistiques d'utilisation.
- (Facultatif) Fournissez une liste des comptes IDs pour lesquels vous souhaitez récupérer des statistiques d'utilisation.

Vous pouvez également utiliser AWS Command Line Interface. La commande suivante est un exemple de récupération des statistiques d'utilisation pour toutes les sources de données et fonctionnalités, calculées par comptes. Assurez-vous de remplacer l'`detector-id` par votre propre ID de détecteur valide. Pour les comptes autonomes, cette commande renvoie le coût d'utilisation des 30 derniers jours pour votre compte uniquement. Si vous êtes un compte GuardDuty administrateur avec des comptes membres, les coûts sont répertoriés par compte pour tous les membres.

Pour trouver le `detectorId` correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la https://console.aws.amazon.com/guardduty/console ou exécutez le ListDetectorsAPI.

Remplacez `SUM_BY_ACCOUNT` par le type avec lequel vous souhaitez calculer les statistiques d'utilisation.

Pour surveiller le coût des sources de données uniquement

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

Pour surveiller le coût des fonctionnalités

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Sécurité dans Amazon GuardDuty

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à GuardDuty, veuillez consulter Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le AWSservice que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de GuardDuty. Elle vous montre comment configurer GuardDuty pour atteindre vos objectifs en matière de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS pour surveiller et sécuriser vos ressources GuardDuty.

Table des matières

Protection des données sur Amazon GuardDuty

Le modèle de responsabilité AWS partagée de s'applique à la protection des données sur Amazon GuardDuty. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent AWS services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec GuardDuty ou d'autres AWS services utilisateurs de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur

externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Chiffrement au repos

Toutes les données des GuardDuty clients sont cryptées au repos à l'aide de solutions de AWS chiffrement.

GuardDuty les données, telles que les résultats, sont chiffrées au repos à l'aide de AWS Key Management Service (AWS KMS) à l'aide AWS de clés gérées par le client.

Chiffrement en transit

GuardDuty analyse les données du journal provenant d'autres services. Il chiffre toutes les données en transit depuis ces services avec HTTPS etKMS. Une GuardDuty fois les informations nécessaires extraites des journaux, elles sont supprimées. Pour plus d'informations sur l' GuardDuty utilisation des informations provenant d'autres services, consultez la section Sources de GuardDuty données.

GuardDuty les données sont cryptées lors du transit entre les services.

Refus d’utiliser vos données pour améliorer le service

Vous pouvez choisir de refuser que vos données soient utilisées pour développer GuardDuty et améliorer d'autres services de AWS sécurité en utilisant la politique de AWS Organizations désinscription. Vous pouvez choisir de vous désinscrire même si aucune donnée de ce type GuardDuty n'est actuellement collectée. Pour plus d'informations sur la procédure de désactivation, veuillez consulter Politiques de désactivation des services IA dans le Guide de l'utilisateur AWS Organizations .

> **Note**
>
> Pour que vous puissiez utiliser la politique de désinscription, vos AWS comptes doivent être gérés de manière centralisée par AWS Organizations. Si vous n'avez pas encore créé d'organisation pour vos AWS comptes, consultez la section Création et gestion d'une organisation dans le Guide de AWS Organizations l'utilisateur.

Les effets de la désactivation sont les suivants :

- GuardDuty supprimera les données collectées et stockées à des fins d'amélioration du service avant votre désinscription (le cas échéant).
- Après votre désinscription, GuardDuty nous ne collecterons ni ne stockerons ces données à des fins d'amélioration du service.

Les rubriques suivantes expliquent comment chaque fonctionnalité GuardDuty peut potentiellement gérer vos données dans le but d'améliorer le service.

Table des matières

GuardDuty Surveillance du temps d'exécution

GuardDuty La surveillance du temps d'exécution permet de détecter les menaces liées à l'exécution pour les clusters Amazon Elastic Kubernetes Service (EKSAmazon) AWS Fargate (Fargate) , Amazon Elastic Container Service (ECSAmazon) uniquement et les instances Amazon Elastic Compute Cloud (EC2Amazon) de votre environnement. AWS Après avoir activé la surveillance du temps d'exécution et déployé l'agent de GuardDuty sécurité pour votre ressource, GuardDuty commencez à surveiller et à analyser les événements d'exécution associés à votre ressource. Ces types d'événements d'exécution incluent les événements de processus, les événements de conteneur, les DNS événements, etc. Pour de plus amples informations, veuillez consulter Types d'événements d'exécution collectés qui GuardDuty utilisent.

Bien qu'il collecte GuardDuty désormais des arguments de ligne de commande que vous pouvez rediriger vers vos charges de travail, il n'utilise actuellement pas ces arguments à des fins d'amélioration du service (il se peut qu'il le fasse à l'avenir). Nous avons commencé à collecter des arguments en ligne de commande en prévision des nouvelles règles de détection des menaces et des résultats qui seront publiés prochainement. Votre confiance, votre confidentialité et la sécurité de votre contenu sont nos priorités absolues et garantissent que notre utilisation est conforme à nos engagements envers vous. Pour plus d'informations, consultez la section Confidentialité des données FAQ.

GuardDuty Protection contre les logiciels malveillants

GuardDuty Malware Protection analyse et détecte les programmes malveillants contenus dans les EBS volumes attachés à vos charges de travail d'EC2instance et de conteneur Amazon

potentiellement compromises, ainsi que dans les fichiers récemment chargés dans les compartiments Amazon S3 que vous avez sélectionnés. Actuellement, GuardDuty ne collecte ni n'utilise les logiciels malveillants détectés pour améliorer le service. Toutefois, à l'avenir, lorsque GuardDuty Malware Protection identifie un fichier de EBS volume ou un fichier S3 comme étant malveillant ou dangereux, GuardDuty Malware Protection collectera et stockera ce fichier afin de développer et d'améliorer ses détections de malwares, ainsi que le GuardDuty service. Ce fichier peut également être utilisé pour développer et améliorer d'autres services AWS de sécurité. Votre confiance, votre confidentialité et la sécurité de votre contenu sont nos priorités absolues et garantissent que notre utilisation est conforme à nos engagements envers vous. Pour plus d'informations, consultez la section Confidentialité des données FAQ.

Journalisation des appels GuardDuty d'API Amazon avec AWS CloudTrail

Amazon GuardDuty est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans GuardDuty. CloudTrail capture tous les appels d'API GuardDuty sous forme d'événements, y compris les appels depuis la GuardDuty console et les appels de code vers les GuardDuty API. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un bucket Amazon Simple Storage Service (Amazon S3), y compris les événements pour. GuardDuty Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite GuardDuty, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour plus d'informations CloudTrail, notamment sur la manière de le configurer et de l'activer, consultez le guide de AWS CloudTrail l'utilisateur.

GuardDuty informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité événementielle prise en charge se produit dans GuardDuty, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements AWS de service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour GuardDuty, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions . Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, veuillez consulter les rubriques :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification de connexion d'utilisateur root ou d'utilisateur IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été effectuée par un autre service AWS

Pour de plus amples informations, veuillez consulter Élément CloudTrail userIdentity.

GuardDuty événements du plan de contrôle dans CloudTrail

Par défaut, CloudTrail enregistre toutes les opérations GuardDuty d'API fournies dans le Amazon GuardDuty API Reference sous forme d'événements dans CloudTrail des fichiers.

GuardDuty événements de données dans CloudTrail

GuardDuty Surveillance du temps d'exécutionutilise un agent de GuardDuty sécurité déployé sur vos clusters Amazon Elastic Kubernetes Service (Amazon EKS), vos AWS Fargate instances Amazon Elastic Compute Cloud (Amazon EC2) et vos tâches (Amazon Elastic Container Service (Amazon ECS) uniquement) pour collecter un module complémentaire Types d'événement d'exécution

collectés () AWS qui collecte pour vos charges de travail puis les envoie `aws-guardduty-agent` à des fins de détection et d'analyse des menaces. GuardDuty

Enregistrement et surveillance des événements de données

Vous pouvez éventuellement configurer les AWS CloudTrail journaux pour afficher les événements de données relatifs à votre agent GuardDuty de sécurité.

Pour créer et configurer CloudTrail, consultez la section Événements liés aux données dans le guide de l'AWS CloudTrailutilisateur et suivez les instructions relatives à la journalisation des événements de données à l'aide des sélecteurs d'événements avancés dans le AWS Management Console. Lorsque vous enregistrez le journal de suivi, veillez à apporter les modifications suivantes :

- Pour le type d'événement Data, choisissez GuardDuty detector.
- Pour le modèle de sélecteur de journal, choisissez Consigner tous les événements.
- Développez la vue JSON pour la configuration. Elle doit être similaire au JSON suivant :

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Après avoir activé le sélecteur pour le parcours, accédez à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/. Vous pouvez télécharger les événements de données depuis le compartiment S3 que vous avez choisi au moment de configurer les CloudTrail journaux.

Exemple : entrées de fichier GuardDuty journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'événement du plan de données.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
```

```
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateIPThreatIntelSet`action (événement du plan de contrôle).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
```

```
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


À partir des informations de cet événement, vous pouvez déterminer que la demande a été effectuée pour créer un `Example` de liste de menaces dans GuardDuty. Vous pouvez également voir que la demande a été effectuée par un utilisateur nommé Alice le 14 juin 2018.

Identity and Access Management pour Amazon GuardDuty

AWS Identity and Access Management (IAM) est un outil AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les GuardDuty ressources. IAMest un AWS service outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Authentification par des identités
- Gestion des accès à l’aide de politiques
- Comment Amazon GuardDuty travaille avec IAM
- Exemples de politiques basées sur l'identité pour Amazon GuardDuty
- Utilisation de rôles liés à un service pour Amazon GuardDuty
- AWS politiques gérées pour Amazon GuardDuty
- Résolution des problèmes liés à GuardDuty l'identité et à l'accès à Amazon

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez GuardDuty.

Utilisateur du service : si vous utilisez le GuardDuty service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles GuardDuty fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans GuardDuty, consultezRésolution des problèmes liés à GuardDuty l'identité et à l'accès à Amazon.

Administrateur du service — Si vous êtes responsable des GuardDuty ressources de votre entreprise, vous avez probablement un accès complet à GuardDuty. C'est à vous de déterminer les GuardDuty fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec GuardDuty, voirComment Amazon GuardDuty travaille avec IAM.

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à GuardDuty. Pour consulter des exemples de politiques GuardDuty basées sur l'identité que vous pouvez utiliser dansIAM, consultez. Exemples de politiques basées sur l'identité pour Amazon GuardDuty

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des AWS API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d’authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le guide de AWS IAM Identity Center l'utilisateur et Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'IAMutilisateur.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes AWS services les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l’utilisateur racine pour vos tâches quotidiennes. Protégez vos informations

d’identification d’utilisateur racine et utilisez-les pour effectuer les tâches que seul l’utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide AWS services d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies AWS services par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d’utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour

de grands ensembles d’utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu’un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d’informations d’identification permanentes, mais les rôles fournissent des informations d’identification temporaires. Pour en savoir plus, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s’authentifie, l’identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d’informations sur les jeux d’autorisations, consultez la rubrique Jeux d’autorisations dans le Guide de l’utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d’accorder l’accès intercompte. Toutefois, dans certains AWS services cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

- Accès multiservices — Certains AWS services utilisent des fonctionnalités dans d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui AWS CLI soumettent des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d’aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d’une politique qui autorise l’action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l’identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Les politiques basées sur l’identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une

politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui

spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.

- Politiques de contrôle des services (SCPs) : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment Amazon GuardDuty travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à GuardDuty, découvrez quelles IAM fonctionnalités sont disponibles GuardDuty.

IAMfonctionnalités que vous pouvez utiliser avec Amazon GuardDuty

IAMfonctionnalité	GuardDuty soutien
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d’une politique	Oui
ACLs	Non
ABAC(balises dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble du fonctionnement de la plupart des IAM fonctionnalités GuardDuty et des autres AWS services, reportez-vous à la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur.

Politiques basées sur l'identité pour GuardDuty

Prend en charge les politiques basées sur l’identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour GuardDuty

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon GuardDuty

Politiques basées sur les ressources au sein de GuardDuty

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L’ajout d’un principal entre comptes à une politique basée sur les ressources ne représente qu’une partie de l’instauration de la relation d’approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte de confiance doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l’entité. Toutefois, si une politique basée sur des ressources accorde l’accès à un principal dans le même compte, aucune autre politique basée sur l’identité n’est requise. Pour plus d'informations, voir Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions politiques pour GuardDuty

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des GuardDuty actions, consultez la section Actions définies par Amazon GuardDuty dans le Service Authorization Reference.

Les actions de politique en GuardDuty cours utilisent le préfixe suivant avant l'action :

```
guardduty
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon GuardDuty

Ressources politiques pour GuardDuty

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de GuardDuty ressources et leurs caractéristiquesARNs, consultez la section Ressources définies par Amazon GuardDuty dans le Service Authorization Reference. Pour savoir quelles actions vous pouvez définir pour chaque ressource, consultez la ARN section Actions définies par Amazon GuardDuty.

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon GuardDuty

Clés de conditions de politique pour GuardDuty

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Pour consulter la liste des clés de GuardDuty condition, consultez la section Clés de condition pour Amazon GuardDuty dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon GuardDuty.

Pour consulter des exemples de politiques GuardDuty basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Amazon GuardDuty

Listes de contrôle d'accès (ACLs) dans GuardDuty

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Contrôle d'accès basé sur les attributs () ABAC avec GuardDuty

Supports ABAC (balises dans les politiques) : Partiel

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l’accès basé sur des étiquettes, vous devez fournir les informations d’étiquette dans l’élément de condition d’une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation d'informations d'identification temporaires avec GuardDuty

Prend en charge les informations d’identification temporaires : oui

Certains AWS services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui AWS services fonctionnent avec des informations d'identification temporaires, consultez AWS services la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d’identification temporaires lorsque vous vous connectez à la console en tant qu’utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour GuardDuty

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour GuardDuty

Prend en charge les rôles de service : oui

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber GuardDuty les fonctionnalités. Modifiez les rôles de service uniquement lorsque GuardDuty vous recevez des instructions à cet effet.

Rôles liés à un service pour GuardDuty

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles GuardDuty liés à un service, consultez. Utilisation de rôles liés à un service pour Amazon GuardDuty

Pour plus de détails sur la création ou la gestion des rôles liés à un service, consultez la section AWS Services compatibles avec. IAM Recherchez un service dans le tableau qui inclut un `Yes` dans la

colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Amazon GuardDuty

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier GuardDuty des ressources. Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par GuardDuty, y compris le format de ARNs pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon GuardDuty dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la GuardDuty console
- Autorisations requises pour activer GuardDuty
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- IAMPolitique personnalisée pour accorder un accès en lecture seule à GuardDuty
- Refuser l'accès aux GuardDuty résultats
- Utilisation d'une IAM politique personnalisée pour limiter l'accès aux GuardDuty ressources

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer GuardDuty des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l’identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique AWS service, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la GuardDuty console

Pour accéder à la GuardDuty console Amazon, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails GuardDuty des ressources de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la GuardDuty console, associez également la politique GuardDuty `ConsoleAccess` ou la politique `ReadOnly` AWS gérée aux entités. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le Guide de IAM l'utilisateur.

Autorisations requises pour activer GuardDuty

Pour accorder les autorisations nécessaires à différentes IAM identités (utilisateurs, groupes et rôles), attachez la AWS politique gérée : AmazonGuardDutyFullAccess politique requise pour les activer GuardDuty.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
```

```
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

IAMPolitique personnalisée pour accorder un accès en lecture seule à GuardDuty

Pour accorder un accès en lecture seule, GuardDuty vous pouvez utiliser la politique `AmazonGuardDutyReadOnlyAccess` gérée.

Pour créer une politique personnalisée qui accorde à un IAM rôle, à un utilisateur ou à un groupe un accès en lecture seule GuardDuty, vous pouvez utiliser l'instruction suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
```

```
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

Refuser l'accès aux GuardDuty résultats

Vous pouvez utiliser la politique suivante pour refuser à un IAM rôle, à un utilisateur ou à un groupe l'accès aux GuardDuty résultats. Les utilisateurs ne peuvent pas consulter les résultats ni les détails les concernant, mais ils peuvent accéder à toutes les autres GuardDuty opérations :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
```

```
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
```

```
}
```

Utilisation d'une IAM politique personnalisée pour limiter l'accès aux GuardDuty ressources

Pour définir l'accès d'un utilisateur en GuardDuty fonction de l'ID du détecteur, vous pouvez utiliser toutes les GuardDutyAPIactions de vos IAM politiques personnalisées, à l'exception des opérations suivantes :

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Utilisez les opérations suivantes dans une IAM politique pour définir l'accès d'un utilisateur en GuardDuty fonction de l'IPSetID et de l' ThreatIntelSet ID :

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

Les exemples suivants montrent comment créer des stratégies à l'aide de certains des opérations précédentes :

- Cette politique permet à un utilisateur d'exécuter l'opération `guardduty:UpdateDetector`, à l'aide de l'ID de détecteur 1234567 dans la région us-east-1 :

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Cette politique permet à un utilisateur d'exécuter l'`guardduty:UpdateIPSet`opération en utilisant l'ID de détecteur 1234567 et l'IPSetID 000000 dans la région us-east-1 :

> **Note**
>
> Assurez-vous que l'utilisateur dispose des autorisations requises pour accéder aux listes d'adresses IP fiables et aux listes de menaces dans GuardDuty. Pour de plus amples informations, veuillez consulter Autorisations requises pour charger les listes d'adresses IP approuvées et les listes de menaces.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- Cette politique permet à un utilisateur d'exécuter l'`guardduty:UpdateIPSet`opération en utilisant n'importe quel identifiant de détecteur et l'IPSetID 000000 dans la région us-east-1 :

> **Note**
>
> Assurez-vous que l'utilisateur dispose des autorisations requises pour accéder aux listes d'adresses IP fiables et aux listes de menaces dans GuardDuty. Pour de plus amples informations, veuillez consulter Autorisations requises pour charger les listes d'adresses IP approuvées et les listes de menaces.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Cette politique permet à un utilisateur d'exécuter l'`guardduty:UpdateIPSet`opération en utilisant son identifiant de détecteur et n'importe quel IPSet identifiant de la région us-east-1 :

> **Note**
>
> Assurez-vous que l'utilisateur dispose des autorisations requises pour accéder aux listes d'adresses IP fiables et aux listes de menaces dans GuardDuty. Pour de plus amples informations, veuillez consulter Autorisations requises pour charger les listes d'adresses IP approuvées et les listes de menaces.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "guardduty:UpdateIPSet",
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Utilisation de rôles liés à un service pour Amazon GuardDuty

Amazon GuardDuty utilise AWS Identity and Access Management (IAM) des rôles liés à un service. Un rôle lié à un service (SLR) est un type unique de IAM rôle directement lié à. GuardDuty Les rôles liés aux services sont prédéfinis par GuardDuty et incluent toutes les autorisations nécessaires pour GuardDuty appeler d'autres AWS services en votre nom.

Avec un rôle lié à un service, vous pouvez le configurer GuardDuty sans ajouter manuellement les autorisations nécessaires. GuardDuty définit les autorisations de son rôle lié au service et, sauf si les autorisations sont définies autrement, seul GuardDuty peut assumer le rôle. Les autorisations définies incluent la politique de confiance et la politique d'autorisations, et cette politique d'autorisations ne peut être attachée à aucune autre IAM entité.

GuardDuty prend en charge l'utilisation de rôles liés aux services dans toutes les régions où cela GuardDuty est disponible. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.

Vous ne pouvez supprimer le rôle GuardDuty lié à un service qu'après l'avoir d'abord désactivé GuardDuty dans toutes les régions où il est activé. Cela protège vos GuardDuty ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'y accéder.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur et recherchez les services dont la valeur est Oui dans la colonne Rôle lié au service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour GuardDuty

GuardDuty utilise le rôle lié au service (SLR) nommé. `AWSServiceRoleForAmazonGuardDuty` SLRPermet d' GuardDuty effectuer les tâches suivantes. Cela permet également GuardDuty d'inclure les métadonnées récupérées appartenant à l'EC2instance dans les résultats qui GuardDuty peuvent être générés concernant la menace potentielle. Le rôle lié à un service

`AWSServiceRoleForAmazonGuardDuty` fait confiance au service `guardduty.amazonaws.com` pour endosser le rôle.

Les politiques d'autorisation permettent GuardDuty d'effectuer les tâches suivantes :

- Utilisez EC2 les actions Amazon pour gérer et récupérer des informations sur vos EC2 instances, vos images et vos composants réseau tels que VPCs les sous-réseaux et les passerelles de transit.
- Utilisez AWS Systems Manager des actions pour gérer les SSM associations sur les EC2 instances Amazon lorsque vous activez la surveillance du temps GuardDuty d'exécution avec un agent automatisé pour AmazonEC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les EC2 instances dotées d'une balise d'inclusion (`GuardDutyManaged:true`).
- Utilisez AWS Organizations des actions pour décrire les comptes associés et l'identifiant de l'organisation.
- Utilisez les actions Amazon S3 pour récupérer des informations sur les compartiments et les objets S3.
- Utilisez AWS Lambda des actions pour récupérer des informations sur vos fonctions et balises Lambda.
- Utilisez EKS les actions Amazon pour gérer et récupérer des informations sur les EKS clusters et gérer les EKSmodules complémentaires Amazon sur les EKS clusters. Les EKS actions récupèrent également les informations relatives aux balises associées à GuardDuty.
- IAMÀ utiliser pour créer la protection contre les EC2 programmes malveillants Autorisations de rôle liées à un service pour Malware Protection pour EC2 après l'activation de.
- Utilisez ECS les actions Amazon pour gérer et récupérer des informations sur les ECS clusters Amazon, et gérez les paramètres du ECS compte Amazon avec`guarddutyActivate`. Les actions relatives à Amazon récupèrent ECS également les informations relatives aux tags associés à GuardDuty.

Le rôle est configuré avec la stratégie gérée AWS suivante, nommée `AmazonGuardDutyServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
```

```
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
```

```
            "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
```

```
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
```

```
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
```

```
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
}
```

Voici la stratégie d'approbation qui est attachée au rôle lié à un service `AWSServiceRoleForAmazonGuardDuty` :

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Pour plus de détails sur les mises à jour `AmazonGuardDutyServiceRolePolicy` de la politique, consultezGuardDuty mises à jour des politiques AWS gérées. Pour recevoir des alertes automatiques concernant les modifications apportées à cette politique, abonnez-vous au RSS fil d'actualité de la Historique de la documentation page.

Création d'un rôle lié à un service pour GuardDuty

Le rôle `AWSServiceRoleForAmazonGuardDuty` lié au service est automatiquement créé lorsque vous l'activez GuardDuty pour la première fois ou lorsque vous l'activez GuardDuty dans une région prise en charge où il n'était pas activé auparavant. Vous pouvez également créer le rôle lié à un service manuellement à l'aide de la IAM console, du AWS CLI, ou du. IAM API

> **Important**
>
> Le rôle lié au service créé pour le compte d'administrateur GuardDuty délégué ne s'applique pas aux comptes des membres GuardDuty .

Vous devez configurer les autorisations pour autoriser un IAM principal (tel qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForAmazonGuardDuty` lié au service soit correctement créé, le IAM principal GuardDuty avec lequel vous l'utilisez doit disposer des autorisations requises. Pour accorder les autorisations requises, attachez la stratégie suivante à cet utilisateur, groupe ou rôle :

> **Note**
>
> Remplacez l'échantillon *`account ID`* dans l'exemple suivant avec votre identifiant de AWS compte réel.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Pour plus d'informations sur la création manuelle du rôle, voir Création d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Modification d'un rôle lié à un service pour GuardDuty

GuardDuty ne vous permet pas de modifier le rôle `AWSServiceRoleForAmazonGuardDuty` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Vous pouvez toutefois modifier la

description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Supprimer un rôle lié à un service pour GuardDuty

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

> **Important**
>
> Si vous avez activé la protection contre les programmes malveillants pourEC2, la suppression `AWSServiceRoleForAmazonGuardDuty` n'est pas automatiquement supprimée`AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Si vous souhaitez effectuer une suppression`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, reportez-vous à la section Suppression d'un rôle lié à un service pour Malware Protection for. EC2

Vous devez d'abord GuardDuty le désactiver dans toutes les régions où il est activé afin de supprimer le`AWSServiceRoleForAmazonGuardDuty`. Si le GuardDuty service n'est pas désactivé lorsque vous essayez de supprimer le rôle lié au service, la suppression échoue. Pour de plus amples informations, veuillez consulter Suspension ou désactivation GuardDuty.

Lorsque vous le désactivez GuardDuty, le `AWSServiceRoleForAmazonGuardDuty` fichier n'est pas supprimé automatiquement. Si vous GuardDuty réactivez, il commencera à utiliser l'existant`AWSServiceRoleForAmazonGuardDuty`.

Pour supprimer manuellement le rôle lié à un service à l'aide de IAM

Utilisez la IAM console AWS CLI, le ou le IAM API pour supprimer le rôle `AWSServiceRoleForAmazonGuardDuty` lié au service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Soutenu Régions AWS

Amazon GuardDuty prend en charge l'utilisation du rôle `AWSServiceRoleForAmazonGuardDuty` lié au service dans tous les Régions AWS endroits où cela GuardDuty est disponible. Pour obtenir la liste des régions dans lesquelles cette GuardDuty option est actuellement disponible, consultez la

section GuardDuty Points de terminaison et quotas Amazon dans le Référence générale d'Amazon Web Services.

Autorisations de rôle liées à un service pour Malware Protection pour EC2

Malware Protection for EC2 utilise le rôle lié au service (SLR) nommé. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Cela SLR permet à Malware Protection EC2 d'effectuer des analyses sans agent pour détecter les logiciels malveillants dans votre GuardDuty compte. Il permet GuardDuty de créer un instantané EBS du volume dans votre compte et de partager cet instantané avec le compte GuardDuty de service. Après avoir GuardDuty évalué le snapshot, celui-ci inclut les métadonnées de charge de travail de l'EC2instance et du conteneur récupérées dans la protection contre les logiciels malveillants pour obtenir des EC2 résultats. Le rôle lié à un service `AWSServiceRoleForAmazonGuardDutyMalwareProtection` fait confiance au service `malware-protection.guardduty.amazonaws.com` pour endosser le rôle.

Les politiques d'autorisation relatives à ce rôle aident Malware Protection for EC2 à effectuer les tâches suivantes :

- Utilisez les actions Amazon Elastic Compute Cloud (AmazonEC2) pour récupérer des informations sur vos EC2 instances, volumes et instantanés Amazon. Malware Protection for fournit EC2 également l'autorisation d'accéder aux métadonnées d'Amazon EKS et ECS du cluster Amazon.
- Créez des instantanés pour les EBS volumes dont la `GuardDutyExcluded` balise n'est pas définie sur. `true` Par défaut, les instantanés sont créés avec une balise `GuardDutyScanId`. Ne supprimez pas cette balise, sinon Malware Protection for n'EC2aura pas accès aux instantanés.

  > **Important**
  >
  > Lorsque vous définissez le `GuardDutyExcluded` paramètre sur`true`, le GuardDuty service ne pourra plus accéder à ces instantanés à l'avenir. Cela est dû au fait que les autres instructions de ce rôle lié au service GuardDuty empêchent toute action sur les instantanés définis sur. `GuardDutyExcluded` `true`

- Autoriser le partage et la suppression d'instantanés uniquement si la balise `GuardDutyScanId` existe et que la balise `GuardDutyExcluded` n'est pas définie sur `true`.

> **Note**
>
> N'autorise pas la protection contre les logiciels malveillants EC2 à rendre les instantanés publics.

- Accédez aux clés gérées par le client, à l'exception de celles dont le `GuardDutyExcluded` tag est défini sur`true`, `CreateGrant` pour appeler pour créer et accéder à un EBS volume chiffré à partir de l'instantané chiffré partagé avec le compte de GuardDuty service. Pour obtenir la liste des comptes de GuardDuty service pour chaque région, voirGuardDuty comptes de service par Région AWS.
- Accédez aux CloudWatch journaux des clients pour créer le groupe de EC2 journaux Malware Protection for Malware et placez les journaux des événements d'analyse des programmes malveillants dans le `/aws/guardduty/malware-scan-events` groupe de journaux.
- Autoriser le client à décider s'il souhaite conserver dans son compte les instantanés sur lesquels le logiciel malveillant a été détecté. Si l'analyse détecte un logiciel malveillant, le rôle lié au service permet d' GuardDuty ajouter deux balises aux instantanés : et. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> La balise `GuardDutyFindingDetected` indique que les instantanés contiennent des logiciels malveillants.

- Déterminez si un volume est chiffré à l'aide d'une clé EBS gérée. GuardDuty exécute l'`DescribeKey`action pour déterminer `key Id` la clé EBS gérée de votre compte.
- Récupérez l'instantané des EBS volumes chiffrés à l'aide de Clé gérée par AWS, depuis votre Compte AWS et copiez-le dans leGuardDuty compte de service. À cette fin, nous utilisons les autorisations `GetSnapshotBlock` et`ListSnapshotBlocks`. GuardDuty scannera ensuite le cliché dans le compte de service. À l'heure actuelle, la protection contre les programmes malveillants pour la EC2 prise en charge de l'analyse des EBS volumes chiffrés avec Clé gérée par AWS peut ne pas être disponible dans tous les Régions AWS. Pour de plus amples informations, veuillez consulter Disponibilité des fonctionnalités propres à la région.
- Autorisez Amazon EC2 à appeler AWS KMS au nom de Malware Protection pour EC2 effectuer plusieurs actions cryptographiques sur les clés gérées par le client. Des actions telles que `kms:ReEncryptTo` et `kms:ReEncryptFrom` sont nécessaires pour partager les instantanés

chiffrés avec les clés gérées par le client. Seules les clés suivantes pour lesquelles la balise `GuardDutyExcluded` n'est pas définie `true` sur sont accessibles.

Le rôle est configuré avec la stratégie gérée AWS suivante, nommée `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
```

```
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
```

```
                "aws:ResourceTag/GuardDutyExcluded": "true"
            }
        }
    },
    {
        "Sid": "PreventPublicAccessToSnapshotPermission",
        "Effect": "Deny",
        "Action": [
            "ec2:ModifySnapshotAttribute"
        ],
        "Resource": "arn:aws:ec2:*:*:snapshot/*",
        "Condition": {
            "StringEquals": {
                "ec2:Add/group": "all"
            }
        }
    },
    {
        "Sid": "CreateGrantPermission",
        "Effect": "Allow",
        "Action": "kms:CreateGrant",
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "Null": {
                "aws:ResourceTag/GuardDutyExcluded": "true"
            },
            "StringLike": {
                "kms:EncryptionContext:aws:ebs:id": "snap-*"
            },
            "ForAllValues:StringEquals": {
                "kms:GrantOperations": [
                    "Decrypt",
                    "CreateGrant",
                    "GenerateDataKeyWithoutPlaintext",
                    "ReEncryptFrom",
                    "ReEncryptTo",
                    "RetireGrant",
                    "DescribeKey"
                ]
            },
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
```

```
        },
        {
            "Sid": "ShareSnapshotKMSPermission",
            "Effect": "Allow",
            "Action": [
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "ec2.*.amazonaws.com"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "GuardDutyLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:CreateLogGroup",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
        },
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
```

```
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

La stratégie d'approbation suivante est attachée au rôle lié à un service `AWSServiceRoleForAmazonGuardDutyMalwareProtection` :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Création d'un rôle lié à un service pour Malware Protection for EC2

Le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié au service est automatiquement créé lorsque vous activez la protection contre les programmes malveillants EC2 pour la première fois ou lorsque vous activez la protection contre les programmes malveillants EC2 dans une région prise en charge où elle n'était pas activée auparavant. Vous pouvez également

créer le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié à un service manuellement à l'aide de la IAM console, du IAMCLI, ou du. IAM API

> **Note**
>
> Par défaut, si vous utilisez Amazon pour la première fois GuardDuty, la protection contre les programmes malveillants EC2 est automatiquement activée.

> **Important**
>
> Le rôle lié au service créé pour le compte d' GuardDuty administrateur délégué ne s'applique pas aux comptes des membres GuardDuty .

Vous devez configurer les autorisations pour autoriser un IAM principal (tel qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié au service soit correctement créé, l'IAMidentité que vous utilisez GuardDuty doit disposer des autorisations requises. Pour accorder les autorisations requises, attachez la stratégie suivante à cet utilisateur, groupe ou rôle :

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Pour plus d'informations sur la création manuelle du rôle, voir Création d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Modification d'un rôle lié à un service pour Malware Protection for EC2

Malware Protection for EC2 ne vous permet pas de modifier le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Vous pouvez toutefois modifier la description du rôle à l'aide deIAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Suppression d'un rôle lié à un service pour Malware Protection for EC2

Si vous n’avez plus besoin d’utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement.

> **Important**
>
> Pour le supprimer`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, vous devez d'abord désactiver la protection contre les programmes malveillants EC2 dans toutes les régions où elle est activée.
> Si la protection contre les programmes malveillants EC2 n'est pas désactivée lorsque vous essayez de supprimer le rôle lié au service, la suppression échouera. Pour de plus amples informations, veuillez consulter Pour activer ou désactiver l'analyse des programmes malveillants GuardDuty initiée.

Lorsque vous choisissez Désactiver pour arrêter le EC2 service de protection contre les programmes malveillants, celui-ci n'`AWSServiceRoleForAmazonGuardDutyMalwareProtection`est pas automatiquement supprimé. Si vous choisissez ensuite Activer pour redémarrer le EC2 service de protection contre les programmes malveillants, GuardDuty vous commencerez à utiliser le service existant`AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Pour supprimer manuellement le rôle lié à un service à l'aide de IAM

Utilisez la IAM console AWS CLI, le ou le IAM API pour supprimer le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié au service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'IAMutilisateur.

Soutenu Régions AWS

Amazon GuardDuty prend en charge l'utilisation du rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié au service dans tous les domaines Régions AWS où Malware Protection for EC2 est disponible.

Pour obtenir la liste des régions dans lesquelles cette GuardDuty option est actuellement disponible, consultez la section GuardDuty Points de terminaison et quotas Amazon dans le Référence générale d'Amazon Web Services.

> **Note**
>
> La protection contre les programmes malveillants n'EC2est actuellement pas disponible dans AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest).

AWS politiques gérées pour Amazon GuardDuty

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par les IAM clients qui fournissent à votre équipe uniquement les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent parfois des autorisations supplémentaires à une politique AWS gérée pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont plus susceptibles de mettre à jour une politique AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir une liste et une description des politiques relatives aux fonctions de travail, voir les politiques AWS gérées pour les fonctions de travail dans le Guide de IAM l'utilisateur.

L'élément de politique `Version` spécifie les règles de syntaxe de langage qui doivent être utilisées pour traiter une politique. Les politiques suivantes incluent la version actuelle qui IAM prend en charge. Pour plus d'informations, voir Éléments IAM JSON de politique : Version.

AWS politique gérée : AmazonGuardDutyFullAccess

Vous pouvez associer la `AmazonGuardDutyFullAccess` politique à votre IAM identité.

Cette politique accorde des autorisations administratives qui permettent à l'utilisateur d'avoir un accès complet à toutes les GuardDuty actions.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `GuardDuty`— Permet aux utilisateurs d'accéder pleinement à toutes les GuardDuty actions.
- `IAM`:
  - Permet aux utilisateurs de créer le rôle GuardDuty lié au service.
  - Permet à un compte administrateur d'activer GuardDuty les comptes des membres.
  - Permet aux utilisateurs de transmettre un rôle GuardDuty qui utilise ce rôle pour activer la fonctionnalité GuardDuty Malware Protection for S3. Cela s'applique quelle que soit la manière dont vous activez la protection contre les programmes malveillants pour S3, que ce soit dans le cadre du GuardDuty service ou indépendamment.
- `Organizations`— Permet aux utilisateurs de désigner un administrateur délégué et de gérer les membres d'une GuardDuty organisation.

L'autorisation d'effectuer une `iam:GetRole` action permet de `AWSServiceRoleForAmazonGuardDutyMalwareProtection` déterminer si le rôle lié au service (SLR) pour Malware Protection for EC2 existe dans un compte.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        },
        {
            "Sid": "AllowPassRoleToMalwareProtectionPlan",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS politique gérée : AmazonGuardDutyReadOnlyAccess

Vous pouvez associer la `AmazonGuardDutyReadOnlyAccess` politique à votre IAM identité.

Cette politique accorde des autorisations en lecture seule qui permettent à un utilisateur de consulter les GuardDuty résultats et les détails de votre GuardDuty organisation.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `GuardDuty`— Permet aux utilisateurs de consulter GuardDuty les résultats et d'effectuer API des opérations commençant par `GetList`, ou`Describe`.
- `Organizations`— Permet aux utilisateurs de récupérer des informations sur la configuration de votre GuardDuty organisation, notamment les détails du compte d'administrateur délégué.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AmazonGuardDutyServiceRolePolicy

Vous ne pouvez pas vous attacher `AmazonGuardDutyServiceRolePolicy` à vos IAM entités. Cette politique AWS gérée est associée à un rôle lié à un service qui permet d' GuardDuty effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Autorisations de rôle liées à un service pour GuardDuty.

GuardDuty mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées GuardDuty depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS fil sur la page Historique du GuardDuty document.

Modification	Description	Date
AmazonGuardDutyServiceRolePolicy – Mise à jour d'une stratégie existante	L'`ec2:DescribeVpcs` autorisation a été ajoutée. Cela permet GuardDuty de suivre les VPC mises à jour, par exemple de récupérer le VPCCIDR.	22 août 2024
AmazonGuardDutyServiceRolePolicy – Mise à jour d'une politique existante	Autorisation ajoutée qui vous permet de transmettre un IAM rôle GuardDuty lorsque vous activez Malware Protection pour S3. `{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": [ "iam:PassRole"`	10 juin 2024

Modification	Description	Date
	`], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "guardduty.amazonaws.com" } } } }`	
AmazonGuardDutyServiceRolePolicy - Mettre à jour vers une politique existante.	Utilisez AWS Systems Manager des actions pour gérer les SSM associations sur les EC2 instances Amazon lorsque vous activez la surveillance du temps GuardDuty d'exécution avec un agent automatisé pour AmazonEC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les EC2 instances dotées d'une balise d'inclusion (`GuardDutyManaged :true`).	26 mars 2024

Modification	Description	Date
AmazonGuardDutyServiceRolePolicy - Mettre à jour vers une politique existante.	GuardDuty a ajouté une nouvelle autorisation : `organization:DescribeOrganization` pour récupérer l'ID d'organisation du VPC compte Amazon partagé et définir la politique de point de VPC terminaison Amazon avec l'ID d'organisation.	9 février 2024
AmazonGuardDutyMalwareProtectionServiceRolePolicy - Mettre à jour vers une politique existante.	Malware Protection for EC2 a ajouté deux autorisations : `GetSnapshotBlock` celle de `ListSnapshotBlocks` récupérer l'instantané d'un EBS volume (crypté à l'aide Clé gérée par AWS) depuis votre compte de service Compte AWS et de le copier sur le compte de GuardDuty service avant de lancer l'analyse des logiciels malveillants.	25 janvier 2024
AmazonGuardDutyServiceRolePolicy – Mise à jour d’une politique existante	Ajout de nouvelles autorisations pour permettre GuardDuty d'ajouter des paramètres de ECS compte `guarddutyActivate` Amazon et d'effectuer des opérations de liste et de description sur les ECS clusters Amazon.	26 novembre 2023

Modification	Description	Date
AmazonGuardDutyReadOnlyAccess – Mise à jour d'une politique existante	GuardDuty a ajouté une nouvelle politique pour `organizations` to`ListAccounts` .	16 novembre 2023
AmazonGuardDutyFullAccess – Mise à jour d'une politique existante	GuardDuty a ajouté une nouvelle politique pour `organizations` to`ListAccounts` .	16 novembre 2023
AmazonGuardDutyServiceRolePolicy – Mise à jour d'une politique existante	GuardDuty a ajouté de nouvelles autorisations pour prendre en charge la prochaine fonctionnalité de surveillance du temps GuardDuty EKS d'exécution.	8 mars 2023

Modification	Description	Date
AmazonGuardDutyServiceRolePolicy – Mise à jour d’une politique existante	GuardDuty a ajouté de nouvelles autorisations permettant de GuardDuty créer un rôle lié au service pour Malware Protection for. EC2 Cela permettra de GuardDuty rationaliser le processus d'activation de la protection contre les programmes malveillants pourEC2. GuardDuty peut désormais effectuer l'IAMaction suivante : `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21 février 2023
AmazonGuardDutyFullAccess – Mise à jour d’une politique existante	GuardDuty mis à jour ARN `iam:GetRole` pour*`AWSServiceRoleForAmazonGuardDutyMalwareProtection` .	26 juillet 2022

Modification	Description	Date
AmazonGuardDutyFullAccess – Mise à jour d’une politique existante	GuardDuty a ajouté un nouveau rôle `AWSServiceName` pour autoriser la création d'un rôle lié à un service à l'aide `iam:CreateServiceLinkedRole` de GuardDuty Malware Protection for EC2 Service. GuardDuty peut désormais effectuer l'`iam:GetRole` action pour obtenir des informations pour`AWSServiceRole` .	26 juillet 2022

Modification	Description	Date
AmazonGuardDutyServiceRolePolicy – Mise à jour d’une politique existante	GuardDuty a ajouté de nouvelles autorisations permettant GuardDuty d'utiliser les actions EC2 réseau d'Amazon pour améliorer les résultats. GuardDuty peut désormais effectuer les EC2 actions suivantes pour obtenir des informations sur la façon dont vos EC2 instances communiquent. Ces informations permettent d'améliorer la précision des résultats. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3 août 2021
GuardDuty a commencé à suivre les modifications	GuardDuty a commencé à suivre les modifications apportées AWS à ses politiques gérées.	3 août 2021

Résolution des problèmes liés à GuardDuty l'identité et à l'accès à Amazon

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec GuardDuty etIAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans GuardDuty

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`IAMutilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `guardduty:`*`GetWidget`* autorisations fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `guardduty:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à exécuter iam :PassRole.

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle GuardDuty.

Certains vous AWS services permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans GuardDuty. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je veux permettre à des personnes extérieures Compte AWS à moi d'accéder à mes GuardDuty ressources.

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises GuardDuty en charge, consultezComment Amazon GuardDuty travaille avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Validation de conformité pour Amazon GuardDuty

Pour savoir si un programme AWS services de conformité AWS service s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez AWS services la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation AWS services est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne AWS services sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation AWS services et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.

- AWS Security Hub— Cela AWS service fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela AWS service détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous AWS service permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Amazon GuardDuty

L'infrastructure mondiale d'AWS repose sur les régions et les zones de disponibilité AWS. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les régions AWS et les zones de disponibilité, veuillez consulter Infrastructure mondiale AWS.

Sécurité de l'infrastructure sur Amazon GuardDuty

En tant que service géré, Amazon GuardDuty est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez API les appels AWS publiés pour accéder GuardDuty via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d’identification de sécurité temporaires et signer les demandes.

Intégrer AWS les services avec GuardDuty

GuardDuty peut être intégré à d'autres services AWS de sécurité. Ces services peuvent ingérer des données pour vous GuardDuty permettre de visualiser les résultats de nouvelles manières. Consultez les options d'intégration suivantes pour en savoir plus sur la façon dont ce service est configuré pour fonctionner avec GuardDuty.

Intégration GuardDuty avec AWS Security Hub

AWS Security Hub collecte des données de sécurité provenant de vos AWS comptes, de vos services et des produits partenaires tiers pris en charge afin d'évaluer l'état de sécurité de votre environnement conformément aux normes du secteur et aux meilleures pratiques. Outre l'évaluation de votre niveau de sécurité, Security Hub crée un emplacement central pour les résultats de tous vos AWS services intégrés et de vos produits AWS partenaires. L'activation de Security Hub GuardDuty permettra automatiquement à Security Hub d'ingérer les données de GuardDuty résultats.

Pour plus d'informations sur l'utilisation de Security Hub avec, GuardDuty voirIntégration avec AWS Security Hub.

Intégration GuardDuty à Amazon Detective

Amazon Detective utilise les données de journal de tous vos AWS comptes pour créer des visualisations de données pour vos ressources et adresses IP qui interagissent avec votre environnement. Les visualisations de Detective vous aident à enquêter rapidement et facilement sur les problèmes de sécurité. Vous pouvez passer de la GuardDuty recherche de détails à la recherche d'informations dans la console Detective une fois que les deux services sont activés.

Pour plus d'informations sur l'utilisation de Detective avec, GuardDuty voirIntégration à Amazon Detective.

Intégration avec AWS Security Hub

AWS Security Hub fournit une vue complète de votre état de sécurité dans 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 provenant de AWS comptes, de services et de produits partenaires tiers pris en charge et vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires.

L' GuardDuty intégration d'Amazon à Security Hub vous permet d' GuardDuty envoyer des résultats depuis Security Hub. Security Hub peut ensuite inclure ces résultats dans son analyse de votre posture de sécurité.

Table des matières

Comment Amazon GuardDuty envoie ses résultats à AWS Security Hub

Dans AWS Security Hub, les problèmes de sécurité sont suivis sous forme de découvertes. Certains résultats proviennent de problèmes détectés par d'autres AWS services ou par des partenaires tiers. Security Hub utilise également un ensemble de règles pour détecter les problèmes de sécurité et générer des résultats.

Security Hub fournit des outils permettant de gérer les résultats provenant de toutes ces sources. Vous pouvez afficher et filtrer les listes de résultats et afficher les informations sur un résultat. Pour de plus amples informations, consultez la section Viewing findings (Affichage des résultats) dans le Guide de l'utilisateur AWS Security Hub . Vous pouvez également suivre le statut d'une analyse dans un résultat. Pour de plus amples informations, veuillez consulter Prendre des mesure en fonction des résultats dans le Guide de l'utilisateur AWS Security Hub .

Tous les résultats de Security Hub utilisent un JSON format standard appelé AWS Security Finding Format (ASFF). ASFFCela inclut des détails sur la source du problème, les ressources concernées et l'état actuel de la découverte. Voir Format AWS de recherche de sécurité (ASFF) dans le guide de AWS Security Hub l'utilisateur.

Amazon GuardDuty est l'un des AWS services qui envoie les résultats à Security Hub.

Types de résultats GuardDuty envoyés à Security Hub

Une fois que vous avez activé GuardDuty Security Hub dans le même compte Région AWS, vous commencez GuardDuty à envoyer tous les résultats générés à Security Hub. Ces résultats sont envoyés à Security Hub à l'aide du format AWS Security Finding (ASFF). DansASFF, le `Types` champ indique le type de recherche.

Latence pour l'envoi de nouvelles découvertes

Lors GuardDuty de la création d'un nouveau résultat, il est généralement envoyé à Security Hub dans les cinq minutes.

Réessayer lorsque Security Hub n'est pas disponible

Si Security Hub n'est pas disponible, GuardDuty réessaie d'envoyer les résultats jusqu'à ce qu'ils soient reçus.

Mise à jour des résultats existants dans Security Hub

Après avoir envoyé un résultat à Security Hub, il GuardDuty envoie des mises à jour pour refléter les observations supplémentaires concernant l'activité de recherche à Security Hub. Les nouvelles observations relatives à ces résultats sont envoyées à Security Hub en fonction des Étape 5 — Fréquence d'exportation des résultats paramètres de votre Compte AWS.

Lorsque vous archivez ou désarchivez un résultat, GuardDuty il ne l'envoie pas à Security Hub. Toute découverte désarchivée manuellement qui devient ensuite active dans n' GuardDuty est pas envoyée à Security Hub.

Afficher GuardDuty les résultats dans AWS Security Hub

Pour consulter vos GuardDuty résultats dans Security Hub, sélectionnez Voir les résultats sous Amazon sur la page GuardDuty de résumé. Vous pouvez également sélectionner Résultats dans le panneau de navigation et filtrer les résultats pour n'afficher que GuardDuty les résultats en sélectionnant le champ Nom du produit : avec une valeur de`GuardDuty`.

Interprétation GuardDuty de la recherche de noms dans AWS Security Hub

GuardDuty envoie les résultats à Security Hub en utilisant le format AWS Security Finding Format (ASFF). DansASFF, le `Types` champ indique le type de recherche. ASFFles types utilisent un schéma de dénomination différent de celui des GuardDuty types. Le tableau ci-dessous détaille tous

les types de GuardDuty recherche ainsi que leurs ASFF équivalents tels qu'ils apparaissent dans Security Hub.

> **Note**
>
> Pour certains types de GuardDuty recherche, Security Hub attribue des noms de ASFF recherche différents selon que le rôle de ressource du détail de la recherche était ACTORou TARGET. Pour plus d'informations, voir Détails d'un résultat.

GuardDuty type de recherche	ASFFtype de recherche
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual

GuardDuty type de recherche	ASFFtype de recherche
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin

GuardDuty type de recherche	ASFFtype de recherche
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity

GuardDuty type de recherche	ASFFtype de recherche
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
Découverte :IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked

GuardDuty type de recherche	ASFFtype de recherche
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed

GuardDuty type de recherche	ASFFtype de recherche
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile

GuardDuty type de recherche	ASFFtype de recherche
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior

GuardDuty type de recherche	ASFFtype de recherche
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Répercussions :IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete

GuardDuty type de recherche	ASFFtype de recherche
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistance :IAMUser/AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions

GuardDuty type de recherche	ASFFtype de recherche
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions

GuardDuty type de recherche	ASFFtype de recherche
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller

GuardDuty type de recherche	ASFFtype de recherche
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B

GuardDuty type de recherche	ASFFtype de recherche
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint

GuardDuty type de recherche	ASFFtype de recherche
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS

GuardDuty type de recherche	ASFFtype de recherche
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Résultats types de GuardDuty

GuardDuty envoie les résultats à Security Hub à l'aide du format AWS Security Finding (ASFF).

Voici un exemple de résultat typique tiré de GuardDuty.

```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
```

```
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
```

```
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


Activation et configuration de l'intégration

Pour utiliser l'intégration avec AWS Security Hub, vous devez activer Security Hub. Pour plus d'informations sur la façon d'activer Security Hub, veuillez consulter Configuration de Security Hub dans le Guide de l'utilisateur AWS Security Hub .

Lorsque vous activez à la fois Security Hub GuardDuty et Security Hub, l'intégration est automatiquement activée. GuardDutycommence immédiatement à envoyer les résultats à Security Hub.

Utilisation GuardDuty des commandes dans Security Hub

AWS Security Hub utilise des contrôles de sécurité pour évaluer vos AWS ressources et vérifier votre conformité par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Vous pouvez utiliser les contrôles relatifs aux GuardDuty ressources et aux plans de protection sélectionnés. Pour plus d'informations, consultez Amazon GuardDuty Controls dans le guide de AWS Security Hub l'utilisateur.

Pour obtenir la liste de tous les contrôles relatifs AWS aux services et aux ressources, consultez la référence aux contrôles Security Hub dans le guide de AWS Security Hub l'utilisateur.

Arrêt de la publication des résultats sur Security Hub

Pour arrêter d'envoyer des résultats à Security Hub, vous pouvez utiliser la console Security Hub ou leAPI.

Consultez la section Désactivation et activation du flux de résultats d'une intégration (console) ou Désactivation du flux de résultats d'une intégration (Security Hub API AWS CLI) dans le guide de l'AWS Security Hub utilisateur.

Intégration à Amazon Detective

Amazon Detective vous aide à analyser et à enquêter rapidement sur les événements de sécurité liés à un ou plusieurs AWS comptes en générant des visualisations de données représentant le comportement et l'interaction de vos ressources au fil du temps. Detective crée des visualisations des GuardDuty résultats.

Detective ingère les détails des résultats pour tous les types de résultat et donne accès aux profils des entités afin d'enquêter sur les différentes entités impliquées dans le résultat. Une entité peut être une Compte AWS, une AWS ressource au sein d'un compte ou une adresse IP externe qui a interagi avec vos ressources. La GuardDuty console permet de basculer vers Amazon Detective à partir des entités suivantes, en fonction du type de recherche : IAM rôle Compte AWS, utilisateur ou session de rôle, agent utilisateur, utilisateur fédéré, EC2 instance Amazon ou adresse IP.

Table des matières

Activation de l'intégration

Pour utiliser Amazon Detective avec, GuardDuty vous devez d'abord activer Amazon Detective. Pour plus d'informations sur l'activation de Detective, veuillez consulter Configuration d'Amazon Detective dans le Guide d'administration Amazon Detective.

Lorsque vous activez à la fois Detective GuardDuty et Detective, l'intégration est automatiquement activée. Une fois activé, Detective ingère immédiatement les données de vos GuardDuty découvertes.

> **Note**
>
> GuardDuty envoie les résultats à Detective en fonction de la fréquence d'exportation des GuardDuty résultats. Par défaut, la fréquence d'exportation pour les mises à jour des résultats existants est de 6 heures. Pour que Detective reçoive les dernières mises à jour de vos résultats, il est recommandé de modifier la fréquence d'exportation à 15 minutes dans chaque région avec laquelle vous utilisez Detective GuardDuty. Pour plus d'informations, voir Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour.

Passer à Amazon Detective à partir d'une découverte GuardDuty

1. Connectez-vous à la https://console.aws.amazon.com/guardduty/console.
2. Choisissez un seul résultat dans votre tableau des résultats.
3. Choisissez Enquêter avec Detective dans le volet des informations du résultat.
4. Choisissez un aspect du résultat à examiner avec Amazon Detective. Cela permet d'ouvrir la console Detective pour ce résultat ou cette entité.

Si le basculement ne se comporte pas comme prévu, veuillez consulter Résolution des problèmes liés au pivot dans le Guide de l'utilisateur Amazon Detective.

> **Note**
>
> Si vous archivez une GuardDuty découverte dans la console Detective, elle est également archivée dans la GuardDuty console.

Utilisation de l'intégration avec un environnement GuardDuty multi-comptes

Si vous gérez un environnement multi-comptes dans GuardDuty, vous devez ajouter vos comptes de membre à Amazon Detective afin de voir les visualisations des données Detective relatives aux résultats et aux entités de ces comptes.

Il est recommandé d'utiliser le même compte GuardDuty administrateur que le compte administrateur pour Detective. Pour plus d'informations sur l'ajout de comptes membres dans Detective, veuillez consulter Invitation de comptes membres (langue française non garantie).

> **Note**
>
> Detective est un service régional, ce qui signifie que vous devez l'activer Detective et ajouter vos comptes membres dans chaque région dans laquelle vous souhaitez utiliser l'intégration.

Suspension ou désactivation GuardDuty

Vous pouvez utiliser la GuardDuty console pour suspendre ou désactiver le GuardDuty service. L'utilisation ne vous est pas facturée GuardDuty lorsque le service est suspendu.

- Tous les comptes des membres doivent être dissociés ou supprimés pour que vous puissiez les suspendre ou les désactiver GuardDuty.
- Si vous suspendez GuardDuty, il ne surveille plus la sécurité de votre AWS environnement et ne génère plus de nouvelles découvertes. Vos résultats existants restent intacts et ne sont pas affectés par la GuardDuty suspension. Vous pouvez choisir de le réactiver GuardDuty ultérieurement.
- Lorsque vous le désactivez GuardDuty dans un compte, celui-ci ne sera désactivé que pour le compte actuellement sélectionné Région AWS. Si vous souhaitez le désactiver complètement GuardDuty, vous devez le désactiver dans chaque région où il est activé.
- Si vous le désactivez GuardDuty, vos résultats existants et la GuardDuty configuration sont perdus et ne peuvent pas être restaurés. Si vous souhaitez enregistrer vos résultats existants, vous devez les exporter avant de confirmer la désactivation GuardDuty. Pour plus d'informations sur la procédure d'exportation des résultats, veuillez consulter Exportation des résultats.
- Si vous avez activé la protection contre les programmes malveillants pour S3 pour un ou plusieurs compartiments protégés de votre compte, la suspension ou la désactivation GuardDuty n'a aucune incidence sur le statut d'un compartiment protégé dans le cadre de la protection contre les programmes malveillants pour S3. Même après la suspension ou la désactivation GuardDuty, votre compte continuera de supporter les coûts d'utilisation associés à la fonctionnalité Malware Protection for S3. Pour plus d'informations sur la désactivation de Malware Protection pour S3, consultezDésactiver la protection contre les programmes malveillants pour S3 pour un compartiment protégé.

Pour suspendre ou désactiver GuardDuty

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Dans la GuardDuty section Suspendre, choisissez Suspendre GuardDuty ou Désactiver GuardDuty, puis Confirmez votre action.

À réactiver GuardDuty après la suspension

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Choisissez Réactiver GuardDuty.

Abonnement aux annonces d'Amazon SNS GuardDuty

Cette section fournit des informations sur l'abonnement à Amazon SNS (Simple Notification Service) pour les GuardDuty annonces visant à recevoir des notifications concernant les nouveaux types de résultats, les mises à jour des types de résultats existants et d'autres modifications de fonctionnalités. Les notifications sont disponibles dans tous les formats pris en SNS charge par Amazon.

GuardDuty SNSEnvoie une annonce concernant les mises à jour du GuardDuty service AWS à n'importe quel compte abonné. Pour recevoir des notifications concernant les résultats enregistrés dans votre compte, veuillez consulter Création de réponses personnalisées aux GuardDuty résultats avec Amazon CloudWatch Events.

> **Note**
>
> Votre IAM utilisateur doit être `sns::subscribe` autorisé à s'abonner à unSNS.

Vous pouvez inscrire une SQS file d'attente Amazon à ce sujet de notification, mais vous devez utiliser un sujet ARN qui se trouve dans la même région. Pour plus d'informations, consultez Tutoriel : Abonnement d'une SQS file d'attente Amazon à une SNS rubrique Amazon dans le guide du développeur Amazon Simple Queue Service.

Vous pouvez également utiliser une AWS Lambda fonction pour déclencher des événements lorsque des notifications sont reçues. Pour plus d'informations, consultez Invoking Lambda functions using SNS Amazon Notifications dans le guide du développeur Amazon Simple Queue Service.

La SNS rubrique Amazon ARNs pour chaque région est présentée ci-dessous.

AWS Région	SNSRubrique Amazon ARN
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
`us-east-2`	`arn:aws:sns:us-east-2:118283430703:G`

AWS Région	SNSRubrique Amazon ARN
	uardDutyAnnounceme nts
us-west-1	arn:aws:sns:us-wes t-1:144182107116:G uardDutyAnnounceme nts
us-west-2	arn:aws:sns:us-wes t-2:934957504740:G uardDutyAnnounceme nts
ca-central-1	arn:aws:sns:ca-cen tral-1:10743005193 3:GuardDutyAnnounc ements
ca-west-1	arn:aws:sns:ca-wes t-1:440427180217:G uardDutyAnnounceme nts
eu-north-1	arn:aws:sns:eu-nor th-1:973841112453: GuardDutyAnnouncem ents
eu-west-1	arn:aws:sns:eu-wes t-1:965013871422:G uardDutyAnnounceme nts

AWS Région	SNSRubrique Amazon ARN
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

AWS Région	SNSRubrique Amazon ARN
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

AWS Région	SNSRubrique Amazon ARN
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS Région	SNSRubrique Amazon ARN
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

Pour vous abonner à l'e-mail de notification de GuardDuty mise à jour dans le AWS Management Console

1. Ouvrez la SNS console Amazon sur https://console.aws.amazon.com/sns/v3/home.
2. Dans la liste des régions, choisissez la même région que le sujet ARN auquel vous souhaitez vous abonner. L'exemple utilise la région `us-west-2`.
3. Dans le panneau de navigation de gauche, choisissez Abonnements, puis Créer un abonnement.
4. Dans la boîte de dialogue Créer un abonnement, pour Sujet ARN, collez le sujet ARN :`arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Pour Protocole, choisissez E-mail. Pour Point de terminaison, tapez une adresse e-mail que vous pouvez utiliser pour recevoir la notification.
6. Choisissez Create subscription (Créer un abonnement).
7. Dans votre application de messagerie, ouvrez le message provenant AWS des notifications et ouvrez le lien pour confirmer votre abonnement.

   Votre navigateur Web affiche une réponse de confirmation d'AmazonSNS.

Pour vous abonner à l'e-mail de notification de GuardDuty mise à jour avec AWS CLI

1. Exécutez la commande suivante avec l' AWS CLI :

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Dans votre application de messagerie, ouvrez le message provenant AWS des notifications et ouvrez le lien pour confirmer votre abonnement.

   Votre navigateur Web affiche une réponse de confirmation d'AmazonSNS.

Format de SNS message Amazon

Exemple de message de notification GuardDuty général :

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"GENERAL\",\"message\":[{\"title
\":\"Updated AmazonGuardDutyFullAccess policy\",\"body\":\"Added permission that
 allows you to pass an IAM role to GuardDuty when you enable Malware Protection for
 S3.\",\"links\":[\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess\"]}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :

```
{
        "version": "1",
        "type": "GENERAL",
        "message": [
            {
                "title": "Updated AmazonGuardDutyFullAccess policy",
                "body": "Added permission that allows you to pass an IAM role to
 GuardDuty when you enable Malware Protection for S3.",
                "links": [
                    "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess"
                ]
             }
        ]
}
```

Un exemple de message de notification de GuardDuty mise à jour concernant de nouvelles découvertes est présenté ci-dessous :

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
```

```
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

Un exemple de message de notification de GuardDuty mise à jour concernant GuardDuty les mises à jour des fonctionnalités est illustré ci-dessous :

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_controlplane\"}]}",
```

```
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```


La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :


```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
    }]
}
```


Un exemple de message de notification de GuardDuty mise à jour concernant les résultats mis à jour est illustré ci-dessous :


```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
```

```
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```


La valeur Message analysée (après suppression des guillemets simples placés en séquence d'échappement) est présentée ci-dessous :


```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

GuardDuty Quotas Amazon

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux AWS service. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, tandis que d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas pour GuardDuty, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez AWS serviceset sélectionnez Amazon GuardDuty.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Vous Compte AWS disposez des quotas suivants pour Amazon GuardDuty par région.

> **Note**
>
> - Pour les quotas spécifiques à GuardDuty Malware Protection for EC2, consultezProtection contre les malwares pour les EC2 quotas.
> - Pour les quotas spécifiques à Malware Protection for S3, consultezQuotas dans la protection contre les malwares pour S3.

GuardDuty quotas par région

Ressource	Par défaut	Commentaires
Détecteurs	1	Nombre maximal de ressources de détecteur que vous pouvez créer par compte AWS et par région. Vous ne pouvez pas demander d'augment ation de quota.

Ressource	Par défaut	Commentaires
Filtres	100	Le nombre maximum de filtres enregistrés par AWS compte et par région. Vous ne pouvez pas demander d'augmentation de quota.
Recherche de la période de conservation	90 jours	Nombre maximal de jours pendant lesquels une découverte est conservée. Vous ne pouvez pas demander d'augmentation de quota.
Adresses IP et plages CIDR par liste d'adresses IP approuvées	2 000	Nombre maximal d'adresses IP et de plages CIDR que vous pouvez inclure dans une seule liste d'adresses IP approuvées. Vous ne pouvez pas demander d'augmentation de quota.

Ressource	Par défaut	Commentaires
Adresses IP et plages CIDR par liste de menaces	250 000	Nombre maximal d'adresses IP et de plages CIDR que vous pouvez inclure dans une liste de menaces. Vous ne pouvez pas demander d'augmentation de quota.
Taille maximale du fichier	35 MO	Taille maximale du fichier utilisé pour charger une liste d'adresses IP ou de plages CIDR à inclure dans une liste d'adresses IP approuvées ou une liste de menaces. Vous ne pouvez pas demander d'augmentation de quota.
Comptes membres (sur invitation) : 1 000	5000	Le nombre maximum de comptes de membres associés à un compte d'administrateur. Vous ne pouvez pas demander d'augmentation de quota.

Ressource	Par défaut	Commentaires
Comptes membres	50 000	Le nombre maximum de comptes de membres associés à un compte administrateur via AWS Organizations. Cela inclut les comptes membres ajoutés à l'organisation sur invitation. Cette valeur par défaut dépend de votre quota actuel de comptes membres dans AWS Organizations. Le nombre de comptes membres ajoutés GuardDuty ne AWS Organizations peut pas dépasser le nombre de comptes membres de votre organisation. Pour plus d'informations sur le nombre de Comptes AWS dans une organisation, voir Valeurs maximales et minimales dans le Guide de AWS Organizations l'utilisateur.

Ressource	Par défaut	Commentaires
Ensembles d'intelligence de menaces	6	Nombre maximal d'ensembles Intel Threat que vous pouvez ajouter par compte AWS et par région. Vous ne pouvez pas demander d'augment ation de quota.
Ensembles d'adresses IP approuvés	1	Le nombre maximum d'ensembles d'adresses IP fiables qui peuvent être téléchargés et activés par AWS compte et par région. Vous ne pouvez pas demander d'augment ation de quota.

Résolution des problèmes liés à Amazon GuardDuty

Lorsque vous rencontrez des problèmes liés à l'exécution d'une action spécifique à GuardDuty, consultez les rubriques de cette section.

Rubriques

Problèmes généraux relatifs à GuardDuty

Je reçois une erreur d'accès lors de l'exportation GuardDuty des résultats. Comment puis-je résoudre ce problème ?

Après avoir configuré les paramètres pour exporter les résultats, s'il n' GuardDuty est pas possible d'exporter les résultats, un message d'erreur s'affiche sur la page Paramètres de la GuardDuty console. Cela peut se produire lorsque vous ne GuardDuty pouvez plus accéder à la ressource cible, par exemple si votre compartiment Amazon S3 a été supprimé ou si l'autorisation d'accès au compartiment a été modifiée. Cela peut également se produire lorsque GuardDuty vous ne pouvez plus accéder à la AWS KMS clé utilisée pour chiffrer les données de votre compartiment Amazon S3. Lorsqu' GuardDuty il ne peut pas exporter, il envoie une notification à l'adresse e-mail associée au compte pour fournir des informations sur ce problème.

Pour résoudre le problème, assurez-vous que les ressources correspondantes existent et GuardDuty que vous disposez des autorisations nécessaires pour accéder aux ressources nécessaires. Si vous ne résolvez pas le problème avant la fin de la période de conservation des résultats de 90 jours GuardDuty, vos résultats ne seront pas exportés. GuardDuty désactivera la recherche des paramètres d'exportation pour ce compte dans la région spécifique. Même au-delà de cette date de conservation, vous pouvez mettre à jour les paramètres de configuration pour recommencer à exporter les résultats dans la région spécifique.

Pour plus d’informations, consultez Exportation des résultats.

Protection contre les programmes malveillants pour les problèmes liés à EC2

Je lance une analyse des logiciels malveillants à la demande, mais cela entraîne une erreur indiquant l'absence des autorisations requises.

Si vous recevez un message d'erreur indiquant que vous ne disposez pas des autorisations requises pour démarrer une analyse des logiciels malveillants à la demande sur une instance Amazon EC2, vérifiez que vous avez associé la politique AWS politique gérée : AmazonGuardDutyFullAccess à votre rôle IAM.

Si vous êtes membre d'une AWS organisation et que vous recevez toujours le même message d'erreur, connectez-vous à votre compte de gestion. Pour plus d'informations, consultez AWS Organizations SCP— Accès refusé.

Je reçois un **`iam:GetRole`** message d'erreur lors de l'utilisation de Malware Protection for EC2.

Si vous recevez cette erreur`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, cela signifie que vous n'êtes pas autorisé à activer l'analyse des programmes malveillants GuardDuty initiée ou à utiliser l'analyse des programmes malveillants à la demande. Vérifiez que vous avez associé la politique AWS politique gérée : AmazonGuardDutyFullAccess à votre rôle IAM.

Je suis un compte GuardDuty administrateur qui doit activer le scan des programmes malveillants GuardDuty initié mais qui n'utilise pas de politique AWS gérée : AmazonGuardDutyFullAccess pour gérer GuardDuty.

- Configurez le rôle IAM que vous utilisez GuardDuty pour disposer des autorisations requises pour activer l'analyse des programmes malveillants GuardDuty initiée par un scanner. Pour plus d'informations sur les autorisations requises, voir Création d'un rôle lié à un service pour Malware Protection for EC2.
- Attachez le AWS politique gérée : AmazonGuardDutyFullAccess à votre rôle IAM. Cela vous aidera à activer le scan des logiciels malveillants GuardDuty initié pour les comptes des membres.

Problèmes de surveillance du temps d'exécution

Mon AWS Step Functions flux de travail échoue de façon inattendue

Si le GuardDuty conteneur a contribué à l'échec du flux de travail, consultezRésolution des problèmes de couverture. Si le problème persiste, pour éviter l'échec du flux de travail dû au GuardDuty conteneur, effectuez l'une des étapes suivantes :

- Ajoutez le `false` tag `GuardDutyManaged` : au cluster Amazon ECS associé.
- Désactivez la configuration automatique de l'agent pour AWS Fargate (ECS uniquement) au niveau du compte. Ajoutez la balise d'inclusion `GuardDutyManaged` : `true` au cluster Amazon ECS associé que vous souhaitez continuer à surveiller avec l'agent GuardDuty automatisé.

Résolution des erreurs liées au manque de mémoire dans Runtime Monitoring (support Amazon EC2 uniquement)

Cette section décrit les étapes de dépannage lorsque vous rencontrez une erreur de mémoire insuffisante suite CPUet limite de mémoire au déploiement manuel de l'agent GuardDuty de sécurité.

Si l' GuardDuty agent `systemd` est arrêté à cause du `out-of-memory` problème et que vous estimez qu'il est raisonnable de fournir plus de mémoire à l' GuardDuty agent, vous pouvez mettre à jour la limite.

1. Ouvrez avec l'autorisation root`/lib/systemd/system/amazon-guardduty-agent.service`.
2. Recherchez `MemoryLimit` et `MemoryMax` mettez à jour les deux valeurs.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Après avoir mis à jour les valeurs, redémarrez l' GuardDuty agent à l'aide de la commande suivante :

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Exécutez la commande suivante pour afficher l'état :

```
sudo systemctl status amazon-guardduty-agent
```

La sortie attendue indiquera la nouvelle limite de mémoire :

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Gestion des problèmes liés à plusieurs comptes

Je souhaite gérer plusieurs comptes mais je n'ai pas l'autorisation AWS Organizations de gestion requise.

Si vous recevez cette erreur`The request failed because you do not have required AWS Organization master permission.`, cela signifie que vous n'êtes pas autorisé à activer l'analyse des programmes malveillants GuardDuty initiée pour plusieurs comptes de votre organisation. Pour plus d'informations sur l'octroi d'autorisations au compte de gestion, consultezMise en place d'un accès fiable pour permettre une analyse des programmes malveillants GuardDuty initiée par un utilisateur.

Autres problèmes de résolution des problèmes

Si vous ne trouvez pas de scénario adapté à votre problème, veuillez consulter les options de résolution des problèmes suivantes :

- Pour les problèmes généraux liés à IAM lorsque vous accédez à https://console.aws.amazon.com/guardduty/, veuillez consulter Résolution des problèmes liés à GuardDuty l'identité et à l'accès à Amazon.
- Pour les problèmes d'authentification et d'autorisation lors de l'accès AWS AWS Console Home, consultez la section Résolution des problèmes liés à l'IAM.

Régions et points de terminaison

Pour savoir Régions AWS où Amazon GuardDuty est disponible, consultez la section GuardDuty Points de terminaison Amazon dans le Référence générale d'Amazon Web Services.

Nous vous recommandons d'activer toutes les GuardDuty options prises en charge Régions AWS. Cela permet GuardDuty de générer des informations sur des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. Cela permet également GuardDuty de surveiller les AWS CloudTrail événements pour les personnes prises en charge Régions AWS, sa capacité à détecter les activités impliquant des services mondiaux étant réduite.

Disponibilité des fonctionnalités propres à la région

Liste des différences régionales pour préciser la disponibilité des GuardDuty fonctionnalités.

ListFindings et GetFindingsStatistics API

Les ListFindingsAPI GetFindingsStatisticset ont un `consoleOnly` indicateur temporaire. Lorsque vous utilisez l'une de ces API ou les deux, l'`consoleOnly`indicateur signifie que l'API peut récupérer des résultats jusqu'à une limite maximale de 1 000.

GuardDuty fonctionnalités présentant une disparité entre les régions

Protection contre les logiciels malveillants pour EC2

GuardDuty prend en charge la fonctionnalité Malware Protection for EC2 dans les Zones Locales AWS dédiées.

Support général de l'API

Les API suivantes figurant dans le Amazon GuardDuty API Reference peuvent présenter des différences régionales en raison de l'indisponibilité de certaines sources de données ou fonctionnalités spécifiées Régions AWS précédemment :

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors

- DescribeOrganizationConfiguration

Types de résultat Amazon EC2 : DefenseEvasion:EC2/UnusualDoHActivity et DefenseEvasion:EC2/UnusualDoTActivity

Le tableau suivant indique Régions AWS où GuardDuty est disponible, mais ces deux types de recherche Amazon EC2 ne sont pas encore pris en charge.

Région AWS	Code région
Asie-Pacifique (Séoul)	ap-northeast-2
Asie-Pacifique (Osaka)	ap-northeast-3
Asie-Pacifique (Jakarta)	ap-southeast-3

AWS GovCloud (US) Régions

Pour obtenir les dernières informations, consultez Amazon GuardDuty dans le guide de AWS GovCloud (US) l'utilisateur.

Régions de Chine

Pour obtenir les dernières informations, veuillez consulter Disponibilité des fonctionnalités et différences de mise en œuvre (langue française non garantie).

GuardDuty actions et paramètres hérités

Amazon GuardDuty a déconseillé certaines actions et certains paramètres de l'API, mais les prend toujours en charge. Il est recommandé d'utiliser les nouvelles actions et les nouveaux paramètres d'API qui remplacent les options héritées. Le tableau suivant compare les actions et paramètres hérités et nouveaux.

Actions/paramètres hérités	Nouvelles actions/Nouveaux paramètres	Comparison (Comparaison)
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Avec la même implémentation dans les deux actions, GuardDuty utilise le terme `Administrator` in`DisassociateFromAdministratorAccount` .
`autoEnable` paramètre dans DescribeOrganizationConfigurationet UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Le compte GuardDuty administrateur peut ainsi auditer et appliquer l' GuardDuty une ou l'autre des valeurs à tous les comptes membres. `autoEnableOrganizationMembers` À l'aide des API, la mise à jour de la configuration de tous les comptes membres peut prendre jusqu'à 24 heures. Pour plus d'informations sur les valeurs possibles du `autoEnableOrganizationMembers` champ, voir autoEnableOrganizationMembres
Paramètre `dataSources` dans les API répertoriées	`features`	À partir de mars 2023, vous pouvez configurer GuardDuty Protection contre les logiciels malveillants pour EC2 et utiliser les nouveaux plans de GuardDuty protection à

Actions/paramètres hérités	Nouvelles actions/Nouveaux paramètres	Comparison (Comparaison)
dans GuardDuty APImodifications en mars 2023.		l'aide de`features`. Les plans de protection lancés avant mars 2023, y compris Malware Protection for EC2, prennent toujours en charge la configuration à l'aide `dataSources` de. Si vous utilisez des API pour configurer un plan de protection, chaque demande d'API peut inclure `dataSources` ou `features`, mais pas les deux.

Historique du document pour Amazon GuardDuty

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version du guide de GuardDuty l'utilisateur Amazon. Pour être informé des mises à jour de cette documentation, vous pouvez vous abonner à un RSS flux.

Modification	Description	Date
Rôle GuardDuty lié au service mis à jour () SLR	GuardDuty a mis à jour le SLR pour inclure l'`ec2:DescribeVpcs` autorisation dans les EC2 actions Amazon. Pour plus d'informations, consultez la section Autorisations de rôle liées à un service pour. GuardDuty	22 août 2024
Ajout de contenu significatif	GuardDuty a ajouté des mises à jour de contenu importantes à la fonctionnalité Malware Protection for S3. • Ajout de nouveaux exemples de schéma de notification pour configurer les EventBridge règles Amazon afin de recevoir des notifications relatives à l'état des ressources du plan de protection contre les logiciels malveillants et au résultat de l'analyse des objets S3. Pour plus d'informations, consultez la section Surveillance des scans d'objets S3 avec Amazon EventBridge.	20 août 2024

	• Ajout d'informations sur le dépannage des défaillances des balises après le scan des objets S3.	
Fonctionnalités mises à jour dans GuardDuty Runtime Monitoring - Amazon EC2	Runtime Monitoring a publié la version 1.3.0 d'un nouvel agent pour Amazon EC2 Resources. Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour Amazon EC2.	19 août 2024
Fonctionnalités mises à jour dans GuardDuty Runtime Monitoring - Amazon EKS	Runtime Monitoring a publié la version 1.7.0 d'un nouvel agent pour Amazon EKS Resources. Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour les EKS clusters Amazon.	17 août 2024

Ajout de contenu significatif	GuardDuty a ajouté de nouvelles informations sur la méthodologie de détection des programmes malveillants et les moteurs de scan qu'il utilise pour les fonctionnalités de protection contre les logiciels malveillants pour S3 et de protection contre les logiciels malveillants pour les EC2 fonctionnalités. Pour plus d'informations, consultez la section Moteur d'analyse pour la détection des GuardDuty programmes malveillants.	15 août 2024
Nouvelle fonctionnalité - Protection des charges de travail liées à l'IA	GuardDuty la détection des menaces fondamentales et la protection Lambda vous aident à mieux sécuriser et détecter les menaces qui pèsent sur les charges de travail basées sur l'IA. AWS Pour plus d'informations, consultez la section Protection des charges de travail basées sur l'IA avec GuardDuty.	14 août 2024

Fonctionnalité mise à jour dans GuardDuty Runtime Monitoring - Fargate (Amazon uniquement) ECS	Runtime Monitoring a publié une nouvelle version d'agent 1.3.0 pour les ressource s AWS Fargate (Amazon ECS uniquement). Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour Fargate-. ECS	9 août 2024
Fonctionnalité mise à jour - Protection contre les logiciels malveillants pour S3	GuardDuty Malware Protectio n for S3 augmente le quota maximal de compartiments S3 de 10 à 25 compartim ents. Ce quota s'appliqu e à un Compte AWS pour chacun Région AWS. Pour plus d'informations, consultez la section Protection contre les programmes malveillants pour S3.	8 août 2024

Mise à jour - Nouveaux types de recherche dans Runtime Monitoring	GuardDuty a ajouté deux nouveaux types de détection de la surveillance du temps d'exécution qui vous aideront à détecter les menaces impliquant la création d'un shell suspect sur la ressource surveillée et l'augmentation des privilèges lorsqu'un processus élève de manière suspecte ses privilèges au rang de root. • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	6 août 2024
Mis à jour - Intégration avec AWS Security Hub	AWS Security Hub fournit une liste de contrôles de GuardDuty sécurité pour évaluer vos ressources et vérifier votre conformité par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Pour plus d'informations, consultez la section Utilisation GuardDuty des contrôles dans Security Hub.	11 juillet 2024

Script de GuardDuty test mis à jour pour les résultats	GuardDuty prend désormais en charge plus de 100 résultats avec différentes AWS ressources dans un compte dédié. Utilisez le `amazon-guardduty-tester` référentiel et suivez les étapes pour tester les résultats et les examiner afin de comprendre les détails des résultats. Pour plus d'informations, consultez la section GuardDuty Résultats des tests dans des comptes dédiés.	28 juin 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié la version 1.2.0 d'un nouvel agent de sécurité pour la EC2 ressource Amazon. Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour l'EC2instance Amazon. Pour plus d'informations sur la mise à jour manuelle de l'agent de sécurité vers cette version, consultez Gestion manuelle de l'agent de sécurité pour l'EC2instance Amazon.	13 juin 2024

Nouvelle fonctionnalité - Protection contre les programmes malveillants pour la disponibilité dans la région S3	GuardDuty Malware Protection for S3 est désormais disponible dans toutes les régions commerciales où elle GuardDuty est disponible. Cette fonctionnalité vous permet de scanner les objets récemment chargés dans les compartiments Amazon S3 afin de détecter d'éventuels malwares ou chargements suspects, et de prendre des mesures pour les isoler avant qu'ils ne soient ingérés dans les processus en aval. Pour plus d'informations sur l'activation de la protection contre les programmes malveillants pour S3, consultez la section Protection contre les GuardDuty programmes malveillants pour S3.	12 juin 2024

Nouvelle fonctionnalité - Protection contre les logiciels malveillants pour S3	GuardDuty annonce la disponibilité générale de Malware Protection for S3, qui vous aide à analyser les objets récemment chargés dans les compartiments Amazon S3 pour détecter d'éventuels malwares ou chargements suspects, et à prendre des mesures pour les isoler avant qu'ils ne soient ingérés dans les processus en aval. Cette fonctionnalité est entièrement gérée par AWS. GuardDuty publie le résultat de l'analyse des objets S3 sur votre bus d'événements EventBridge par défaut. Vous pouvez GuardDuty autoriser l'ajout de balises à vos objets S3 numérisés. Vous pouvez créer des flux de travail en aval, tels que l'isolation dans un compartiment de quarantaine, ou définir des politiques de compartiment à l'aide de balises qui empêchent les utilisateurs ou les applications d'accéder à certains objets. Pour plus d'informations, consultez la section Protection contre les GuardDuty programmes malveillants pour S3. Il est actuellement disponible dans les régions suivantes :	11 juin 2024

	• USA Est (Virginie du Nord) • USA Est (Ohio) • USA Ouest (Oregon) • Europe (Irlande) • Europe (Francfort) • Europe (Stockholm) • Asie-Pacifique (Sydney) • Asia Pacific (Tokyo) • Asie-Pacifique (Singapour)	
AmazonGuardDutyFullAccessPolitique mise à jour	Autorisation ajoutée qui vous permet de transmettre un IAM rôle GuardDuty lorsque vous activez Malware Protection pour S3. Pour plus d'informations sur cette mise à jour des politiques, consultez la section GuardDuty Mises à jour des politiques AWS gérées.	10 juin 2024

Fonctionnalité mise à jour dans GuardDuty RDS Protection	RDSLa protection étend le support pour surveiller l'activité de connexion sur vos SQL bases RDS de données Postgre. Dans le cadre de cette extension, GuardDuty nous commencer ons automatiquement à surveiller les données de RDS connexion des SQL bases de données Postgre pour les comptes qui ont déjà activé GuardDuty RDS la protectio n. Pour plus d'informations, consultez RDSla section Protection.	6 juin 2024
Fonctionnalité mise à jour dans GuardDuty Runtime Monitoring - Fargate (Amazon uniquement) ECS	Runtime Monitoring a publié une nouvelle version d'agent 1.2.0 pour les ressource s AWS Fargate (Amazon ECS uniquement). Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour Fargate-. ECS	31 mai 2024

Fonctionnalité mise à jour dans GuardDuty Malware Protection pour EC2	Pour chaque EBS volume Amazon attaché à vos EC2 instances Amazon et à vos charges de travail de conteneur, GuardDuty Malware Protection for EC2 a augmenté la taille du EBS volume à analyser jusqu'à 2 048 Go. Pour plus d'informations sur l'analyse EBS des volumes Amazon attachés à vos instances, consultez GuardDuty Malware Protection for EC2.	29 mai 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Surveillance du temps d'exécution pour Amazon ECS -Les ressources Fargate permettent désormais de détecter les menaces potentiel les sur vos tâches lancées par et. AWS Batch AWS CodePipeline Pour plus d'informations, consultez Comment fonctionne la surveillance du temps d'exécution avec Fargate (ECSAmazon uniquement).	28 mai 2024

Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié la version 1.6.1 d'un nouvel agent pour Amazon EKS Resources. Pour plus d'informations sur les notes de mise à jour, consultez l'historique des versions de l'agent EKS complémentaire.	14 mai 2024
Support régional étendu pour la surveillance du temps d'exécution	GuardDuty étend le soutien à la surveillance du temps d'exécution à la région de l'Ouest canadien (Calgary). Pour plus d'informations sur la mise en route de la surveilla nce du temps d'exécution, voir Activation de la surveillance du temps d'exécution.	7 mai 2024
Support régional étendu pour la RDS protection	GuardDuty étend le support de RDS protection aux éléments suivants Régions AWS : • Canada Ouest (Calgary) • Asie-Pacifique (Hyderabad) • Europe (Espagne) • Europe (Zurich) • Moyen-Orient (UAE) • Israël (Tel Aviv) • Asie-Pacifique (Melbourne) Pour plus d'informations sur l'activation de cette fonctionn alité, consultez RDSla section Protection.	3 mai 2024

Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié une nouvelle version d'agent 1.1.0 pour les ressource s AWS Fargate (Amazon ECS uniquement). Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour Fargate-. ECS	1er mai 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié la version 1.6.0 d'un nouvel agent pour les EKS ressource s Amazon. Pour plus d'informa tions sur les notes de mise à jour, consultez l'historique des versions de l'agent EKS complémentaire.	29 avril 2024
Support pour IPAddressv6	GuardDuty a ajouté la IPAddressv6 prise en charge des détails IP locaux et distants. Vous pouvez utiliser les attributs de filtre associés pour filtrer GuardDuty les résultats ou créer des règles de suppression.	18 avril 2024
Expérience de console mise à jour pour configurer l'exporta tion des résultats	GuardDuty a mis à jour l'expérience de la console pour exporter les résultats générés dans votre Comptes AWS compartiment Amazon S3. Pour plus d'informations, consultez la section Exportati on GuardDuty des résultats.	1er avril 2024

Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié la version 1.1.0 d'un nouvel agent de sécurité pour la EC2 ressource Amazon. Cette version prend en charge la configuration GuardDuty automatique des agents dans Runtime Monitoring pour les EC2 instances Amazon. Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour l'EC2instance Amazon.	28 mars 2024

Disponibilité générale de la surveillance du temps d'exécution pour les EC2 instances Amazon	GuardDuty annonce la disponibilité générale (GA) de Runtime Monitoring pour les EC2 instances Amazon. Vous avez désormais la possibilité d'activer la configuration automatique de l'agent qui permet GuardDuty d'installer et de gérer l'agent de sécurité pour vos EC2 instances Amazon en votre nom. Avec l'agent GuardDuty automatisé, vous pouvez également utiliser des balises d'inclusion ou d'exclusion GuardDuty pour indiquer d'installer et de gérer l'agent de sécurité sur certaines EC2 instances Amazon uniquement. Pour plus d'informations, consultez Comment fonctionne la surveillance du temps d'exécution avec EC2 les instances Amazon. Liste des nouveaux types de trouvailles publiés en même temps que cette AG • Exécution : Runtime/SuspiciousTool • Exécution : Runtime/SuspiciousCommand • DefenseEvasion:Temps d'exécution/ SuspiciousCommand	28 mars 2024

- DefenseEvasion:Temps d'exécution/ PtraceAntiDebugging
- Exécution : Runtime/ MaliciousFileExecuted

Amazon GuardDuty a mis à jour le rôle lié au service () SLR	Utilisez AWS Systems Manager des actions pour gérer les SSM associati ons sur les EC2 instances Amazon lorsque vous activez la surveillance du temps GuardDuty d'exécution avec un agent automatisé pour AmazonEC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les EC2 instances dotées d'une balise d'inclusion (`GuardDuty Managed :true`). • La liste suivante indique les nouvelles autorisations : `"ssm:DescribeAssoc iation", "ssm:DeleteAssocia tion", "ssm:UpdateAssociati on", "ssm:CreateAs sociation", "ssm:StartAssoc iationsOnce", "ssm:AddTagsT oResource", "ssm:CreateAsso ciation", "ssm:UpdateAssoci ation", "ssm:SendCommand", "ssm:GetCommandInv ocation"`	26 mars 2024

Fonctionnalité mise à jour dans Runtime Monitoring	Avec la dernière version v1.5.0 de l'agent de GuardDuty sécurité (module complémentaire) pour AmazonEKS, Runtime Monitoring prend désormais en charge la configuration de paramètres spécifiques de votre agent de GuardDuty sécurité, tels que CPU les paramètres de mémoire, `PriorityClass` les paramètres et les paramètres de DNS politique. Pour plus d'informations, consultez la section Configuration des paramètres GuardDuty de l'agent de sécurité (EKSmodule complémentaire).	7 mars 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié une nouvelle version d'agent 1.5.0 pour Amazon EKS Resources. Pour plus d'informations sur les notes de mise à jour, consultez l'historique des versions de l'agent EKS complémentaire.	7 mars 2024

Support pour le Canada-Ouest (Calgary)	Amazon GuardDuty est désormais disponible dans la région du Canada Ouest (Calgary). Certains des plans de protection proposés GuardDuty peuvent ne pas être disponibles dans cette région. Pour obtenir les informations les plus récentes, consultez la section Régions et points de terminaison.	6 mars 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Les versions 1.0.0 et 1.1.0 de l'agent de GuardDuty sécurité pour les EKS clusters Amazon ne seront plus prises en charge à compter du 14 mai 2024. Pour plus d'informations sur les mesures que vous pouvez prendre avant la fin du support standard, consultez l'agent GuardDuty de sécurité pour les EKS clusters Amazon.	16 février 2024

Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring prend en charge la dernière version 1.29 de Kubernetes avec la version 1.4.1 de l'agent de sécurité existant. Le support est disponible depuis le lancement de cette version de Kubernetes. Pour plus d'informations sur les versions de Kubernetes prises en charge, voir Versions de Kubernetes prises en charge par l'agent de sécurité. GuardDuty	16 février 2024

Fonctionnalité mise à jour dans Runtime Monitoring - Disponibilité régionale	GuardDuty Runtime Monitoring prend désormais en charge le partage d'Amazon VPC au sein de celui-ci AWS Organizations. GuardDuty service-linked role (SLR) dispose d'une nouvelle autorisation, `organizations:DescribeOrganization` qui permet de récupérer l'identifiant de l'organisation pour le VPC compte Amazon partagé afin de définir la politique du point de terminaison. Pour plus d'informations sur les conditions préalables à l'utilisation d'un point de VPC terminaison Amazon partagé dans Runtime Monitoring, consultez Support for shared Amazon VPC. Cette fonctionnalité est disponible dans toutes les régions où la surveillance du temps d'exécution est prise GuardDuty en charge.	12 février 2024

Fonctionnalité mise à jour dans Runtime Monitoring - Disponibilité régionale	GuardDuty Runtime Monitoring prend désormais en charge le partage d'Amazon VPC au sein de celui-ci AWS Organizations. GuardDuty service-linked role (SLR) dispose d'une nouvelle autorisation, `organizations:DescribeOrganization` qui permet de récupérer l'identifiant de l'organisation pour le VPC compte Amazon partagé afin de définir la politique du point de terminaison. Pour plus d'informations sur les conditions préalables à l'utilisation d'un point de VPC terminaison Amazon partagé dans Runtime Monitoring, consultez Support for shared Amazon VPC. Actuellement, cette fonctionnalité est disponible dans certains des Régions AWS. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.	9 février 2024
Fonctionnalité mise à jour avec prise en charge de nouvelles fonctionnalités Régions AWS : Malware Protection pour EC2	Malware Protection prend EC2 actuellement en charge l'analyse EBS des volumes chiffrés Clés gérées par AWS dans la région ouest des États-Unis (Oregon).	6 février 2024

Fonctionnalité mise à jour avec prise en charge de nouvelles fonctionnalités Régions AWS : Malware Protection pour EC2	Pour l'EC2instant, Malware Protection prend en charge l'analyse EBS des volumes Clés gérées par AWS chiffrés avec les méthodes suivantes Régions AWS : • Asie-Pacifique (Singapour) (`ap-southeast-1`) • Europe (Francfort) (`eu-central-1`) • Asie-Pacifique(Osaka) (`ap-northeast-3`) • USA Est (Ohio) (`us-east-2`) • Europe (Milan) (`eu-south-1`) • Asie-Pacifique (Tokyo) (`ap-northeast-1`) • Asie-Pacifique (Séoul) (`ap-northeast-2`) • Canada (Centre) (`ca-central-1`) • Europe (Irlande) (`eu-west-1`) • USA Est (Virginie du Nord) (`us-east-1`)	5 février 2024

Fonctionnalité mise à jour dans Runtime Monitoring	GuardDuty Runtime Monitoring a publié une nouvelle version GuardDuty de l'agent de sécurité (v1.0.2) pour les EC2 instances Amazon. Cette version de l'agent inclut le support de la dernière version d'Amazon ECSAMIs. Pour plus d'informations sur l'historique des versions de l'agent, consultez GuardDuty Security Agent for Amazon EC2 instances.	2 février 2024

Fonctionnalité mise à jour avec prise en charge de nouvelles fonctionnalités Régions AWS : Malware Protection pour EC2	Pour l'EC2instant, Malware Protection prend en charge l'analyse EBS des volumes Amazon Clés gérées par AWS chiffrés avec les méthodes suivantes Régions AWS : • Europe (Londres) (`eu-west-2`) • Europe (Stockholm) (`eu-north-1`) • Asie-Pacifique (Hong Kong) (`ap-east-1`) • Afrique (Le Cap) (`af-south-1`) • Moyen-Orient (Bahreïn) (`me-south-1`) • Asie-Pacifique (Hyderabad) (`ap-south-2`) • Europe (Espagne) (`eu-south-2`) • Asie-Pacifique (Melbourne) (`ap-southeast-4`) • Asie-Pacifique (Sydney) (`ap-southeast-2`) • Israël (Tel Aviv) (`il-central-1`)	31 janvier 2024

Mise à jour de la gestion des comptes avec AWS Organizations	Réorganisation du contenu sous Gestion des comptes avec AWS Organizations. , a ajouté des étapes pour modifier le compte d' GuardDuty administrateur délégué et a mis à jour Comprendre la relation entre le compte d' GuardDuty administrateur et les comptes de membre.	30 janvier 2024
Fonctionnalité mise à jour avec prise en charge de nouvelles Régions AWS	Pour l'EC2instant, Malware Protection prend en charge l'analyse EBS des volumes Clés gérées par AWS chiffrés avec les méthodes suivantes Régions AWS : • Asie-Pacifique (Jakarta) (`ap-southeast-3`) • USA Ouest (Californie du Nord) (`us-west-1`) • Moyen-Orient (UAE) (`me-central-1`) • Europe (Zurich) (`eu-central-2`) • Asie-Pacifique (Mumbai) (`ap-south-1`) • Amérique du Sud (Sao Paulo) (`sa-east-1`)	29 janvier 2024

Fonctionnalité mise à jour dans Malware Protection pour EC2	Malware Protection prend EC2 actuellement en charge l'analyse des EBS volumes chiffrés à l'aide de Clés gérées par AWS. Malware Protection for EC2 Service Linked Role (SLR) dispose de deux nouvelles autorisations : `GetSnapshotBlock` et. `ListSnapshotBlocks` Ces autorisations vous aideront à GuardDuty récupérer l'instantané d'un EBS volume (chiffré à l'aide de Clé gérée par AWS) depuis votre compte de service Compte AWS et à le copier sur le compte de GuardDuty service avant de lancer l'analyse des logiciels malveillants. Actuellement, cette fonctionnalité n'est disponible qu'en Europe (Pariseu-west-3) (). Pour plus d'informations, consultez la section Volumes pris en charge pour l'analyse des programmes malveillants.	25 janvier 2024

Fonctionnalité mise à jour dans Runtime Monitoring	GuardDuty Runtime Monitoring a publié une nouvelle version GuardDuty de l'agent de sécurité (v1.0.1) avec des optimisations et des améliorations générales des performances. Pour plus d'informations sur l'historique des versions de l'agent, consultez GuardDuty Security Agent for Amazon EC2 instances.	23 janvier 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié la version 1.4.1 d'un nouvel agent pour Amazon EKS Resources. Pour plus d'informations, consultez l'historique des versions de l'agent EKS complémentaire.	16 janvier 2024
Runtime Monitoring a publié un nouvel agent v1.4.0 pour Amazon Resources EKS	Runtime Monitoring a publié une nouvelle version d'agent 1.4.0 pour les EKS ressources Amazon. Pour plus d'informations, consultez l'historique des versions de l'agent EKS complémentaire.	21 décembre 2023

Ajout de types de résultats basés sur le S3 et l'apprentissage AWS CloudTrail automatique (ML) en Europe (Zurich), en Europe (Espagne), en Asie-Pacifique (Hyderabad), en Asie-Pacifique (Melbourne) et en Israël (Tel Aviv)	Le S3 et les CloudTrail résultats suivants qui identifient le comportement anormal à l'aide GuardDuty du modèle d'apprentissage automatique (ML) de détection des anomalies sont désormais disponibles dans les régions d'Europe (Zurich), d'Europe (Espagne), d'Asie-Pacifique (Hyderabad), d'Asie-Pacifique (Melbourne) et d'Israël (Tel Aviv) : • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior	21 décembre 2023

	• Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty prend en charge 50 000 comptes membres via AWS Organizations	Un GuardDuty administrateur délégué peut désormais gérer un maximum de 50 000 comptes de membres via AWS Organizations. Cela inclut également un maximum de 5 000 comptes membres associés au compte GuardDuty administrateur sur invitation.	20 décembre 2023

GuardDuty Support de surveillance du temps d'exécution étendu à 19 Régions AWS	La surveillance du temps d'exécution est désormais disponible en Asie-Pacifique (Jakarta), Europe (Paris), Asie-Pacifique (Osaka), Asie-Pacifique (Séoul), Moyen-Orient (Bahreïn), Europe (Espagne), Asie-Pacifique (Hyderabad), Asie-Pacifique (Melbourne), Israël (Tel Aviv), États-Unis Ouest (Californie du Nord), Europe (Londres), Asie-Pacifique (Hong Kong), Europe (Milan), Moyen-Orient (UAE), Amérique du Sud (São Paulo), Asie-Pacifique (Mumbai), Canada (centre), Afrique (Le Cap), Europe (Zurich).	6 décembre 2023

GuardDuty étend la capacité de surveillance du temps d'exécution	Outre la détection des menaces qui pèsent sur vos EKS clusters Amazon, GuardDuty annonce la disponibilité générale de Runtime Monitoring pour détecter les menaces pesant sur vos ECS charges de travail Amazon et d'une version préliminaire pour détecter les menaces pesant sur vos EC2 instances Amazon. Pour plus d'informations sur ceux qui prennent Régions AWS actue llement en charge la surveilla nce du temps d'exécution, voir Régions et points de terminais on.	26 novembre 2023

Amazon GuardDuty a mis à jour le rôle lié au service () SLR	GuardDuty a ajouté de nouvelles autorisations permettant d'utiliser ECS les actions Amazon pour gérer et récupérer des informations sur les ECS clusters Amazon, et de gérer les paramètre s du ECS compte Amazon avec`guarddutyActivate` . Les actions relatives à Amazon récupèrent ECS également les informations relatives aux tags associés à GuardDuty. • Les autorisations suivantes ont été ajoutées dans le cadre de l' GuardDuty extension de la fonctionn alité de surveillance du temps d'exécution : `"ecs:ListClusters", "ecs:DescribeClu sters", "ecs:PutAccountSett ingDefault"`	26 novembre 2023
Mise à jour des politiques AWS gérées	GuardDuty a ajouté une nouvelle autorisation, `organizations:List Accounts` à la AmazonGua rdDutyFullAccessPolicyet AmazonGuardDutyRea dOnlyAccess.	16 novembre 2023

GuardDuty a publié de nouveaux types de résultats qui utilisent la surveillance des journaux EKS d'audit.	EKSAudit Log Monitoring prend désormais en charge les types de résultats suivants en Asie-Pacifique (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	11 novembre 2023

GuardDuty a publié de nouveaux types de résultats qui utilisent la surveillance des journaux EKS d'audit.	EKSAudit Log Monitoring prend désormais en charge les types de résultats suivants dans les régions Asie-Pacifique (Hyderabad`ap-south-2`) (), Europe (Zurich`eu-central-2`) () et Europe (Espagne) (`eu-south-2`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	10 novembre 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty a publié de nouveaux types de résultats qui utilisent la surveillance des journaux EKS d'audit.	EKSLa surveillance des journaux d'audit prend désormais en charge les types de résultats suivants. Ces types de recherche ne sont pas encore disponibles dans les régions Asie-Pacifique (Hyderabad`ap-south-2`) (), Europe (Zurich`eu-central-2`) (), Europe (Espagne`eu-south-2`) () et Asie-Pacifique (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	8 novembre 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKSRuntime Monitoring a publié le nouvel agent v1.3.1	EKSRuntime Monitoring a publié une nouvelle version de l'agent 1.3.1 qui inclut d'importants correctifs et mises à jour de sécurité.	23 octobre 2023
Nouvel attribut de filtre pour le résultat	GuardDuty a ajouté un nouveau critère pour filtrer les résultats générés. DNSle suffixe de domaine de demande fournit le domaine de deuxième et de premier niveau impliqué dans l'activité qui a incité GuardDuty à générer le résultat.	17 octobre 2023
EKSRuntime Monitoring a publié un nouvel agent v1.3.0 compatible avec Kubernetes version 1.28	EKSRuntime Monitoring a publié une nouvelle version d'agent 1.3.0 qui prend en charge la version 1.28 de Kubernetes. Ajout de la prise en charge d'Ubuntu Pour plus d'informations, consultez l'historique des versions de l'agent EKS complémentaire.	5 octobre 2023

Ajout de types de résultats basés sur S3 et l'apprentissage AWS CloudTrail automatique (ML) dans les régions Asie-Pacifique (Jakarta) et Moyen-Orient (UAE)	Le S3 et les CloudTrail résultats suivants qui identifient le comportement anormal à l'aide GuardDuty du modèle d'apprentissage automatique (ML) de détection des anomalies sont désormais disponibles dans les régions Asie-Pacifique (Jakarta) et Moyen-Orient (UAE) : • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	20 septembre 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKSLa surveillance du temps d'exécution introduit GuardDuty la gestion des agents de sécurité au niveau du cluster	EKSLa surveillance du temps d'exécution ajoute la prise en charge GuardDuty de la gestion de l'agent de sécurité pour les EKS clusters individuels afin de surveiller les événements d'exécution provenant uniquement de ces clusters sélectifs. EKSLa surveillance du temps d'exécution étend cette fonctionnalité grâce à la prise en charge des balises.	13 septembre 2023
GuardDuty Protection contre les logiciels malveillants pour EC2 étendre le support à un plus grand nombre Régions AWS	Malware Protection for EC2 est désormais disponible en Asie-Pacifique (Hyderabad), en Asie-Pacifique (Melbourne), en Europe (Zurich) et en Europe (Espagne).	11 septembre 2023

GuardDuty est désormais disponible dans la région Israël (Tel Aviv)	La région d'Israël (Tel Aviv) a été ajoutée à la Régions AWS liste des régions GuardDuty désormais disponibles. Les plans de protection suivants sont également disponibl es dans la région Israël (Tel Aviv) : • EKSProtectioninclut à la fois la surveillance du journal d'EKSaudit et la surveillance du temps EKS d'exécution. • Protection Lambda. • Protection contre les logiciels malveillants pour EC2. • Protection S3. Pour plus d'informations sur la disponibilité des plans de protection dans la région Israël (Tel Aviv), veuillez consulter Régions et points de terminais on.	24 août 2023

GuardDuty ajout d'une configuration d'activation automatique pour votre organisation au niveau du plan de protection	Mettez à jour la configuration organisationnelle des plans de protection de votre région. Les options de configuration possibles sont soit l'activation pour tous les comptes, soit l'activation automatique pour les nouveaux comptes, soit l'activation automatique pour aucun des comptes de votre organisation.	16 août 2023
Les types de recherche S3 qui identifient les comportements anormaux à l'aide GuardDuty du modèle d'apprentissage automatique (ML) de détection des anomalies sont désormais disponibles en Asie-Pacifique (Osaka)	Les types de résultat suivants sont disponibles dans la région Asie-Pacifique (Osaka) : • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10 août 2023

EKSLa surveillance du temps d'exécution est désormais disponible en Asie-Pacifique (Melbourne)	EKSLa surveillance du temps d'exécution au sein de GuardDuty EKS Protection permet de détecter les menaces liées à l'exécution pour vos EKS clusters Amazon dans AWS l'environnement. Elle est désormais prise en charge dans la région Asie-Pacifique (Melbourne).	08 août 2023
Mise à jour de la liste des GuardDuty résultats qui invoquent une analyse des programmes malveillants GuardDuty initiée à l'origine	Certains types de EKS détection de la surveillance des temps d'exécution peuvent désormais invoquer une analyse des programmes malveillants GuardDuty initiée par un logiciel malveillant dans votre Compte AWS.	19 juillet 2023
GuardDuty prend en charge 10 000 comptes membres via AWS Organizations	Un compte GuardDuty administrateur peut désormais gérer un maximum de 10 000 comptes de membres via AWS Organizations. Cela inclut également un maximum de 5 000 comptes membres associés au compte GuardDuty administrateur sur invitation.	29 juin 2023

EKSRuntime Monitoring annonce trois nouveaux types de résultats.	EKSRuntime Monitoring prend en charge trois nouveaux types de résultats basés sur la technique d'injection de processus. Les nouveaux types de recherche sont les suivants : Runtime/ DefenseEvasion .Proc, :Runtime/ ProcessInjection .Ptrace et :Runtime/. DefenseEvasion ProcessInjection DefenseEvasion ProcessInjection VirtualMemoryWrite.	22 juin 2023
EKSRuntime Monitoring a publié un nouvel agent v1.2.0 qui prend en charge la version 1.27 de Kubernetes	EKSRuntime Monitoring a publié une nouvelle version d'agent 1.2.0 qui prend également en charge les instances ARM64 basées. Ajout de la prise en charge de Bottlerocket. Pour plus d'informations, consultez l'historique des versions de l'agent EKS complémentaire.	16 juin 2023

GuardDuty la console fournit une vue résumée de vos résultats.	Le tableau de bord récapitulatif de la GuardDuty console fournit une vue agrégée des GuardDuty résultats. À l'heure actuelle, le tableau de bord affiche les données via différents widgets pour les 10 000 dernières découvertes générées pour votre compte (ou les comptes de membre si vous êtes un compte GuardDuty administrateur) pour la région actuelle.	12 juin 2023
EKSLa surveillance des journaux d'audit est désormais disponible en Asie-Pacifique (Hyderabad), en Asie-Pacifique (Melbourne), en Europe (Zurich) et en Europe (Espagne)	Activez la surveillance des journaux EKS d'audit (dans EKS Protection) pour vos comptes afin de surveiller les journaux EKS d'audit de vos EKS clusters Amazon et de les analyser pour détecter toute activité potentiellement malveillante et suspecte.	1er juin 2023
EKSLa surveillance des journaux d'audit est désormais disponible au Moyen-Orient (UAE)	EKSLa surveillance des journaux d'audit est désormais disponible au Moyen-Orient (UAE). Activez la surveillance des journaux EKS d'audit pour vos comptes afin de surveiller les journaux d'EKSaudit de vos EKS clusters Amazon et de les analyser pour détecter toute activité potentiellement malveillante et suspecte.	3 mai 2023

GuardDuty Protection contre les programmes malveillants pour les EC2 annonces Analyse des programmes malveillants à la demande	Malware Protection for vous EC2 aide à détecter la présence potentielle de logiciels malveillants dans les EBS volumes Amazon attachés à vos EC2 instances Amazon et à vos charges de travail de conteneur. Il propose désormais deux types de scans : GuardDuty initiés et à la demande. GuardDuty l'analyse des programmes malveillants initiée par -lance automatiquement une analyse sans agent dans les EBS volumes Amazon uniquement lorsqu'elle GuardDuty génère l'un des résultats invoquant une analyse des programmes malveillants GuardDuty initiée par cette dernière. Vous pouvez lancer une analyse des programmes malveillants à la demande pour EC2 les instances Amazon de votre compte en fournissant le nom de ressource Amazon (ARN) associé à cette EC2 instance Amazon. Pour plus d'informations sur les différences entre les deux types de scan, consultez la section Protection contre les programmes malveillants pour EC2.	27 avril 2023

	• GuardDuty-analyse des logiciels malveillants initiée • Analyse des programmes malveillants à la demande	
GuardDuty annonce Lambda Protection	La protection Lambda vous aide à identifier les menaces de sécurité potentielles dans vos fonctions AWS Lambda . • Types de résultat de la protection Lambda • Corriger une fonction Lambda potentiellement compromise	20 avril 2023
GuardDuty est désormais disponible dans la région Asie-Pacifique (Melbourne)	La région Asie-Pacifique (Melbourne) a été ajoutée à la liste Régions AWS des GuardDuty destinations disponibles. Pour plus d'informations sur les fonctionnalités disponibles dans cette région, veuillez consulter Régions et points de terminaison.	19 avril 2023

GuardDuty a ajouté 3 nouveaux types de EC2 résultats	GuardDuty introduit de nouveaux types de détection pour détecter l'utilisation de DNS résolveurs externes et de DNS technologies cryptées. Pour plus d'informations sur les Régions AWS domaines dans lesquels ces types de recherche sont pris en charge, consultez Régions et points de terminaison. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5 avril 2023

GuardDuty annonce la surveillance du temps EKS d'exécution dans EKS Protection	EKSLa surveillance du temps d'exécution au sein de EKS Protection permet de détecter les menaces liées à l'exécution pour vos EKS clusters Amazon dans AWS l'environnement. Il utilise un agent EKS complémentaire Amazon (`aws-guardduty-agent`) qui collecte les événements d'exécution de vos EKS charges de travail. Après avoir GuardDuty reçu ces événements d'exécution, il les surveille et les analyse afin d'identifier les menaces de sécurité suspectes potentielles. Pour plus d'informations, consultez les sections Détails de la recherche et Types de recherche relatifs à la surveillance du temps EKS d'exécution.	30 mars 2023

GuardDuty ajoute une nouvelle fonctionnalité — `autoEnableOrganizationMembers`	Amazon GuardDuty ajoute une nouvelle option de configuration d'organisation qui permet aux GuardDuty administrateurs d'auditer et de faire appliquer (si nécessaire) les comptes des administrateurs. Cette option GuardDuty est activée pour `ALL` les membres de leur organisation. Il est recommandé d'utiliser `autoEnableOrganizationMembers` au lieu de `autoEnable` . `autoEnable` est obsolète, mais toujours pris en charge. Les éléments suivants APIs sont concernés par cette nouvelle fonctionnalité : • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23 mars 2023

La fonctionnalité de RDS protection d'Amazon GuardDuty est désormais disponible pour tous	GuardDuty RDSLa protection surveille et établit le profil de l'activité de RDS connexion afin d'identifier les comportements de connexion suspects sur vos instances de base de données Amazon Aurora. Pour plus d'informations sur les types de RDS protection Régions AWS pris en charge, consultez la section Régions et points de terminaison.	16 mars 2023

GuardDuty annonce l'activation de la fonctionnalité	Historiquement, la configuration des fonctionnalités et des sources de données était GuardDuty API autorisée, mais désormais, tous les nouveaux types de GuardDuty protection seront configurés en tant que fonctionnalités et non en tant que sources de données. GuardDuty prend toujours en charge les sources de données via API mais n'en ajoutera pas de nouvellesAPI. L'activation des fonctionnalités affecte le comportement de la personne APIs utilisée pour activer GuardDuty ou du type de protection qu'elle contient GuardDuty. Si vous gérez vos GuardDuty comptes par le biais API d'un CFN modèle ou d'un modèle, consultez GuardDuty APIles modifications apportées en mars 2023. SDK	16 mars 2023
GuardDuty La protection contre les logiciels malveillants EC2 est désormais disponible dans la région Moyen-Orient (UAE)	La EC2 fonctionnalité de protection contre les programmes malveillants GuardDuty est prise en charge dans la région Moyen-Orient (UAE). Pour de plus amples informations, veuillez consulter Régions et points de terminaison.	13 mars 2023

Amazon GuardDuty a mis à jour le rôle lié au service () SLR	GuardDuty a ajouté les nouvelles autorisations suivantes pour prendre en charge la prochaine fonctionn alité de surveillance du temps GuardDuty EKS d'exécution. • Utilisez EKS les actions Amazon pour gérer et récupérer des informati ons sur les EKS clusters, ainsi que pour gérer les EKS modules complémen taires sur les EKS clusters. Les EKS actions récupèren t également les informati ons relatives aux balises associées à GuardDuty. `"eks:ListClusters", "eks:DescribeClu ster", "ec2:DescribeVpcEndp ointServices", "ec2:DescribeSecurity Groups"`	8 mars 2023
Amazon GuardDuty a mis à jour le rôle lié au service () SLR	Le GuardDuty SLR a été mis à jour pour permettre la création d'une protection contre les programmes malveillants une EC2 SLR fois que la protectio n contre les programmes malveillants EC2 a été activée.	21 février 2023

GuardDuty nécessite la TLS version 1.2 ou une version ultérieure	Pour communiquer avec les AWS ressources, GuardDuty nécessite et prend en charge la TLS version 1.2 ou ultérieur e. Pour plus d'informations, veuillez consulter Protection des données et Sécurité de l'infrastructure.	14 février 2023
GuardDuty est désormais disponible dans la région Asie-Pacifique (Hyderabad)	La région Asie-Pacifique (Hyderabad) a été ajoutée à la liste des régions Régions AWS disponibles GuardDuty . Pour de plus amples informations, veuillez consulter Régions et points de terminaison.	14 février 2023
Le guide de GuardDuty l'utilisateur Amazon est conforme aux IAM meilleures pratiques	Guide mis à jour pour s'aligner sur les IAM meilleures pratiques. Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité dans IAM.	10 février 2023
GuardDuty est désormais disponible dans la région Europe (Espagne)	L'Europe (Espagne) a été ajoutée à la liste des pays Régions AWS où GuardDuty elle est disponible. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.	8 février 2023

GuardDuty est désormais disponible dans la région Europe (Zurich)	L'Europe (Zurich) a été ajoutée à la liste Régions AWS des GuardDuty destinations disponibles. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.	12 décembre 2022
Version préliminaire d'une nouvelle fonctionnalité : GuardDuty RDS Protection	GuardDuty RDSLa protection surveille et établit le profil de l'activité de RDS connexion afin d'identifier les comportem ents de connexion suspects sur vos instances de base de données Amazon Aurora. Actuellement, elle est disponibl e pour une version préliminaire dans cinq Régions AWS. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.	30 novembre 2022
GuardDuty est désormais disponible dans la région Moyen-Orient (UAE)	Le Moyen-Orient (UAE) a été ajouté à la liste des Régions AWS endroits où GuardDuty est disponible. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.	6 octobre 2022

Ajout de contenu pour une nouvelle fonctionnalité : GuardDuty Malware Protection pour EC2	GuardDuty Malware Protection for EC2 est une amélioration facultative d'Amazon GuardDuty. Tout en GuardDuty identifiant les ressources à risque, Malware Protection for EC2 détecte les logiciels malveillants susceptib les d'être à l'origine de la compromission. Lorsque Malware Protection for EC2 est activé, chaque fois qu'un comportement suspect est GuardDuty détecté sur une EC2 instance Amazon ou qu'une charge de travail de conteneur indique la présence d'un GuardDuty logiciel malveillant, Malware Protectio n EC2 lance une analyse sans agent sur les EBS volumes attachés aux charges de travail d'EC2instance ou de conteneur touchées afin de détecter la présence de logiciels malveillants. Pour plus d'informations sur le EC2 fonctionnement de Malware Protection for et sur la configuration de cette fonctionnalité, consultez la section Protection contre les GuardDuty programmes malveillants pour EC2.	26 juillet 2022

- Pour plus d'informations sur la protection contre les programmes malveillants pour EC2 obtenir des informations, consultez la section Recherche de détails.
- Pour plus d'informations sur la correction de l'EC2instance compromise et d'un conteneur autonome, consultez la section Résolution des problèmes de sécurité découverts par. GuardDuty
- Pour plus d'informations sur les CloudWatch journaux d'audit pour les analyses de programmes malveillants et les raisons pour lesquelles une ressource est ignorée lors d'une analyse de programmes malveillants, consultez la section Comprendre CloudWatch les journaux et les raisons des sauts.
- Pour plus d'informations sur les détections de fausses menaces positives, consultez la section Signalement des faux positifs dans GuardDuty Malware Protection for EC2.

Retrait d'un type de résultat	Exfiltration:S3/ObjectRead.Unusual a été retiré.	5 juillet 2022
Ajout de nouveaux types de recherche S3 qui identifient les comportements anormaux à l'aide GuardDuty du modèle d'apprentissage automatique (ML) de détection des anomalies.	Les nouveaux types de résultat S3 suivants ont été ajoutés. Ces types de recherche identifient si une API demande a invoqué une IAM entité de manière anormale. Le modèle ML évalue toutes les API demandes de votre compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Pour en savoir plus sur chacun de ces nouveaux résultats, veuillez consulter Types de résultat S3 (langue française non garantie). • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5 juillet 2022

Ajout de contenu de GuardDuty EKS protection pour GuardDuty	GuardDuty peut désormais générer des résultats pour vos EKS ressources Amazon grâce à la surveillance des journaux EKS d'audit. Pour savoir comment configurer cette fonctionnalité, consultez EKSla section Protection sur Amazon GuardDuty. Pour une liste des résultats que GuardDuty vous pouvez générer pour les EKS ressources Amazon, consultez les résultats de Kubernetes. De nouvelles directives de correction ont été ajoutées pour permettre de corriger ces résultats dans le guide de correction des résultats Kubernetes.	25 janvier 2022
Ajout d'un nouveau résultat	Un nouveau résultat, UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS, a été ajouté. Ce résultat vous informe lorsqu'un AWS compte extérieur à votre AWS environnement accède aux informations d'identification de votre instance.	20 janvier 2022

Mise à jour des types de résultat pour simplifier l'identification des problèmes liés à log4j	Amazon GuardDuty a mis à jour les types de résultats suivants afin d'identifier et de hiérarchiser les problèmes liés aux modèles CVE -2021-44228 et CVE -2021-45046 : Backdoor : /C & .B ; Backdoor : EC2 /C & .B ! CActivity EC2 CActivity DNS; Comportement :EC2/NetworkPortUnusual.	22 décembre 2021
Modifications des résultats	Remplacement de UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration par UnauthorizedAccess :IAMUser/InstanceCredentialExfiltration.OutsideAWS Cette version améliorée du résultat apprend les emplacements habituels à partir desquels vos informations d'identification sont utilisées afin de réduire les résultats provenant du trafic acheminé via des réseaux sur site. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	7 septembre 2021
Mettre à jour vers GuardDuty SLR	GuardDuty SLRIl a été mis à jour avec de nouvelles actions visant à améliorer la précision des résultats.	3 août 2021

Informations de source de données ajoutées pour chaque type de résultat.	Les descriptions de recherche contiennent désormais des informations sur les sources de données GuardDuty utilisées pour générer cette recherche.	10 mai 2021
Retrait de 13 types de résultat.	13 résultats ont été retirés pour être remplacés par de nouveaux Anomalous Behavior résultats. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.Unusual, Impact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	12 mars 2021

Ajout de 8 nouveaux types de résultat pour les comportements anormaux.	Ajout de 8 nouveaux types de IAMUser recherche basés sur le comportement anormal des IAM principaux. CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehaviorImpact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	12 mars 2021
Ajout de EC2 résultats basés sur la réputation du domaine.	Ajout de 4 nouveaux types de résultat Impact basés sur la réputation du domaine. Impact:EC2/AbusedDomainRequest.Reputation Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. Une nouvelle EC2 découverte a également été ajoutée pour C&CActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 janvier 2021

Ajout de 4 nouveaux types de résultat.	Ajout de 3 nouvelles aliciousI PCaller découvertes S3 M. Discovery:S3/MaliciousIPCallerExfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Une nouvelle EC2 découverte a également été ajoutée pour C&CActivity. Backdoor:EC2/C&CActivity.B	21 décembre 2020
Suppression du type de résultat UnauthorizedAccess:EC2/TorIPCaller.	Le type de UnauthorizedAccess:EC2/TorIPCaller recherche est désormais retiré de GuardDuty. En savoir plus.	1er octobre 2020
Ajout du type de résultat Impact:EC2/WinRmBruteForce.	Ajout d'un nouveau résultat Impact, Impact:EC2/WinRmBruteForce. En savoir plus.	17 septembre 2020
Ajout du type de résultat Impact:EC2/PortSweep.	Ajout d'un nouveau résultat Impact, Impact:EC2/PortSweep. En savoir plus.	17 septembre 2020
GuardDuty est désormais disponible dans les régions Afrique (Le Cap) et Europe (Milan).	L'Afrique (Le Cap) et l'Europe (Milan) ont été ajoutées à la liste des AWS régions disponibles. GuardDuty En savoir plus	31 juillet 2020

Ajout de nouveaux détails d'utilisation pour le suivi des GuardDuty coûts.	Vous pouvez désormais utiliser de nouvelles mesures pour interroger les données relatives aux coûts GuardDuty d'utilisation de votre compte et des comptes que vous gérez. Un nouvel aperçu des coûts d'utilisation est disponible dans la console à l'adresse https://console.aws.amazon.com/guardduty/. Des informations plus détaillées sont disponibles via leAPI.	31 juillet 2020
Ajout de contenu couvrant la protection S3 grâce à la surveillance des événements de données S3 dans GuardDuty.	GuardDuty S3 Protection est désormais disponible via la surveillance des événements du plan de données S3 en tant que nouvelle source de données. Cette fonctionnalité sera automatiquement activée pour les nouveaux comptes. Si vous l'utilisez déjà, GuardDuty vous pouvez activer la nouvelle source de données pour vous-même ou pour vos comptes membres.	31 juillet 2020
Ajout de 14 nouveaux résultats S3.	14 nouveaux types de résultat S3 ont été ajoutés pour les sources du plan de contrôle et du plan de données S3.	31 juillet 2020

Ajout d'une prise en charge supplémentaire pour les résultats S3 et modification de 2 noms de types de résultat existants.	GuardDuty les résultats incluent désormais plus de détails sur les résultats impliquant des compartiments S3. Les types de résultat existants qui étaient liés à l'activité S3 ont été renommés : Policy:IAMUser/S3BlockPublicAccessDisabled a été modifié en Policy:S3/BucketBlockPublicAccessDisabled. Stealth:IAMUser/S3ServerAccessLoggingDisabled a été modifié en Stealth:S3/ServerAccessLoggingDisabled.	28 mai 2020
Ajout de contenu pour AWS Organizations l'intégration.	GuardDuty s'intègre désormais aux administrateurs AWS Organizations délégués pour vous permettre de gérer les GuardDuty comptes au sein de votre organisation. Lorsque vous définissez un administrateur délégué comme compte d' GuardDuty administrateur, vous pouvez automatiquement autoriser tous GuardDuty les membres de l'organisation à être gérés par le compte d'administrateur délégué. Vous pouvez également l'activer automatiquement GuardDuty dans les nouveaux comptes AWS Organizations membres. En savoir plus.	20 avril 2020

Ajout de contenu pour la fonctionnalité d'exportation des résultats.	Ajout d'un contenu qui décrit la fonctionnalité d'exportation des résultats de GuardDuty.	14 novembre 2019
Ajout du type de résultat UnauthorizedAccess:EC2/MetadataDNSRebind.	Ajout d'un nouveau résultat Unauthorized, UnauthorizedAccess:EC2/MetadataDNSRebind. En savoir plus.	10 octobre 2019
Ajout du type de résultat Stealth:IAMUser/S3ServerAccessLoggingDisabled.	Ajout d'un nouveau résultat Stealth, Stealth:IAMUser/S3ServerAccessLoggingDisabled. En savoir plus.	10 octobre 2019
Ajout du type de résultat Policy:IAMUser/S3BlockPublicAccessDisabled.	Ajout d'un nouveau résultat Policy, Policy:IAMUser/S3BlockPublicAccessDisabled. En savoir plus.	10 octobre 2019
Suppression du type de résultat Backdoor:EC2/XORDDOS.	Le type de Backdoor:EC2/XORDDOS recherche est désormais retiré de GuardDuty. En savoir plus	12 juin 2019
Ajout du type de résultat PrivilegeEscalation.	Le type de résultat Privilege Escalation détecte lorsque les utilisateurs tentent d'attribuer des privilèges transférés plus permissifs à leurs comptes. En savoir plus	14 mai 2019
GuardDuty est désormais disponible dans la région Europe (Stockholm).	L'Europe (Stockholm) a été ajoutée à la liste des AWS régions disponibles. GuardDuty En savoir plus	9 mai 2019

Ajout d'un nouveau type de résultat, Recon:EC2/PortProbeEMRUnprotectedPort.	Ce résultat vous indique qu'un port sensible EMR associé sur une EC2 instance n'est pas bloqué et qu'il fait l'objet d'une enquête active. En savoir plus	8 mai 2019
Ajout de 5 nouveaux types de détection qui détectent si vos EC2 instances sont potentiellement utilisées pour des attaques par déni de service (DoS).	Ces résultats vous informent sur EC2 les instances de votre environnement qui se comportent d'une manière qui pourrait indiquer qu'elles sont utilisées pour effectuer des attaques par déni de service (DoS). En savoir plus	8 mars 2019
Ajout d'un nouveau type de résultat : Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsagele type de recherche vous indique que les informations de connexion de votre utilisateur root Compte AWS sont utilisées pour envoyer des demandes programmatiques aux AWS services. En savoir plus	24 janvier 2019
Le type de résultat UnauthorizedAccess:IAMUser/UnusualASNCaller a été retiré	Le type de résultat UnauthorizedAccess:IAMUser/UnusualASNCaller a été retiré. Vous serez désormais informé des activités invoquées depuis des réseaux inhabituels via d'autres types de GuardDuty recherche actifs. Le type de recherche généré sera basé sur la catégorie du API qui a été invoqué depuis un réseau inhabituel. En savoir plus	21 décembre 2018

Ajout de deux nouveaux types de résultat : PenTest:IAMUser/ParrotLinux et PenTest:IAMUser/PentooLinux	PenTest:IAMUser/ParrotLinux le type de recherche vous indique qu'un ordinateur exécutant Parrot Security Linux passe des API appels en utilisant les informations d'identification qui appartiennent à votre AWS compte. PenTest:IAMUser/PentooLinux le type de recherche vous indique qu'une machine exécutant Pentoo Linux passe des API appels en utilisant les informations d'identification qui appartiennent à votre AWS compte. En savoir plus	21 décembre 2018
Ajout de la prise en charge de la SNS rubrique relative GuardDuty aux annonces Amazon	Vous pouvez désormais vous abonner à la SNS rubrique GuardDuty des annonces pour recevoir des notifications concernant les nouveaux types de recherche, les mises à jour des types de recherche existants et les autres modifications apportées aux fonctionnalités. Les notifications sont disponibles dans tous les formats pris en SNS charge par Amazon. En savoir plus	21 novembre 2018

Ajout de deux nouveaux types de résultat : UnauthorizedAccess:EC2/TorClient et UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientle type de recherche vous indique qu'une EC2 instance de votre AWS environnement établit des connexions à un nœud Tor Guard ou Authority. UnauthorizedAccess:EC2/TorRelayfinding type vous indique qu'une EC2 instance de votre AWS environnement établit des connexions à un réseau Tor d'une manière qui suggère qu'elle agit comme un relais Tor. En savoir plus	16 novembre 2018
Ajout d'un nouveau type de résultat : CryptoCurrency:EC2/BitcoinTool.B	Ce résultat vous indique qu'une EC2 instance de votre AWS environnement interroge un nom de domaine associé au Bitcoin ou à une autre activité liée aux cryptomonnaies. En savoir plus	9 novembre 2018
Ajout de la prise en charge de la mise à jour de la fréquence des notifications envoyées à CloudWatch Events	Vous pouvez désormais mettre à jour la fréquence des notifications envoyées à CloudWatch Events pour les occurrences ultérieures de résultats existants. Les valeurs possibles sont 15 minutes, 1 heure ou, par défaut, 6 heures. En savoir plus	9 octobre 2018

Prise en charge de régions supplémentaires	Ajout du support régional pour AWS GovCloud (US-Ouest) En savoir plus	25 juillet 2018
Ajout de la prise en charge AWS CloudFormation StackSets de GuardDuty	Vous pouvez utiliser le GuardDuty modèle Enable Amazon pour activer GuardDuty simultanément plusieurs comptes. En savoir plus	25 juin 2018
Ajout de la prise en charge des GuardDuty règles d'archivage automatique	Les clients peuvent désormais créer des règles fines d'archivage automatique pour la suppression de résultats. Pour les résultats correspon dant à une règle d'archivage automatique, marquez-les GuardDuty automatiquement comme archivés. Cela permet aux clients de poursuivre les réglages GuardDuty pour ne conserver que les résultats pertinents dans le tableau des résultats actuel. En savoir plus	4 mai 2018
GuardDuty est disponible dans la région Europe (Paris)	GuardDuty est désormais disponible en Europe (Paris), ce qui vous permet d'étendre la surveillance continue de la sécurité et la détection des menaces dans cette région. En savoir plus	29 mars 2018

La création de comptes d' GuardDuty administrateur et de comptes de membre via AWS CloudFormation est désormais prise en charge.	Pour plus d'informations, consultez `AWS::GuardDuty::master` et `AWS::GuardDuty::member` .	6 mars 2018
Ajout de neuf nouvelles détections CloudTrail d'anomalies basées sur des données.	Ces nouveaux types de recherche sont automatiquement activés GuardDuty dans toutes les régions prises en charge. En savoir plus	28 février 2018
Ajout de trois nouvelles détections d'intelligence de menaces (types de résultat).	Ces nouveaux types de recherche sont automatiquement activés GuardDuty dans toutes les régions prises en charge. En savoir plus	5 février 2018
Augmentation des limites pour les comptes des GuardDuty membres.	Avec cette version, vous pouvez ajouter jusqu'à 1 000 comptes GuardDuty membres par AWS compte (compte GuardDuty administrateur). En savoir plus	25 janvier 2018

Modifications apportées au téléchargement et gestion ultérieure des listes d'adresses IP fiables et des listes de menaces pour les comptes d'GuardDuty administrateur et les comptes de membres.	Avec cette version, les utilisateurs de GuardDuty comptes d'administrateur peuvent télécharger et gérer des listes d'adresses IP fiables et des listes de menaces. Les utilisateurs des GuardDuty comptes membres ne peuvent pas télécharger et gérer des listes. Les listes d'adresses IP fiables et les listes de menaces téléchargées par le compte administrateur sont imposées aux GuardDuty fonctionnalités de ses comptes membres. En savoir plus	25 janvier 2018

Mises à jour antérieures

Modification	Description	Date
Publication initiale	Publication initiale du guide de GuardDuty l'utilisateur Amazon.	28 novembre 2017

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.