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 des sources de AWS données et des journaux spécifiques dans votre AWS environnement. GuardDuty utilise des flux de renseignements sur les menaces, tels que des listes d'adresses IP et de domaines malveillants, et des modèles d'apprentissage automatique (ML) pour identifier les activités inattendues et potentiellement non autorisées dans votre AWS environnement. Cela inclut les problèmes suivants :

- Augmentation des privilèges, utilisation d'informations d'identification divulguées ou communication avec des adresses IP et des domaines malveillants.
- Présence de programmes malveillants sur vos instances Amazon EC2 et vos charges de travail de conteneur, ainsi que de fichiers récemment chargés dans vos compartiments Amazon S3.
- Découverte de modèles inhabituels d'événements de connexion dans votre base de données.

Par exemple, GuardDuty peut détecter des instances EC2 potentiellement compromises et des charges de travail de conteneurs diffusant des logiciels malveillants ou minant des bitcoins. Il surveille également le comportement d'accès aux AWS comptes pour détecter tout signe de compromission potentielle, tels que des déploiements d'infrastructure non autorisés, des instances déployées dans une région qui n'a jamais été utilisée auparavant ou des appels d'API inhabituels suggérant une modification de la politique de mot de passe afin de réduire la solidité du mot de passe.

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

- Surveille automatiquement les sources de données de base : lorsque vous activez GuardDuty un Compte AWS, commence GuardDuty automatiquement 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 d' AWS CloudTrail événements, les journaux de flux VPC (provenant d'instances Amazon EC2) et les journaux DNS. 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 plus d'informations, consultez Source de données de base.
- Activez les plans de GuardDuty protection facultatifs : pour une meilleure visibilité du niveau de sécurité de votre AWS environnement, GuardDuty propose différents plans de protection 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 d'audit EKS, l'activité de connexion RDS, les journaux S3, les volumes EBS, la surveillance du temps d'exécution et 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 optionnels dans un plan Région AWS de protection 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.

  > **Note**
  >
  > 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.

Détecte la présence de malwares et génère des résultats de sécurité

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. Vous pouvez explorer la génération Exemples de résultats et afficher les informations associéesDétails d'un résultat. Pour plus d'informations sur la liste complète des résultats de sécurité pouvant être générés pour chaque type de ressource identifié par GuardDuty, voirTypes de résultats.

Gérez les résultats de sécurité générés

Vous pouvez configurer Amazon EventBridge pour recevoir des notifications lorsqu'il GuardDuty génère un résultat, suivre les étapes recommandées pour corriger le résultat, filtrer les résultats générés pour identifier les tendances ou exporter les résultats vers un compartiment S3. Pour plus d'informations, consultez 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

- 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.

- 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 du réseau de partenaires (APN) AWS pris en charge. 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.

Gestion d'un environnement à comptes multiples

Vous pouvez gérer un AWS environnement à comptes multiples en utilisant AWS Organizations (recommandé) ou en utilisant la méthode d'invitation. Pour plus d'informations, consultez Gestion de plusieurs comptes .

Conformité PCI DSS

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 (DSS) de l'industrie des cartes de paiement (PCI) a été validée. Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section PCI DSS niveau 1.

Tarification en GuardDuty

Niveau gratuit d'AWS vous permet d'explorer et d'essayer Services AWS 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 Malware Protection for EC2) et Malware Protection for 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.

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]
GuardDuty Protection EKS	Oui	Oui
GuardDuty Protection Lambda	Oui	Oui
GuardDuty Protection contre les logiciels malveillants pour EC2 – GuardDuty-analyse des logiciels malveillants initiée	Oui	Oui
GuardDuty 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
GuardDuty Protection RDS	Oui	Oui

Plan de protection	Inclus dans l' GuardDuty essai gratuit de 30 jours	Possède son propre essai gratuit de 30 jours [1]	
GuardDuty Surveillance du temps d'exécution	Non	Oui	
GuardDuty Protection S3	Oui	Oui	

[1] En général, un plan de protection peut comporter son propre essai gratuit de 30 jours. Par exemple, lorsque vous activez un plan de protection qui devient généralement disponible après l'expiration de l'essai gratuit de GuardDuty 30 jours pour votre compte, vous pouvez utiliser l'essai gratuit de 30 jours de ce plan de protection. 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 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 plus d'informations, consultez 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 commencez à encourir des frais d'utilisation associés. Pour consulter votre facture, accédez à Cost Explorer dans la console https://console.aws.amazon.com/billing/. 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 plus d'informations, consultez 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 afficher les AWS CLI commandes disponibles pour GuardDuty, consultez la référence des commandes de la CLI.

GuardDuty API HTTPS

Vous pouvez y accéder GuardDuty et par AWS programmation en utilisant l'API GuardDuty HTTPS, qui vous permet d'envoyer des requêtes HTTPS directement au service. Pour plus d'informations, consultez le Guide de référence des GuardDuty API.

AWS SDK

AWS fournit des kits de développement logiciel (SDK) composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Python, Ruby, .NET, iOS, Android, etc.). Les SDK constituent un moyen pratique de créer un accès programmatique à. GuardDuty Pour en savoir plus sur les kits de développement logiciel AWS , y compris les procédures pour les télécharger et les installer, consultez Outils pour Amazon Web Services.

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 Source de données de base notamment les journaux d' AWS CloudTrail événements, les événements AWS CloudTrail de gestion, les journaux de flux Amazon VPC et les journaux DNS. 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 connexion RDS, les journaux S3, les volumes EBS, la surveillance de l'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 Source 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 les AWS services mondiaux tels que l'IAM. 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 rôle, un utilisateur ou un groupe IAM 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 logiciels malveillants pour EC2. 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 Source 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 for EC2 d'effectuer des analyses sans agent afin de détecter les logiciels malveillants dans votre GuardDuty compte. Il permet GuardDuty de créer un instantané du volume EBS dans votre compte et de partager cet instantané avec le compte de GuardDuty service. Pour plus d’informations, consultez 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.

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 l'adresse 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**
>
> Pour ce processus, vous devez faire partie de 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.
   - 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, consultezGérer 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 du résultat en haut du volet pour ouvrir les détails JSON complets du résultat. Le fichier JSON complet peut également être téléchargé à partir de ce panneau. Le JSON contient des informations supplémentaires non incluses dans la vue 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 clé KMS 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 clé KMS avec une politique autorisant l'utilisation GuardDuty de cette clé pour le chiffrement. Les étapes suivantes vous aideront à créer une clé KMS. Si vous utilisez une clé KMS provenant 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 clé KMS et de votre compartiment S3 doit être la même. 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 une procédure détaillée sur la création de clés KMS, veuillez consulter Création de clés du Guide du développeur AWS Key Management Service .

   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 de clé suivante à votre clé KMS, 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 stratégie de clé, assurez-vous que la syntaxe JSON 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* par la région de votre clé KMS. Remplacez *444455556666* par le propriétaire de la clé KMS Compte AWS . Remplacez *KMS KeyId* par l'ID de clé KMS que vous avez choisie pour le chiffrement. Pour identifier toutes ces valeurs (région et ID de clé), consultez l'ARN de votre clé KMS. Compte AWS Pour localiser l'ARN de clé, veuillez consulter la section Recherche de l'ID et de l'ARN d'une clé.

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

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

l. Choisissez 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 : configurer 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 une rubrique SNS qui sera la cible d'une EventBridge règle, puis vous l'utiliserez EventBridge pour créer une règle qui capture les données de GuardDuty résultats. 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 une rubrique SNS pour vos alertes de résultats

1. Ouvrez la console Amazon SNS à partir de l'adresse 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 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 l'état de l'e-mail de confirmation, accédez à la console SNS 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 rubrique SNS, et pour Rubrique, choisissez le nom de la rubrique SNS que vous avez créée 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 recherche JSON 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 dans ces filtres GuardDuty. Pour plus d’informations, consultez 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 d'adresses IP fiables, ou pour que GuardDuty les adresses IP de surveillance ne soient pas contrôlées normalement, vous pouvez configurer des adresses IP fiables et des listes de menaces.

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 l' 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 plus d’informations, consultez Gérer 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 d'un ID de détecteur est `12abc34d567e8fa901bc2d34e56789f0`.

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

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

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 flux VPC, des journaux DNS, voir. Source 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. Parmi les objets de fonctionnalité, citons les journaux d'audit EKS, la surveillance de l'activité de connexion RDS, les journaux d'activité du réseau Lambda et les volumes EBS. Pour plus d’informations, consultez Activation des fonctionnalités dans GuardDuty.

Résultat

Un problème potentiel de sécurité a été détecté par GuardDuty. Pour plus d’informations, consultez 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 opérations GetFindingset ListFindingsAPI.

Vous pouvez également consulter vos GuardDuty résultats grâce aux CloudWatch événements Amazon. GuardDuty envoie les résultats à Amazon CloudWatch via le protocole HTTPS. Pour plus d’informations, consultez Création de réponses personnalisées aux GuardDuty résultats avec Amazon CloudWatch Events.

IAM PassRole

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

Ressource du plan de protection contre les logiciels

Après avoir activé Malware Protection for S3 pour un bucket, GuardDuty crée une ressource de plan Malware Protection for EC2. Cette ressource est associée à l'identifiant du plan Malware Protection for EC2, un identifiant unique pour votre compartiment protégé. Utilisez la ressource du plan Malware Protection pour effectuer des opérations d'API sur une ressource protégée.

Bucket 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 listage d'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 instances Amazon EC2 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 instances EC2 et à votre volume EBS à une liste de balises d'inclusion ou 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 plus d'informations, consultez Options d'analyse avec balises définies par l'utilisateur.

Conservation des instantanés

Lorsque GuardDuty Malware Protection for EC2 est activée, elle permet de conserver les instantanés de vos volumes EBS dans votre compte. AWS GuardDuty génère les volumes EBS répliqués en fonction des instantanés de vos volumes EBS. Vous ne pouvez conserver les instantanés de vos volumes EBS que si le scan Malware Protection for EC2 détecte des malwares dans les répliques des volumes EBS. Si aucun logiciel malveillant n'est détecté dans les volumes EBS répliqués, supprime GuardDuty automatiquement les instantanés de vos volumes EBS, quel que soit le paramètre de conservation des instantanés. Pour plus d'informations, consultez 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'un VPC spécifique, d'une AMI spécifique ou d'une balise EC2 spécifique. 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 crypto-monnaies.

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 plus d'informations, consultez 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 plus d'informations, consultez 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 plus d'informations, voir Utilisation de listes d'adresses IP approuvées et de listes de menaces.

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 flux VPC, les journaux DNS 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 « protections » `dataSources` dans les API. 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, `dataSources` par exemple via l'API, 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 via 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 API qui sont invoquées pour activer GuardDuty ou protéger les types qu'elles contiennent GuardDuty. Pour plus d’informations, consultez GuardDuty Modifications de l'API.

GuardDuty Modifications apportées à l'API en mars 2023

Les GuardDuty API configurent des fonctionnalités de protection qui ne figurent pas dans la liste desSource 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 API suivantes dans le Amazon GuardDuty API Reference :

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

Activation des fonctionnalités par rapport aux sources de données

Historiquement, toutes les GuardDuty fonctionnalités étaient transmises via un `dataSources` objet dans l'API. À partir de mars 2023, GuardDuty préfère `features` l'objet à l'`dataSources`objet dans l'API. 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 des `dataSources` un objet `features` lors d'une transmission via une 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 demande ou de la réponse d'API est le même dans chaque Région AWS endroit GuardDuty 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

Les GuardDuty API continueront à renvoyer un `dataSources` objet le cas échéant, et elles 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 utilisation d' AWS Organizations en utilisant à la fois la notation d'objets `dataSources` et `features` dans la même demande d'API. Pour activer les types de GuardDuty protection, vous devez migrer vos sources de données existantes vers l'`features`objet en utilisant les mêmes API 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 Source 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 via des API, des SDK ou des AWS CloudFormation modèles et que vous souhaitez activer de nouvelles GuardDuty fonctionnalités potentielles, vous devrez modifier votre code et votre modèle, respectivement. Pour plus d'informations, consultez les API mises à jour dans le Amazon GuardDuty API Reference.
- Pour les GuardDuty fonctionnalités configurées avant cette mise à niveau, vous pouvez continuer à utiliser les API, les SDK ou le AWS CloudFormation modèle. 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 plus d'informations, consultez 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.
  - Cela concerne les API suivantes :

- 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 DNS	`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`
Surveillance des journaux d'audit EKS	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Protection contre les logiciels malveillants pour EC2	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
Événements de connexion RDS	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
Surveillance d'exécution EKS		`EKS_RUNTIME_MONITORING`
Surveillance du temps d'exécution		`RUNTIME_MONITORING`

GuardDuty agent de sécurité pour les clusters Amazon EKS		`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 instances Amazon EC2		`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.

Source 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, il existe un essai gratuit de 30 jours qui inclut la détection des menaces pour toutes les sources de données de base. Au cours de cet essai gratuit et par la suite, vous pouvez surveiller l'utilisation mensuelle estimée sur la page d'utilisation de la GuardDuty console, ventilée par source de données. En tant que compte d' GuardDuty administrateur délégué, vous pouvez consulter le coût d'utilisation mensuel estimé ventilé par les comptes de membres de votre organisation qui ont été activés GuardDuty.

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 journaux d'événements

AWS CloudTrail vous fournit un historique des appels d' AWS API pour votre compte, y compris les appels d'API effectués à l' AWS Management Console aide AWS des SDK, des outils de ligne de commande et de certains AWS services. CloudTrail vous aide également à identifier les utilisateurs et les comptes qui ont invoqué des AWS API pour les services compatibles 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 également les événements CloudTrail de gestion. 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. Il n'y a pas de frais supplémentaires pour GuardDuty accéder aux événements enregistrés dans CloudTrail.

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 ou l'API. 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.

AWS CloudTrail événements de gestion

Les événements de gestion sont également appelés 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 (opérations d'API `AttachRolePolicy` IAM)

- Configuration des règles de routage des données (opérations d'API `CreateSubnet` Amazon EC2)
- Configuration de la journalisation (opérations AWS CloudTrail `CreateTrail` d'API)

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 (Amazon EC2) au sein de votre environnement. AWS

Lorsque vous l'activez GuardDuty, il commence immédiatement à analyser les journaux de flux VPC provenant des instances Amazon EC2 de votre compte. Il consomme les événements de journaux de flux VPC directement depuis la fonctionnalité des journaux de flux VPC par le biais d'un flux indépendant et redondant de journaux de flux. Ce processus n'affecte pas les éventuelles configurations de journaux de flux existantes.

GuardDuty Protection Lambda

> La protection Lambda est une amélioration facultative d'Amazon. GuardDuty Actuellement, la surveillance de l'activité du réseau Lambda inclut les journaux de flux Amazon VPC provenant de toutes les fonctions Lambda de votre compte, même les journaux qui n'utilisent pas de réseau VPC. Pour protéger votre fonction Lambda contre les menaces de sécurité potentielles, vous devez configurer la protection Lambda dans votre compte. GuardDuty Pour plus d’informations, consultez GuardDuty Protection Lambda.

Surveillance du temps d'exécution dans GuardDuty

> Lorsque vous gérez l'agent de sécurité (manuellement ou via GuardDuty) dans EKS Runtime Monitoring ou Runtime Monitoring pour les instances EC2, et qu'GuardDuty il est actuellement déployé sur une instance Amazon EC2 et que vous Types d'événement d'exécution collectés le recevez de cette instance GuardDuty , l'analyse des journaux de flux VPC provenant de cette instance Amazon EC2 ne Compte AWS vous 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 et la conservation de vos journaux de flux, vous devez configurer la fonctionnalité de journaux de flux VPC.

Journaux DNS

Si vous utilisez des résolveurs AWS DNS pour vos instances Amazon EC2 (paramètre par défaut), GuardDuty vous pouvez accéder à vos journaux DNS de demandes et de réponses et les traiter via les résolveurs DNS AWS internes. Si vous utilisez un autre résolveur DNS, tel qu'OpenDNS ou GoogleDNS, ou si vous configurez vos propres résolveurs GuardDuty DNS, vous 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 DNS 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'a aucune incidence sur GuardDuty l'analyse.

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

Protection EKS sur Amazon GuardDuty

La surveillance des journaux d'audit EKS vous aide à détecter les activités potentiellement suspectes dans des clusters EKS au sein d'Amazon Elastic Kubernetes Service (Amazon EKS). EKS Audit Log Monitoring utilise les journaux d'audit EKS pour capturer les activités chronologiques des utilisateurs, des applications utilisant l'API Kubernetes et du plan de contrôle. Pour plus d'informations, consultez Surveillance du journal d'audit EKS.

> **Note**
>
> La surveillance du temps d'exécution EKS est gérée dans le cadre de la surveillance du temps d'exécution. Pour plus d'informations, consultez Surveillance du temps d'exécution dans GuardDuty.

Fonctionnalités d'EKS Protection

Surveillance du journal d'audit EKS

Les journaux d'audit EKS capturent les actions séquentielles au sein de votre cluster Amazon EKS, notamment les activités des utilisateurs, des applications utilisant l'API Kubernetes 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 permet aux journaux d'audit EKS d'être ingérés en tant qu'Amazon CloudWatch Logs via la fonction de journalisation du plan de contrôle EKS. GuardDuty ne gère pas la journalisation de votre plan de contrôle Amazon EKS et ne rend pas les journaux d'audit EKS accessibles sur votre compte si vous ne les avez pas activés pour Amazon EKS. Pour gérer l'accès à vos journaux d'audit EKS et leur conservation, vous devez configurer la fonction de journalisation du plan de contrôle Amazon EKS. Pour de plus amples informations, veuillez consulter Activation et désactivation de journaux de plan de contrôle dans le Guide de l'utilisateur Amazon EKS.

Pour plus d'informations sur la configuration de la surveillance des journaux d'audit EKS, veuillez consulterSurveillance des journaux d'audit EKS.

Surveillance des journaux d'audit EKS

La surveillance des journaux d'audit EKS vous aide à détecter les activités potentiellement suspectes dans vos clusters EKS au sein d'Amazon Elastic Kubernetes Service. Lorsque vous activez la surveillance du journal d'audit EKS, vous GuardDuty commencez immédiatement à effectuer une surveillance à Surveillance du journal d'audit EKS partir de vos clusters Amazon EKS 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 de contrôle Amazon EKS via un flux indépendant et duplicatif de journaux d'audit. Ce processus ne nécessite aucune configuration supplémentaire et n'affecte aucune configuration de journalisation du plan de contrôle Amazon EKS existante que vous pourriez avoir.

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

La surveillance du journal d'audit EKS n'est peut-être pas disponible partout Régions AWS où GuardDuty elle est disponible. Pour plus d’informations, consultez 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, EKS Audit Log Monitoring est déjà inclus 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 EKS Audit Log Monitoring pour la première fois avec une période d'essai gratuite de 30 jours.

Configuration de la surveillance des journaux d'audit EKS pour un compte autonome

Choisissez votre méthode d'accès préférée pour activer ou désactiver la surveillance des journaux d'audit EKS pour un compte autonome.

Console

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

3. Dans l'onglet Configuration, vous pouvez consulter l'état de configuration actuel de la surveillance des journaux d'audit EKS. Dans la section Surveillance des journaux d'audit EKS, choisissez Activer pour activer ou Désactiver pour désactiver la fonctionnalité de surveillance des journaux d'audit EKS.
4. Choisissez Enregistrer.

API/CLI

- Exécutez l'opération d'updateDetectorAPI en utilisant l'ID de détecteur régional du compte GuardDuty administrateur délégué et en transmettant le nom de l'`features`objet `EKS_AUDIT_LOGS` et le statut comme `ENABLED` ou`DISABLED`.

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

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

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

Configuration de la surveillance des journaux d'audit EKS dans des 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 EKS Audit Log Monitoring ; 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 la surveillance du journal d'audit EKS 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'audit EKS pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour configurer la surveillance du journal d'audit EKS 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 panneau de navigation, choisissez Protection EKS.
3. Dans l'onglet Configuration, vous pouvez consulter l'état de configuration actuel de la surveillance des journaux d'audit EKS dans la section correspondante. Pour mettre à jour la configuration du compte GuardDuty administrateur délégué, choisissez Modifier dans le volet EKS Audit Log Monitoring.
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 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 Enregistrer.

API/CLI

Exécutez l'opération d'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features` `name` en tant que `EKS_AUDIT_LOGS` et `status` en tant que `ENABLED` ou `DISABLED`.

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

Vous pouvez activer ou désactiver la surveillance du journal d'audit EKS en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser l'*identifiant de détecteur* valide du compte GuardDuty administrateur délégué.

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

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

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Pour désactiver la surveillance des journaux d'audit EKS, remplacez `ENABLED` par `DISABLED`.

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

Choisissez votre méthode d'accès préférée afin d'activer la surveillance des journaux d'audit EKS 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 Protection EKS

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

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

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

API/CLI

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

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 des journaux d'audit EKS pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée afin d'activer la surveillance des journaux d'audit EKS 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 EKS.

3. Sur la page EKS Protection, 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 Enregistrer.

API/CLI

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

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 des journaux d'audit EKS pour les nouveaux comptes 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 plus d'informations, consultez Step 3 - Accept an invitation.

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

Console

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

Pour activer automatiquement la surveillance des journaux d'audit EKS 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 :
   - À l'aide de la page Protection EKS :

     1. Dans le panneau de navigation, choisissez Protection EKS.
     2. Sur la page Protection EKS, choisissez Modifier dans Surveillance des journaux d'audit EKS.
     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 des journaux d'audit EKS sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
     5. Choisissez 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 journaux d'audit EKS.

4. Choisissez Enregistrer.

API/CLI

- Pour activer ou désactiver de manière sélective la surveillance des journaux d'audit EKS pour vos nouveaux comptes, exécutez l'opération d'API UpdateOrganizationConfiguration en utilisant votre propre *ID de détecteur*.
- L'exemple suivant montre comment activer la surveillance des journaux d'audit EKS pour les nouveaux membres qui rejoignent votre organisation. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 des journaux d'audit EKS pour les comptes membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver la surveillance des journaux d'audit EKS 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, veuillez consulter la colonne Surveillance des journaux d'audit EKS pour connaître l'état de votre compte membre.

3. Pour activer ou désactiver la surveillance des journaux d'audit EKS

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

API/CLI

Pour activer ou désactiver de manière sélective la surveillance des journaux d'audit EKS pour vos comptes membres, invoquez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur*.

L'exemple suivant montre comment activer la surveillance des journaux d'audit EKS pour un compte membre unique. Pour la désactiver, remplacez `ENABLED` par `DISABLED`. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace.

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

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

Protection Lambda sur Amazon GuardDuty

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 associées au compte, y compris les journaux qui n'utilisent pas le réseau VPC, 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 du réseau Lambda inclut les journaux de flux Amazon VPC de toutes les fonctions Lambda pour votre compte, y compris les journaux qui n'utilisent pas le réseau VPC et qui sont susceptibles d'être modifiés, notamment en cas d'extension à d'autres activités réseau telles que les données de requête DNS générées par l'invocation 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 flux VPC de toutes vos fonctions Lambda, y compris celles qui n'utilisent pas le réseau VPC. Pour les fonctions Lambda configurées pour utiliser le réseau VPC, il n'est pas nécessaire d'activer les journaux de flux VPC 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 les journaux de flux VPC et non VPC) 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 les instructions de GuardDuty la console ou de l'API, 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 Enregistrer.

API/CLI

Exécutez l'opération d'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features` `name` en tant que `LAMBDA_NETWORK_LOGS` et `status` en tant que `ENABLED` ou `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 *`ID de détecteur`* valide.

> **Note**
>
> L'exemple de code suivant active la surveillance de l'activité du réseau Lambda. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

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

API/CLI

Exécutez l'opération d'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features` `name` en tant que `LAMBDA_NETWORK_LOGS` et `status` en tant que `ENABLED` ou `DISABLED`.

Vous pouvez activer ou désactiver la surveillance de l'activité réseau Lambda en exécutant la commande suivante AWS CLI . Assurez-vous d'utiliser l'*`identifiant de détecteur`* valide du compte GuardDuty administrateur délégué.

> **Note**
>
> L'exemple de code suivant active la surveillance de l'activité du réseau Lambda. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

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

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 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 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 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 du réseau Lambda pour vos comptes membres, invoquez l'opération d'API updateMemberDetectors à l'aide de votre propre *`ID de détecteur`*.
- 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`.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 du réseau Lambda pour vos comptes membres, invoquez l'opération d'API updateMemberDetectors à l'aide de votre propre *ID de détecteur*.
- 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`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 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 Enregistrer.

API/CLI

- Pour activer ou désactiver la surveillance de l'activité du réseau Lambda pour les nouveaux comptes membres, invoquez l'opération d'API UpdateOrganizationConfiguration à l'aide de votre propre *`ID de détecteur`*.
- 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`.

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

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

Vous pouvez également transmettre une liste d'ID de compte 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 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 l'API updateMemberDetectors à l'aide de votre propre *`ID de détecteur`*.

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`.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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.

Protection contre les malwares pour EC2 sur Amazon GuardDuty

Malware Protection for EC2 vous aide à détecter la présence potentielle de malwares en analysant les volumes Amazon Elastic Block Store (Amazon EBS) attachés aux instances et aux charges de travail des conteneurs Amazon Elastic Compute Cloud (Amazon EC2). Malware Protection for EC2 propose des options d'analyse qui vous permettent de décider si vous souhaitez inclure ou exclure des instances Amazon EC2 et des charges de travail de conteneur spécifiques au moment de l'analyse. Il offre également la possibilité de conserver les instantanés des volumes Amazon EBS attachés aux instances Amazon EC2 ou aux charges de travail des conteneurs, dans vos comptes. GuardDuty Les instantanés ne sont conservés que lorsqu'un logiciel malveillant est détecté et que les résultats de la protection contre les logiciels malveillants pour EC2 sont générés.

Malware Protection for EC2 propose deux types de scans pour détecter les activités potentiellement malveillantes dans vos instances Amazon EC2 et les charges de travail de vos conteneurs GuardDuty : un scan anti-malware initié et un scan anti-malware 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 GuardDuty initié, GuardDuty chaque fois qu'un résultat indique la présence potentiel le d'un malware dans une instance Amazon EC2 ou une charge de travail de conteneur GuardDuty , lance automatiq uement un scan anti-malware sans agent sur les volumes Amazon EBS attachés à votre ressource potentiellement affectée. Pour plus d'informa tions, consultez GuardDuty-	Vous pouvez lancer une analyse des logiciels malveilla nts à la demande en fournissa nt l'Amazon Resource Name (ARN) associé à votre instance Amazon EC2 ou à votre charge de travail de conteneur. Vous pouvez lancer une analyse des programmes malveilla nts à la demande même si aucune GuardDuty recherche n'est générée pour votre ressource. Pour plus d'informa tions, consultez Analyse des

Factor	GuardDuty-analyse des logiciels malveillants initiée	Analyse des programmes malveillants à la demande
	analyse des logiciels malveillants initiée.	logiciels malveillants à la demande.
Configuration requise	Pour utiliser le scan GuardDuty anti-malware initié, vous devez l'activer pour votre compte. Pour plus d'informations, consultez Configuration de l' GuardDutyanalyse 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.
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 une 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 EC2 vous aide également à sélectionner les ressources à analyser ou à ignorer. Malware Protectio n for EC2 ne lancera pas d'analyse automatique sur les ressources que vous choisisse z 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 fournisse z l'ARN de la ressource manuellement.

*Vous devrez payer des frais d'utilisation pour créer des instantanés de volume EBS et les retenir. Pour plus d'informations sur la configuration de votre compte afin de conserver les instantanés, consultezConservation des instantanés.

La protection contre les logiciels malveillants pour EC2 est une amélioration optionnelle et est conçue de manière à ne pas affecter les performances de vos ressources. GuardDuty Pour plus d'informations sur le fonctionnement de Malware Protection for EC2 au sein de Malware Protection for EC2 GuardDuty, consultezFonctionnalité de la protection contre les programmes malveillants pour EC2. Pour plus d'informations sur la disponibilité de Malware Protection for EC2 dans différents pays Régions AWS, consultezRégions et points de terminaison.

> **Note**
>
> GuardDuty Malware Protection for EC2 ne prend pas en charge Fargate avec Amazon EKS ou Amazon ECS.

Fonctionnalité de la protection contre les programmes malveillants pour EC2

Volume Elastic Block Storage (EBS)

Cette section explique comment Malware Protection for EC2, y compris le scan GuardDuty anti-malware initié et le scan anti-malware à la demande, analyse les volumes Amazon EBS associés à vos instances Amazon EC2 et à vos charges de travail de conteneur. Avant de poursuivre, tenez compte des personnalisations suivantes :

- Options d'analyse : Malware Protection for EC2 permet de spécifier des balises afin d'inclure ou d'exclure les instances Amazon EC2 et les volumes Amazon EBS 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. Le scan GuardDuty anti-malware initié et le scan anti-malware à la demande prennent en charge le `GuardDutyExcluded` tag global. Pour plus d’informations, consultez 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 volumes Amazon EBS dans votre compte. AWS 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 plus d’informations, consultez Conservation des instantanés.

Lorsque vous GuardDuty générez un résultat indiquant la présence potentielle d'un logiciel malveillant dans une instance Amazon EC2 ou une charge de travail de conteneur et que vous avez activé le type de scan GuardDuty initié dans Malware Protection for EC2, un scan GuardDuty anti-malware initié peut être invoqué sur la base de vos options d'analyse.

Pour lancer une analyse des logiciels malveillants à la demande sur les volumes Amazon EBS associés à une instance Amazon EC2, fournissez l'Amazon Resource Name (ARN) de l'instance Amazon EC2.

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 volumes EBS pertinents attachés à la ressource potentiellement affectée et les partage avec le. GuardDuty compte de service À partir de ces instantanés, GuardDuty crée une réplique chiffrée du volume EBS dans le compte de service.

Une fois l'analyse terminée, GuardDuty supprime les volumes EBS répliqués chiffrés et les instantanés de vos volumes EBS. Si un logiciel malveillant est détecté et que vous avez activé le paramètre de conservation des instantanés, les instantanés de vos volumes EBS ne seront pas supprimés et seront automatiquement conservés dans votre compte. AWS Lorsqu'aucun logiciel malveillant n'est détecté, les instantanés de vos volumes EBS 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, veuillez consulter Tarification d'Amazon EBS.

GuardDuty conservera chaque volume EBS répliqué dans le compte de service pendant 55 heures au maximum. En cas de panne de service ou de défaillance d'un volume EBS répliqué et de son analyse des logiciels malveillants, ce volume EBS 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 volumes EBS répliqués du compte de service une fois la panne ou la panne résolue, ou une fois la période de rétention prolongée expirée.

Volumes Amazon EBS pris en charge pour l'analyse des programmes malveillants

Dans tous les appareils compatibles Régions AWS GuardDuty avec la fonctionnalité Malware Protection for EC2, vous pouvez scanner les volumes Amazon EBS chiffrés ou non chiffrés. Vous pouvez avoir des volumes Amazon EBS chiffrés avec l'une ou l'autre clé Clé gérée par AWSou une clé gérée par le client. Actuellement, certains d'entre eux prennent en Régions AWS charge à la fois le chiffrement de vos volumes Amazon EBS, 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 de GuardDuty savoir si vos volumes Amazon EBS sont chiffrés ou non :

- Les volumes Amazon EBS non chiffrés ou chiffrés avec Clé gérée par AWS — GuardDuty utilisent leur propre clé pour chiffrer les répliques des volumes Amazon EBS.

  Si votre compte appartient à un compte Région AWS qui ne prend pas en charge l'analyse de volumes Amazon EBS chiffrés avec la valeur par défaut Clé gérée par AWS pour EBS, consultez. Modification de l'ID de AWS KMS clé par défaut d'un volume Amazon EBS

- Les volumes Amazon EBS chiffrés à l'aide d'une clé gérée par le client GuardDuty utilisent la même clé pour chiffrer le volume EBS répliqué.

Malware Protection for EC2 ne prend pas en charge l'analyse des instances `productCode` Amazon EC2 avec as. `marketplace` Si une analyse des logiciels malveillants est lancée pour une telle instance Amazon EC2, 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.

Modification de l'ID de AWS KMS clé par défaut d'un volume Amazon EBS

Par défaut, l'appel de l'CreateVolumeAPI avec le chiffrement défini sur `true` sans spécifier l'ID de clé KMS crée un volume Amazon EBS chiffré avec la AWS KMS clé par défaut pour le chiffrement EBS. Toutefois, lorsqu'aucune clé de chiffrement n'est fournie explicitement, vous pouvez modifier la clé par défaut en appelant l'ModifyEbsDefaultKmsKeyIdAPI ou en utilisant la AWS CLI commande correspondante.

Pour modifier l'ID de clé EBS par défaut, ajoutez l'autorisation nécessaire suivante à votre politique IAM : `ec2:modifyEbsDefaultKmsKeyId`. Tout volume Amazon EBS nouvellement créé que vous choisissez de chiffrer mais que vous ne spécifiez pas d'ID de clé KMS associé utilisera l'ID de clé par défaut. Utilisez l'une des méthodes suivantes pour mettre à jour l'ID de clé par défaut d'EBS :

Pour modifier l'ID de clé KMS par défaut d'un volume Amazon EBS

Effectuez l’une des actions suivantes :

- Utilisation d'une API — Vous pouvez utiliser l'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 clé KMS par défaut qui cryptera les volumes Amazon EBS si vous ne fournissez pas d'ID de clé KMS. 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 instances Amazon EC2 ou vos charges de travail de conteneur lorsqu'une analyse des programmes malveillants 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 volumes EBS 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 volumes EBS répliqués en fonction des instantanés de vos volumes EBS. Une fois l'analyse terminée et le paramètre de conservation des instantanés activé dans votre compte, les instantanés de vos volumes EBS ne seront conservés que lorsqu'un logiciel malveillant est détecté et que la Protection contre les programmes malveillants pour les types de détection EC2 est générée. Que vous ayez activé ou non le paramètre de conservation des instantanés, lorsqu'aucun logiciel malveillant n'est détecté, les instantanés de vos volumes EBS sont GuardDuty automatiquement supprimés.

Coût d'utilisation des instantanés

Lors de l'analyse des programmes malveillants, lors de la GuardDuty création des instantanés de vos volumes Amazon EBS, 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, veuillez consulter Tarification d'Amazon EBS.

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 Malware Protection for 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 *detector-id* par votre propre `detectorId` valide.
3. `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 le scan GuardDuty anti-malware initié, vous pouvez également spécifier des balises afin d'inclure ou d'exclure les instances Amazon EC2 et les volumes Amazon EBS 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 ressources EC2, consultez Marquer vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2 ou baliser vos ressources Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

> **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 instances EC2 de l'analyse des logiciels malveillants

Si vous souhaitez exclure une instance Amazon EC2 ou un volume Amazon EBS pendant le processus de numérisation, vous pouvez définir la `GuardDutyExcluded` balise sur n'importe quelle instance Amazon EC2 ou volume Amazon EBS, GuardDuty et vous 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 for EC2. Vous pouvez également ajouter une balise d'instance Amazon EC2 à une liste d'exclusion. Si vous ajoutez plusieurs balises à la liste des balises d'exclusion, toute instance Amazon EC2 contenant au moins une de ces balises sera exclue du processus d'analyse des logiciels malveillants.

Choisissez votre méthode d'accès préférée pour ajouter une balise associée à une instance Amazon EC2 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 Malware Protection for 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 la section Restrictions relatives aux balises dans le guide de l'utilisateur Amazon EC2 ou Restrictions relatives aux balises dans le guide de l'utilisateur Amazon EC2.

Si aucune valeur n'est fournie pour une clé et que l'instance EC2 est étiquetée avec la clé spécifiée, cette instance EC2 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 logiciels malveillants en excluant une instance EC2 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 de *`detector-id`* par votre propre `detectorId` valide.

  `MapEquals` est une liste de paires `Key`/`Value`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 la section Restrictions relatives aux balises dans le guide de l'utilisateur

Amazon EC2 ou Restrictions relatives aux balises dans le guide de l'utilisateur Amazon EC2.

Pour inclure des instances EC2 dans l'analyse des logiciels malveillants

Si vous souhaitez analyser une instance EC2, ajoutez sa balise à la liste d'inclusion. Lorsque vous ajoutez une balise à une liste de balises d'inclusion, une instance EC2 qui ne contient aucune des balises ajoutées est ignorée de l'analyse des logiciels malveillants. Si vous ajoutez plusieurs balises à la liste des balises d'inclusion, une instance EC2 contenant au moins une de ces balises est incluse dans l'analyse des logiciels malveillants. Parfois, une instance EC2 peut être ignorée pendant le processus d'analyse. Pour plus d'informations, consultez 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 instance EC2 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 Malware Protection for 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 instance EC2 est étiquetée avec la clé spécifiée, l'instance EC2 sera incluse dans le processus d'analyse Malware Protection for EC2, quelle que soit la valeur attribuée à la balise.

API/CLI

- Mettez à jour les paramètres d'analyse des logiciels malveillants pour inclure une instance EC2 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 de *detector-id* par votre propre `detectorId` valide. Remplacez l'exemple *TestValue*par *TestKey*la `Value` paire `Key` et de la balise associée à votre ressource EC2.

`MapEquals` est une liste de paires `Key`/`Value`.

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

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --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 la section Restrictions relatives aux balises dans le guide de l'utilisateur Amazon EC2 ou Restrictions relatives aux balises dans le guide de l'utilisateur Amazon EC2.

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

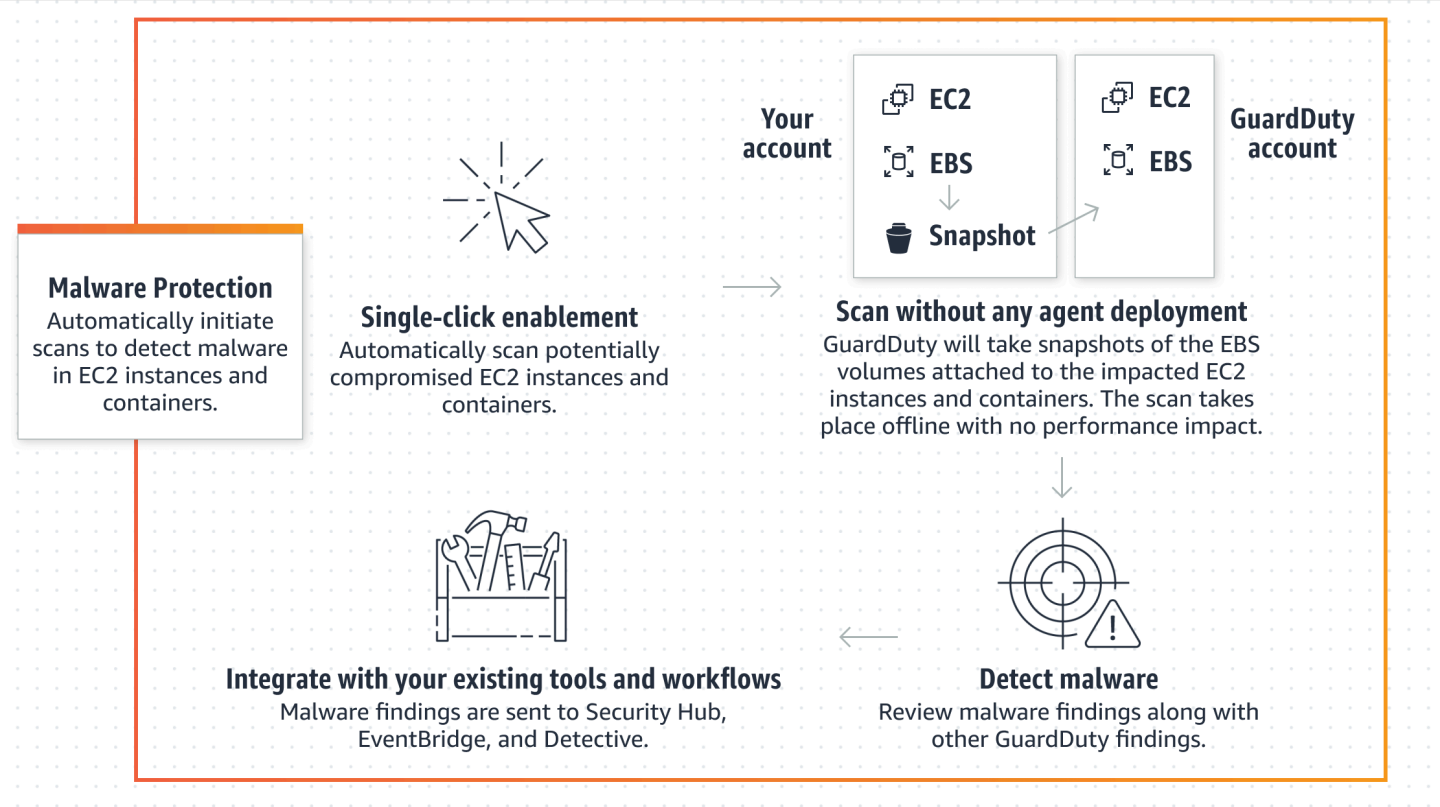
Par défaut, les instantanés de vos volumes EBS sont créés avec une balise `GuardDutyScanId`. Ne supprimez pas cette balise car cela GuardDuty empêcherait l'accès aux instantanés. Les deux types de scan de Malware Protection for EC2 n'analysent pas les instances Amazon EC2 ou les volumes Amazon EBS dont `GuardDutyExcluded` la balise est définie sur. `true` Si une protection contre les logiciels malveillants pour EC2 analyse une telle ressource, un ID de scan sera généré mais l'analyse sera ignorée pour une `EXCLUDED_BY_SCAN_SETTINGS` raison. Pour plus d'informations, consultez 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 qu'une activité malveillante indique la présence potentielle d'un logiciel malveillant dans votre instance ou votre charge de travail de conteneur Amazon EC2 GuardDuty et Résultats qui invoquent une analyse des programmes malveillants GuardDuty initiée par un programme malveillant génère GuardDuty , lance automatiquement une analyse sans agent sur les volumes Amazon Elastic Block Store (Amazon EBS) attachés à l'instance ou à la charge de travail de conteneur Amazon EC2 potentiellement affectée afin de GuardDuty 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 pour conserver les instantanés de vos volumes EBS uniquement si Malware Protection for EC2 détecte la présence d'un logiciel malveillant. Pour plus d'informations, consultez Personnalisations de la protection contre les programmes malveillants pour EC2.

Pour chaque instance Amazon EC2 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 volumes Amazon EBS attachés à votre instance Amazon EC2 ou à votre charge de travail de conteneur sont analysés, veuillez consulter Fonctionnalité de la protection contre les programmes malveillants pour EC2.

L'image suivante décrit le fonctionnement de l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant.



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 plus d'informations, consultez 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 Malware Protection for EC2 avant l'annonce du scan anti-malware à la demande et que ce GuardDuty compte utilise déjà le modèle tarifaire correspondant Région AWS, vous pouvez continuer à utiliser le scan GuardDuty anti-malware 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 volume Amazon EBS et leur conservation s'appliquent. Pour plus d'informations, consultez la section Tarification d'Amazon EBS.

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 Malware Protection for EC2.

3. Le volet Protection contre les programmes malveillants pour EC2 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 Enregistrer.

API/CLI

- Exécutez l'opération d'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant l'objet `dataSources` avec `EbsVolumes` défini 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 *`ID de détecteur`* valide.

  > **Note**
  >
  > L'exemple de code suivant active l'analyse des programmes malveillants GuardDuty initiée par l'utilisateur. Pour la désactiver, remplacez `true` par `false`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 plus d'informations, consultez 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 les Autorisations de rôle liées à un service pour Malware Protection for EC2 comptes membres gérés via 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 plus d'informations, consultez 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 for 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 page Protection contre les programmes malveillants pour EC2, 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 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 Enregistrer.

API/CLI

Exécutez l'opération d'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features` `name` en tant que `EBS_MALWARE_PROTECTION` et `status` en tant que `ENABLED` ou `DISABLED`.

Vous pouvez activer ou désactiver l'analyse des programmes malveillants GuardDuty initiée en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser l'*`identifiant de détecteur`* valide du compte GuardDuty administrateur délégué.

> **Note**
>
> L'exemple de code suivant active l'analyse des programmes malveillants GuardDuty initiée par l'utilisateur. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 page Protection contre les programmes malveillants pour EC2

   1. Dans le volet de navigation, choisissez Malware Protection for EC2.
   2. Sur la page Protection contre les programmes malveillants pour EC2, 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 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 page Protection contre les programmes malveillants pour EC2, 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 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 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 par vos comptes membres, appelez l'opération updateMemberDetectorsAPI à l'aide de votre propre *`identifiant de détecteur`*.
- 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`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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. Sur Malware Protection for 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 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. Les comptes des membres gérés par invitation peuvent configurer manuellement une analyse des logiciels malveillants GuardDuty initiée pour leurs comptes. Pour plus d’informations, consultez 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 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 logiciels malveillants pour EC2 ou des 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 page Protection contre les programmes malveillants pour EC2 :
     1. Dans le volet de navigation, choisissez Malware Protection for EC2.
     2. Sur la page Protection contre les programmes malveillants pour EC2, choisissez Modifier dans le GuardDutyscan de programmes malveillants lancé.
     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 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 Enregistrer.

API/CLI

- Pour activer ou désactiver l'analyse des programmes malveillants GuardDuty lancée pour les nouveaux comptes membres, appelez l'opération UpdateOrganizationConfigurationAPI à l'aide de votre propre *`identifiant de détecteur`*.
- 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`.

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

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

  Vous pouvez également transmettre une liste d'ID de compte 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 une analyse des programmes malveillants GuardDuty initiée.

API/CLI

Pour activer ou désactiver de manière sélective l'analyse des programmes malveillants GuardDuty initiée par vos comptes membres, appelez l'opération updateMemberDetectorsAPI à l'aide de votre propre *`identifiant de détecteur`*.

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`.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 par vos comptes membres, exécutez l'opération updateMemberDetectorsAPI à l'aide de votre propre *`identifiant de détecteur`*. 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`.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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

Le rôle lié au service (SLR) GuardDuty Malware Protection for EC2 doit être créé 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 programmes 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 reflex pour le compte du membre. Pour plus d'informations sur RLS, veuillez consulter Autorisations de rôle liées à un service pour Malware Protection for 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 DisassociateMembersl'API sur les comptes 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.

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

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```

3. Utilisez le compte administrateur pour exécuter l'CreateMembersAPI afin 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 d'une instance ou d'un conteneur Amazon EC2.

- 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 logiciels malveillants à la demande vous permet de détecter la présence de logiciels malveillants sur les volumes Amazon Elastic Block Store (Amazon EBS) attachés à vos instances

Amazon EC2. Aucune configuration n'est nécessaire, vous pouvez initier une analyse des logiciels malveillants à la demande en fournissant l'Amazon Resource Name (ARN) de l'instance Amazon EC2 que vous souhaitez analyser. Vous pouvez lancer une analyse des programmes malveillants à la demande par le biais de la GuardDuty console ou de l'API. 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 programmes malveillants dans vos instances Amazon EC2 sans activer l'analyse des programmes malveillants GuardDuty initiée par un programme malveillant.
- 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 le type de détection Malware Protection for EC2 généré, 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 logiciels malveillants sur la même instance EC2, veuillez consulter 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 volume total d'Amazon EBS analysé pour chaque analyse des logiciels malveillants. Pour plus d'informations, consultez les GuardDuty tarifs Amazon. Pour plus d'informations sur le coût de création des instantanés des volumes Amazon EBS et leur conservation, veuillez consulter Tarification d'Amazon EBS.

Fonctionnement de l'analyse des logiciels malveillants à la demande

Grâce à l'analyse des logiciels malveillants à la demande, vous pouvez initier une demande d'analyse des logiciels malveillants pour votre instance Amazon EC2 même lorsqu'elle est actuellement

utilisée. Après avoir lancé une analyse des programmes malveillants à la demande, GuardDuty crée des instantanés des volumes Amazon EBS attachés à l'instance Amazon EC2 dont le nom de ressource Amazon (ARN) a été fourni pour l'analyse. Ensuite, GuardDuty partage ces instantanés avec leGuardDuty compte de service. GuardDuty crée des répliques de volumes EBS chiffrés à partir de ces instantanés du compte de GuardDuty service. Pour plus d'informations sur la manière dont les volumes Amazon EBS sont analysés, veuillez consulter Volume Elastic Block Storage (EBS).

> **Note**
>
> GuardDuty crée les instantanés des données qui ont déjà été écrites sur les volumes Amazon EBS 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 volumes EBS 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 volumes EBS sont supprimés.

Par défaut, les instantanés de vos volumes EBS sont créés avec une balise `GuardDutyScanId`. Ne supprimez pas cette balise car cela GuardDuty empêcherait l'accès aux instantanés. Les deux types de scan de Malware Protection for EC2 n'analysent pas les instances Amazon EC2 ou les volumes Amazon EBS dont `GuardDutyExcluded` la balise est définie sur. `true` Si une protection contre les logiciels malveillants pour EC2 analyse une telle ressource, un ID de scan sera généré mais l'analyse sera ignorée pour une `EXCLUDED_BY_SCAN_SETTINGS` raison. Pour plus d'informations, consultez 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 (SCP) incluses 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 instance Amazon EC2 détenue par vos comptes.

En tant que compte GuardDuty membre, lorsque vous lancez une analyse des programmes malveillants à la demande pour vos instances Amazon EC2, vous pouvez recevoir un message

d'erreur. Vous pouvez vous connecter au compte de gestion pour comprendre pourquoi une SCP a été configurée pour votre compte membre. Pour de plus amples informations, veuillez consulter Effets des SCP 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 programmes malveillants à la demande pour leurs propres instances Amazon EC2.

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 l'AWS politique gérée : AmazonGuardDutyFullAccess est attaché à l'utilisateur IAM ou au rôle IAM. Vous aurez besoin de la clé d'accès et de la clé secrète associées à l'utilisateur IAM ou au rôle IAM.
- 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 votre compte membre n'en dispose pasAutorisations de rôle liées à un service pour Malware Protection for EC2, le lancement d'une analyse des programmes malveillants à la demande pour une instance Amazon EC2 appartenant à votre compte créera automatiquement le SLR pour Malware Protection for EC2.

> **Important**
>
> Assurez-vous que personne ne supprime les autorisations SLR pour Malware Protection for 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 plus d'informations, consultez 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 page Protection contre les programmes malveillants pour EC2 :

      i. Dans le volet de navigation, sous Plans de protection, sélectionnez Malware Protection for EC2.

      ii. Sur la page Protection contre les programmes malveillants pour EC2, indiquez l'ARN[1] de l'instance Amazon EC2 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 l'analyse à la demande et indiquez l'ARN d'instance Amazon EC2[1] pour laquelle vous souhaitez initier l'analyse.

      iii. S'il s'agit d'une nouvelle analyse, sélectionnez un ID d'instance Amazon EC2 sur la page Analyses des logiciels malveillants.

      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 plus d'informations, consultez Surveillance de l'état et des résultats de l'analyse des logiciels malveillants.

API/CLI

Appelez StartMalwareScanqui accepte `resourceArn` l'instance Amazon EC2 [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 ARN d'instance Amazon EC2, veuillez consulter Amazon Resource Name (ARN). Pour les instances Amazon EC2, vous pouvez utiliser l'exemple de format ARN suivant en remplaçant les valeurs de partition, de région, d'ID Compte AWS et d'ID d'instance Amazon EC2. Pour plus d'informations sur la longueur de votre ID d'instance, veuillez consulter ID de ressource.

```
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 de programmes malveillants à la demande sur la même instance EC2 une heure après le début de la précédente analyse de programmes malveillants. 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 des scans et des résultats de la protection contre les GuardDuty logiciels malveillants pour EC2.

Surveillance de l'état des scans et des résultats de la protection contre les GuardDuty logiciels malveillants pour EC2

Vous pouvez surveiller l'état de chaque analyse GuardDuty Malware Protection for EC2. 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
   - ARN d'Instance EC2
   - 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 la même `CriterionKey` que ci-dessous, assurez-vous de remplacer l'exemple de `EqualsValue` par votre propre valeur AWS *`scan-id`* valide.

Remplacez l'exemple de `detector-id` par votre propre *`detector-id`* valide. Vous pouvez modifier la valeur *`max-results`* (jusqu'à 50) et *`sort-criteria`*. L'`AttributeName` est obligatoire et doit être `scanStartTime`.

```
aws guardduty describe-malware-scans --detector-
id 60b87779336485625 54d637e0e4bb3b2 --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 plus d'informations, consultez Fonctionnalité de la protection contre les programmes 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
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

Région AWS	Code région	GuardDuty ID de compte de service (**`userId`**)
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
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 (EAU) (Inscription)	me-central-1	828603743433

Protection contre les programmes malveillants pour les quotas EC2

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 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 EC2 a 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 détails JSON 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

Portée	Par défaut	Commentaires
		détectée. Par exemple, si 10 fichiers associés à une seule menace sont GuardDuty détectés, la menace affichera un maximum de 5 fichiers.
Volumes EBS par analyse et par instance	11	Nombre maximal de volumes EBS GuardDuty pouvant être numérisés par instance EC2. Si plus de 11 volumes EBS doivent être analysés, GuardDuty Malware Protection for EC2 les trie `deviceName` par ordre alphabétique et sélectionne les 11 premiers volumes EBS.
Taille du volume EBS	2048 GO	Associée à une instance Amazon EC2 et à une charge de travail de conteneur, GuardDuty Malware Protection for EC2 peut scanner chaque volume Amazon EBS d'une taille maximale de 2 048 Go. Ce quota s'applique à tous ceux Région AWS où la prise en charge de Malware Protection for 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 : • New Technology File System (NTFS) • X File System (XFS) • Second extended (ext2) File System • Fourth extended (ext4) File System • File Allocation Table (FAT) File System • Virtual File Allocation Table (VFAT) File System	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 plus d'informations, consultez Options d'analyse avec balises définies par l'utilisateur.
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.

Portée	Par défaut	Commentaires
Période de conservation de l'analyse des logiciels malveillants	90	Nombre maximal de jours pendant lesquels GuardDuty Malware Protection for 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 des scans et des résultats de la protection contre les GuardDuty logiciels malveillants pour EC2.
Transactions par seconde (TPS) pour l'analyse des logiciels 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.
- En tant que compte d' GuardDuty administrateur délégué, vous recevrez une EventBridge notification Amazon chaque fois qu'un compte membre active cette fonctionnalité pour son compartiment Amazon S3.
- Actuellement, le type de recherche Malware Protection for S3 ne prend pas en charge l'intégration avec AWS Security Hub Amazon Detective. Cela s'applique uniquement au type de recherche Malware Protection for S3.

Table des matières

- Désactiver la protection contre les programmes malveillants pour S3 pour un compartiment protégé
- Quotas dans la protection contre les malwares pour S3

Comment fonctionne Malware Protection for S3 ?

Cette section décrit les composants de Malware Protection for S3 qui vous aideront à comprendre son fonctionnement.

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.

Autorisations IAM PassRole

Malware Protection for S3 utilise un IAM PassRole 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 rôle IAM 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 rôle IAM existant pour inclure le nom de l'autre compartiment, le cas échéant. Pour plus d’informations, consultez Prérequis : créer ou mettre à jour une politique IAM PassRole .

Marquage facultatif des objets en fonction du résultat de l'analyse

Lorsque vous activez Malware Protection for S3 pour votre compartiment, une étape facultative permet d'activer le balisage des objets S3 scannés. L'IAM inclut PassRole 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 value.

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 basé sur des balises (TBAC) afin de pouvoir prendre des mesures sur les objets potentiellement malveillants. Pour plus d'informations, consultez Ajouter le TBAC à la ressource du 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.

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 autorisations IAM, GuardDuty il crée et gère une règle EventBridge gérée nommée. `DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`

Garde-fous pour la protection des données

> Malware Protection for S3 écoute les EventBridge notifications Amazon. Lorsqu'un objet est chargé dans le compartiment sélectionné ou dans l'un des préfixes, GuardDuty télécharge cet objet à l'aide d'un AWS PrivateLink, puis le lit, le déchiffre et le scanne dans un environnement isolé de la même région. Pendant la durée de l'analyse, stocke GuardDuty temporairement l'objet S3 téléchargé dans l'environnement de numérisation. Une fois l'analyse des programmes malveillants terminée, GuardDuty la copie téléchargée de l'objet est supprimée.

Afficher le 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.

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, à l'aide de l'API/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 à l'aide d'une plateforme d'infrastructure en tant que code (IaC) telle que Terraform. Pour plus d'informations, voir Ressource : `aws_guardduty_malware_protection_plan`.
- Supporte le balisage des objets S3 scannés (facultatif) : après chaque analyse de logiciels malveillants, GuardDuty une balise indiquant l'état d'analyse de l'objet S3 chargé est ajoutée. Vous pouvez utiliser cette balise pour configurer le contrôle d'accès basé sur les balises (TBAC) pour les objets S3. Par exemple, vous pouvez restreindre l'accès aux objets S3 jugés malveillants et dont la valeur de balise est égale à`THREATS_FOUND`.
- EventBridge Notifications Amazon — Lorsque vous configurez une EventBridge règle, vous recevez une notification concernant l'état de l'analyse des programmes malveillants dans S3.

  Votre compte d' GuardDuty administrateur délégué recevra une EventBridge notification lorsqu'un compte membre active cette protection pour un compartiment Amazon S3 appartenant à son propre compte.
- CloudWatch métriques — Affichez les métriques intégrées dans GuardDuty la console. Ces métriques incluent des détails sur vos objets S3.

Lorsque vous l'activez également GuardDuty, vous recevrez un résultat de sécurité lorsqu'un objet S3 est identifié comme contenant un fichier potentiellement malveillant. GuardDuty recommande des mesures pour vous aider à corriger le résultat généré.

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 Service AWS 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.

API Amazon S3 GET et coût PUT d'utilisation

Vous devrez payer des frais d'utilisation lorsque vous GuardDuty exécuterez les API Amazon S3 basées sur l' PassRoleIAM. Par exemple, après avoir adopté l'IAM PassRole, GuardDuty exécute l'`PutObject`API pour ajouter l'objet de test au bucket sélectionné. Cela permet GuardDuty d'évaluer le statut activé de la fonctionnalité.

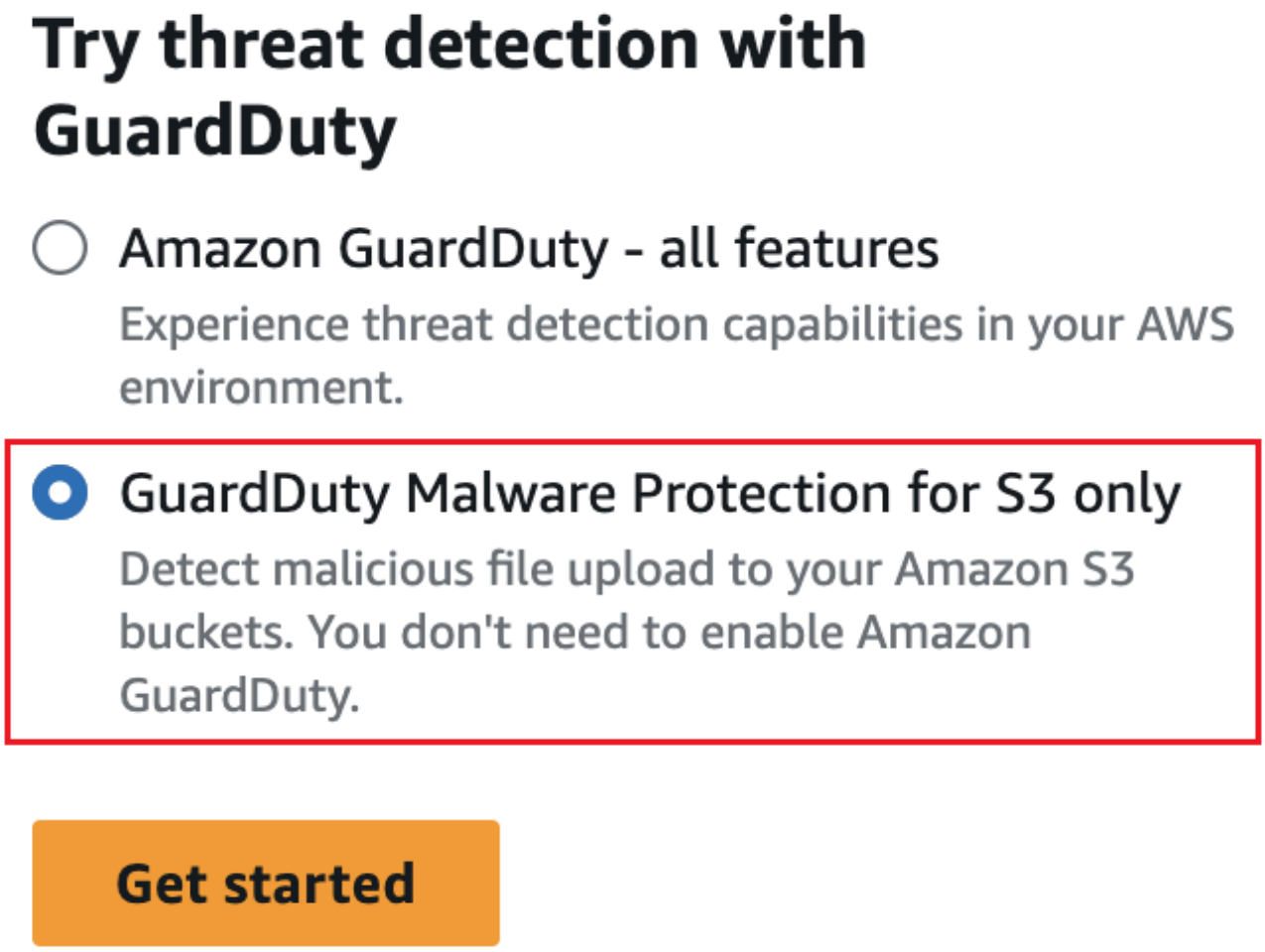
Pour plus d'informations sur la tarification des appels d'API S3 dans votre Région AWS compte, consultez la section Demandes et extraction de données sous l'onglet Stockage et demandes de la page de tarification d'Amazon S3.

(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 commenciez à utiliser Malware Protection for S3 de manière indépendante 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 IAM PassRole
2. Activez la protection contre les programmes malveillants pour S3 pour votre compartiment

Prérequis : créer ou mettre à jour une politique IAM PassRole

Pour que Malware Protection for S3 puisse analyser et (éventuellement) ajouter des balises à vos objets S3, vous devez créer et associer un rôle IAM 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 clés KMS à accéder à l'objet avant de scanner et de placer un objet de test sur des compartiments avec le chiffrement DSSE-KMS et SSE-KMS pris en charge.

> **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 avez déjà un IAM existant PassRole, vous pouvez mettre à jour sa politique pour inclure les détails d'une autre

ressource de compartiment S3. La Ajouter des autorisations de politique IAM rubrique fournit un exemple expliquant comment procéder.

Utilisez les politiques suivantes pour créer ou mettre à jour un IAM PassRole.

Politiques

- Ajouter des autorisations de politique IAM
- Ajouter une politique de relation de confiance

Ajouter des autorisations de politique IAM

Vous pouvez choisir de mettre à jour la politique intégrée d'un IAM existant ou PassRole d'en créer un nouveau. PassRole Pour plus d'informations sur les étapes, voir Création d'un rôle IAM ou Modification d'une politique d'autorisations de rôle dans le Guide de l'utilisateur IAM.

Ajoutez le modèle d'autorisations suivant à votre rôle IAM préféré. Remplacez les valeurs d'espace réservé suivantes par les valeurs appropriées associées à votre compte :

- Pour *DOC-EXAMPLE-BUCKET*, remplacez-le par le nom de votre compartiment Amazon S3.

  Pour utiliser le même IAM PassRole pour plusieurs ressources de compartiment S3, mettez à jour une politique existante, comme indiqué dans l'exemple suivant :

  ```
  ...
  ...
  "Resource": [
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
  ],
  ...
  ...
  ```

  Assurez-vous d'ajouter une virgule (,) avant d'ajouter un nouvel ARN associé au compartiment S3. Procédez ainsi chaque fois que vous faites référence à un compartiment S3 `Resource` dans le modèle de politique.
- Pour *111122223333*, remplacez-le par votre identifiant. Compte AWS
- Pour *us-east-1*, remplacez par votre. Région AWS

- Pour *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/*"
```

Modèle de PassRole politique IAM

```
{
    "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:::DOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketNotification",
                "s3:GetBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
            ]
        },
        {
            "Sid": "AllowPutValidationObject",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/malware-protection-resource-
validation-object"
            ]
        },
        {
            "Sid": "AllowCheckBucketOwnership",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
            ]
```

```
        },
        {
           "Sid": "AllowMalwareScan",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-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 rôle IAM. Pour plus d'informations sur les étapes à suivre, 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
- (Facultatif) Marquez les objets numérisés
- Autorisations
- (Facultatif) Marquez l'identifiant du plan de protection contre les programmes malveillants
- Étapes à suivre après avoir activé la protection contre les programmes malveillants pour S3

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'être`us-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.

(Facultatif) Marquez 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 plus d'informations, consultez 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 de l'état de numérisation des objets S3.
- Configurez une politique de contrôle d'accès basé 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 les balises (TBAC), consultez. Utilisation 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 plus d'informations, consultez Utilisation d'Amazon EventBridge.
- Lorsque le rôle IAM 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 rôle IAM requise pour le balisage, consultez. Prérequis : créer ou mettre à jour une politique IAM PassRole

  GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour plus d'informations, consultez Utilisation d'Amazon EventBridge.

Pour sélectionner une option sous Marquer les objets numérisés

- Lorsque vous souhaitez ajouter GuardDuty des balises à vos objets S3 numérisés, sélectionnez Marquer 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 rôle IAM 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 rôle IAM

1. Si vous avez déjà effectué les étapes ci-dessousPrérequis : créer ou mettre à jour une politique IAM PassRole , procédez comme suit :

   - Dans la section Permissions, pour le nom du rôle IAM, choisissez un nom de rôle IAM qui inclut les autorisations nécessaires.
2. Si vous n'avez pas encore effectué les étapes ci-dessousPrérequis : créer ou mettre à jour une politique IAM PassRole , procédez comme suit :

a. Choisissez Afficher les autorisations.

b. Sous Détails des autorisations, choisissez l'onglet Politique. Cela montre un modèle des autorisations IAM requises.

   Copiez ce modèle, puis choisissez Fermer à la fin de la fenêtre Détails des autorisations.

c. Choisissez Attach policy qui ouvre la console IAM dans un nouvel onglet. Vous pouvez choisir de créer un nouveau rôle IAM ou de mettre à jour un rôle IAM 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 rôle IAM.

   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 console IAM est ouverte. Ajoutez cette politique de relation de confiance à votre rôle IAM 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 du tag et la valeur du tag 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 ressources de contrôle d'accès basée sur des balises (TBAC) : lorsque vous activez le balisage, assurez-vous d'ajouter la politique TBAC à la ressource de votre compartiment S3 avant qu'un objet ne soit chargé dans le compartiment sélectionné. Pour plus d'informations, consultez Ajouter le TBAC à la ressource du compartiment S3.
2. Surveiller l'état du plan de protection contre les programmes malveillants : surveillez la colonne État de protection pour 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 sur 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-dessous Surveillance de l'état de numérisation des objets 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-dessous Surveillance de l'état de numérisation des objets 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 *	Votre seau n'est pas protégé. Il est possible que certaines analyses de programmes malveillants associées à cet objet S3 ne soient pas terminées. S'il n'est pas résolu, le problème peut entraîner une défaillance critique de tous les objets. Il peut y avoir une ou plusieurs causes profondes potentielles.

État	Description
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.

Le tableau suivant fournit des informations détaillées sur le statut et les étapes correspondantes pour résoudre ces problèmes.

Statut	Problème	Détails du statut	Étapes de résolution des problèmes
Avertissement	Impossible de mettre l'objet de test	Pour valider la configuration du bucket sélectionné, GuardDuty place un objet de test dans votre bucket.	Au rôle IAM sélectionné, ajoutez les autorisations suivantes GuardDuty afin de placer l'objet de test sur la ressource sélectionnée : `{ "Sid": "AllowPut ValidationObject", "Effect": "Allow", "Action": [ "s3:PutObject" ], "Resource": [ "arn:aws:s3::: DOC-EXAMPLE-BUCKET /malware-`

Statut	Problème	Détails du statut	Étapes de résolution des problèmes

			<pre>protection-resource-validat
			ion-object"
			]
			}</pre>
			Remplacez *DOC-EXAMPLE-BUCKET par le nom de votre compartiment* Amazon S3. Pour plus d'informations sur les autorisations des rôles IAM, consultezPrérequis : créer ou mettre à jour une politique IAM PassRole .
			
			Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

Statut	Problème	Détails du statut	Étapes de résolution des problèmes

	Impossible de surveiller la configuration de Malware Protection pour S3	Le rôle IAM ne dispose pas des autorisations nécessaires GuardDuty pour surveiller la configuration de Malware Protection for S3 pour ce compartiment.	Ajoutez les autorisations suivantes à votre rôle IAM :
			
			{
			"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": {
			"StringEquals": {
			"events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
			}
			}
			},
			{
			"Sid": "AllowEnableS3EventBridgeEvents",
			"Effect": "Allow",
			"Action": [
			"s3:PutBucketNotification",
			"s3:GetBucketNotification"

Statut	Problème	Détails du statut	Étapes de résolution des problèmes

			<pre>],
			"Resource": [
			"arn:aws:s3::: *DOC-EXAMPLE-BUCKET* "
			]
			}</pre> Quelques minutes peuvent être nécessaires pour que la valeur de la colonne Status passe à Active.

Statut	Problème	Détails du statut	Étapes de résolution des problèmes
Erreur	EventBridge la notification est désactivée pour ce compartiment S3.	GuardDuty utilise EventBridge pour recevoir une notification lorsqu'un nouvel objet est chargé dans ce compartiment S3. Cette autorisation est absente de votre rôle IAM.	• Option 1 : ajoutez la déclaration d'autorisation suivante à votre rôle IAM : `{ "Sid": "AllowEnableS3EventBridgeEvents", "Effect": "Allow", "Action": [ "s3:PutBucketNotification", "s3:GetBucketNotification" ], "Resource": [ "arn:aws:s3::: DOC-EXAMPLE-BUCKET " ] }` Remplacez *DOC-EXAMPLE-BUCKET par 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 sur https://console.aws.amazon.com/s3/. 2. Sur la page Compartiments, sous l'onglet Buckets à usage général, sélectionnez le nom du bucket associé à cette erreur. 3. Sur cette page de bucket, choisissez l'onglet Propriétés.

Statut	Problème	Détails du statut	Étapes de résolution des problèmes
			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.

Statut	Problème	Détails du statut	Étapes de résolution des problèmes
	EventBridge la règle gérée pour recevoir les événements du compartiment S3 est manquante.	Les autorisations des règles EventBridge gérées permettant de gérer la configuration des EventBridge règles sont manquantes.	Ajoutez la déclaration d'autorisation suivante à votre rôle IAM : `{ "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.

Statut	Problème	Détails du statut	Étapes de résolution des problèmes
	Ce compartiment S3 n'existe plus.	Ce compartiment S3 a été supprimé de votre compte et n'existe plus.	Si la suppression du compartiment S3 n'était pas intentionnelle, vous pouvez en créer un nouveau à l'aide de la console Amazon S3. Une fois le compartiment créé avec succès, activez Malware Protection for S3 en suivant les étapes décrites dans la Configuration de la protection contre les programmes malveillants pour S3 pour votre compartiment page.

Surveillance de l'état de numérisation des objets 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 console et des API, 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 potentielles des résultats d'analyse des 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`— GuardDuty ne prend pas en charge l'analyse de ce type d'objet. Cet objet S3 est ignoré au moment de la numérisation. Pour plus d'informations sur les objets pris en charge, consultezQuotas dans la protection contre les malwares pour S3.
- `ACCESS_DENIED`— GuardDuty Impossible d'accéder à cet objet pour le scanner. Vérifiez les autorisations de rôle IAM associées à ce compartiment. Pour plus d’informations, consultez Prérequis : créer ou mettre à jour une politique IAM PassRole .

- `FAILED`— GuardDuty impossible d'effectuer une analyse des programmes malveillants sur cet objet en raison d'une erreur interne.

Méthodes de surveillance du résultat de l'analyse des objets S3

- Utilisation d'Amazon EventBridge
- Utilisation des CloudWatch métriques Amazon pour le plan de protection contre les logiciels malveillants
- Activation du balisage d'objets dans Malware Protection for S3

Utilisation d'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 PassRole n'a pas les autorisations nécessaires pour étiqueter l'objet.

    Le Ajouter des autorisations de politique IAM modèle inclut l'autorisation de GuardDuty baliser un objet.
  - La ressource ou l'objet du bucket spécifié dans l'IAM PassRole 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 Service AWS 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 Tarification de la protection contre les programmes malveillants pour S3.

Toutes les valeurs qui apparaissent en *`rouge`* sont des espaces réservés pour l'exemple. Ces valeurs changeront en fonction du résultat de l'analyse de votre objet S3.

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": "DOC-EXAMPLE-BUCKET"
        },
        "resourceStatus": "ACTIVE"
    }
}
```

Exemple de schéma de notification pour **`GuardDuty Malware Protection Resource Status Error`** ou **`GuardDuty Malware Protection Resource Status Warning`**

```
{
    "version": "0",
    "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
    "detail-type": "GuardDuty Malware Protection Resource Status Error or 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": "DOC-EXAMPLE-BUCKET"
        },
        "resourceStatus": "ERROR",
        "statusReasons": [{
            "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
        }, {
            "code": "PROTECTED_RESOURCE_DELETED"
        }]
```

```
    }
}
```

La `resourceStatus` valeur peut être `Warning` soit`Error`.

Lorsque la colonne Status d'un bucket protégé devient Warning ou Error, la `statusReasons` valeur est renseignée en fonction de la raison sous-jacente. Pour plus d'informations sur les étapes de résolution des problèmes, consultezRésolution des problèmes liés à l'état du plan de protection contre les.

Événements de défaillance survenus après l'étiquetage

Schéma de l'événement :

```
{
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
 }
```

Exemple de schéma de notification :

```
{
    "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": "DOC-EXAMPLE-BUCKET",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6"
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "status": "FAILED",
            "failureReason": "ACCESS_DENIED"
```

```
        }]
    }
}
```

`failureReason`Les valeurs potentielles incluent `ACCESS_DENIED` et`MAX_TAG_LIMIT_EXCEEDED`.

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": {
        "versionId": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "DOC-EXAMPLE-BUCKET",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE"
        },
        "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": {
        "versionId": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "DOC-EXAMPLE-BUCKET",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "threats": [
                {
                    "name": "EICAR-Test-File (not a virus)"
                }
            ]
        }
    }
}
```


Utilisation des CloudWatch métriques Amazon pour le plan de protection contre les logiciels malveillants

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` Statistiques valides : SUM 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` Statistiques valides : somme 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`
	Statistiques valides : somme
	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` Statistiques valides : somme 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` Statistiques valides : somme Unités : nombre

> **Note**
>
> Par défaut, les statistiques des CloudWatch métriques sont AVG.

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`	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.

Activation du balisage d'objets dans Malware Protection for 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 plus d'informations, consultez Tarification de la protection contre les programmes malveillants pour S3.
- Vous devez conserver les autorisations de balisage requises pour votre IAM préféré PassRole associé à ce compartiment ; sinon, GuardDuty vous ne pourrez pas ajouter de balises à vos objets numérisés. L'IAM inclut PassRole déjà les autorisations permettant d'ajouter des balises aux objets S3 scannés. Pour plus d'informations, consultez Prérequis : créer ou mettre à jour une politique IAM PassRole .
- Par défaut, vous pouvez associer jusqu'à 10 balises à un objet S3. Pour plus d'informations, consultez 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).

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 plus d'informations, consultez 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 value.

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 plus d'informations, consultez Utilisation d'Amazon EventBridge.
- Lorsque le rôle IAM 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 rôle IAM requise pour le balisage, consultez. Prérequis : créer ou mettre à jour une politique IAM PassRole

  GuardDuty publie également le résultat de l'analyse sur votre bus d' EventBridge événements par défaut. Pour plus d'informations, consultez Utilisation d'Amazon EventBridge.

Ajouter le TBAC à la ressource du compartiment S3

Vous pouvez utiliser les politiques de ressources du compartiment S3 pour gérer le contrôle d'accès basé sur les 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`* par`s3`.

La liste suivante explique ce que vous pouvez faire avec 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 ayant accès de potentiellement remplacer la paire clé-valeur du tag.

Exemple de politique de ressources du compartiment S3 :

Remplacez *`IAM-Role-name`* par l'IAM PassRole 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:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-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:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-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.

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.

Quota général

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.
5 Go	Non	Quantité maximale de données (en Go) GuardDuty pouvant être extraites et analysées à partir d'un fichier d'archive

AWS valeur de quota par défaut	Est-il ajustable ?	Description
		. 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.
10	Non	Nombre maximal de compartiments S3 pour lesquels vous pouvez activer la protection contre les programmes malveillants pour S3. Cette valeur de quota s'applique au niveau de la région.

AWS valeur de quota par défaut	Est-il ajustable ?	Description
25	Au niveau du compte	Le nombre maximum d'opérations du plan de contrôle pouvant être initiées par seconde dans chaque région. Les opérations d'API incluent la création, la lecture, la mise à jour et la suppression de ressources. Cette valeur de quota s'applique au Compte AWS niveau.

Fichiers soumis à une analyse des logiciels malveillants

Le support est-il disponible ?	Description
Non	Si le fichier est une archive protégée par mot de passe, les octets chiffrés seront analysés. L'archive ne sera ni extraite ni décompressée.

Fonctions d'Amazon S3

Le support est-il disponible ?	Description
Oui	Les objets S3 peuvent être récupérés sans restauration asynchrone.

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.

Le support est-il disponible ?	Description
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 rôle IAM Passrole inclut l'autorisation d'utiliser la clé. Pour plus d’informations, consultez Ajouter des autorisations de politique IAM.

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.
Oui	Les objets S3 verrouillés sont verrouillés sur la base de WORM - Write Once Read Many. Malware Protection for S3 peut accéder aux objets et les scanner.

Le support est-il disponible ?	Description
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 la section Gérer le cycle de vie de votre stockage dans le guide de l'utilisateur Amazon S3.
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 plus d’informations, consultez Utilisation du contrôle d'accès basé sur des balises (TBAC) avec Malware Protection pour S3.

Protection contre les programmes malveillants pour le quota régional S3

Le support est-il disponible ?	Description
Oui	Le Compte AWS propriétaire du compartiment S3 possède également la ressource du plan de protection contre les logiciels malveillants. Les deux ressources sont identiques Région AWS.
Non	Les ressources du plan de protection contre les programmes malveillants ne peuvent pas être réparties entre plusieurs Comptes AWS. Si un Compte AWS compte est autorisé à créer la ressource du plan de protection contre les programme s malveillants dans un autre Compte AWS compte propriétaire d'un compartiment S3 (DOC-EXAMPLE-BUCKET1), l'ancien compte peut configurer la ressource du plan pour DOC-EXAMPLE-BUCKET1.

Le support est-il disponible ?	Description
Non	Vous ne pouvez pas configurer la ressource du plan de protection contre les programmes malveillants entre les régions.

Protection RDS dans GuardDuty

Dans Amazon, RDS Protection GuardDuty analyse et établit le profil de l'activité de connexion RDS pour détecter les menaces d'accès potentielles à vos bases de données Amazon Aurora (édition compatible Amazon Aurora MySQL et édition compatible Aurora PostgreSQL) et à Amazon RDS for PostgreSQL. Cette fonctionnalité vous permet d'identifier les comportements de connexion potentiellement suspects. La protection RDS 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 Protection détecte une tentative de connexion potentiellement suspecte ou anormale indiquant une menace pour votre base de données, elle GuardDuty génère une nouvelle découverte contenant des informations sur la base de données potentiellement compromise.

Vous pouvez activer ou désactiver la fonctionnalité de protection RDS 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, la protection RDS est déjà activée et incluse dans la période d'essai gratuite de 30 jours. Pour plus d’informations, consultez Estimation du coût.

> **Note**
>
> Lorsque la fonction de protection RDS n'est pas activée, elle GuardDuty ne collecte pas votre activité de connexion RDS 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 la protection RDS, consultezDisponibilité des fonctionnalités propres à la région.

Bases de données Amazon Aurora et Amazon RDS prises en charge

Le tableau suivant indique les versions de base de données Aurora et Amazon RDS prises en charge.

Moteur de base de données Amazon Aurora et Amazon RDS	Versions de moteur prises en charge
Aurora MySQL	• Versions 2.10.2 ou ultérieures • Versions 3.02.1 ou ultérieures
Aurora PostgreSQL	• 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
RDS for PostgreSQL	• 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 • RDS pour PostgreSQL version 15 • RDS pour PostgreSQL version 16

Comment la protection RDS utilise-t-elle la surveillance de l'activité de connexion RDS ?

La protection RDS d'Amazon vous GuardDuty aide à protéger les bases de données Amazon Aurora (Aurora) prises en charge dans votre compte. Après avoir activé la fonction de protection RDS, commence GuardDuty immédiatement à surveiller l'activité de connexion RDS à partir des bases de données Aurora de votre compte. GuardDuty surveille et profile en permanence l'activité de connexion RDS pour détecter toute activité suspecte, par exemple un accès non autorisé à la base de données Aurora sur votre compte, par un acteur externe invisible auparavant. Lorsque vous activez la protection RDS 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 plus d'informations, consultez Surveillance de l'activité de connexion RDS.

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 plus d'informations, consultez Types de résultat de la protection RDS. Si vous désactivez la protection RDS, la surveillance de l'activité de connexion RDS est GuardDuty immédiatement interrompue et aucune menace potentielle ne peut être détectée pour les instances de base de données prises en charge.

> **Note**
>
> GuardDuty ne gère pas votre activité de connexion Bases de données prises en charge ou celle de RDS, et ne met pas l'activité de connexion RDS à votre disposition.

Configuration de la protection RDS pour un compte autonome

Console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Dans le panneau de navigation, choisissez Protection RDS.
3. La page Protection RDS 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'opération d'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features` `name` en tant que `RDS_LOGIN_EVENTS` et `status` en tant que `ENABLED` ou `DISABLED`.

Vous pouvez également activer ou désactiver la protection RDS en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser votre propre *`ID de détecteur`* valide.

> **Note**
>
> L'exemple de code suivant active la protection RDS. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

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

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

Configuration de la protection RDS dans des 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 protection RDS 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 la surveillance de l'activité de connexion RDS 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 protection RDS pour un compte d' GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour configurer la surveillance de l'activité de connexion RDS 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 RDS.

3. Sur la page Protection RDS, 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 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 Enregistrer.

API/CLI

Exécutez l'opération d'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant l'objet `features` `name` en tant que `RDS_LOGIN_EVENTS` et `status` en tant que `ENABLED` ou `DISABLED`.

Vous pouvez activer ou désactiver la protection RDS en exécutant la AWS CLI commande suivante. Assurez-vous d'utiliser l'*`identifiant de détecteur`* valide du compte GuardDuty administrateur délégué.

> **Note**
>
> L'exemple de code suivant active la protection RDS. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

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

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Activer automatiquement la protection RDS pour tous les comptes membres

Choisissez votre méthode d'accès préférée pour activer la fonctionnalité de protection RDS 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 Protection RDS

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

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

API/CLI

- Pour activer ou désactiver la protection RDS de manière sélective pour vos comptes membres, invoquez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur*.
- L'exemple suivant montre comment vous pouvez activer la protection RDS pour un compte membre unique. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 RDS pour tous les comptes membres actifs existants

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

Console

Pour configurer la protection RDS 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 RDS.
3. Sur la page Protection RDS, 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 RDS de manière sélective pour vos comptes membres, invoquez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur*.
- L'exemple suivant montre comment vous pouvez activer la protection RDS pour un compte membre unique. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 RDS pour les nouveaux comptes membres

Choisissez votre méthode d'accès préférée pour activer l'activité de connexion RDS 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 soit la protection RDS, soit la page des comptes.

Pour activer automatiquement la protection RDS 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 RDS :
     1. Dans le panneau de navigation, choisissez Protection RDS.
     2. Sur la page Protection RDS, 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 RDS sera automatiquement activée pour son compte. Seul le compte GuardDuty administrateur délégué de l'organisation peut modifier cette configuration.
     5. Choisissez 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 tous les comptes sous Surveillance de l'activité de connexion RDS.

4. Choisissez Enregistrer.

API/CLI

- Pour activer ou désactiver la protection RDS de manière sélective pour vos comptes membres, invoquez l'opération d'API UpdateOrganizationConfiguration en utilisant votre propre *ID de détecteur*.
- L'exemple suivant montre comment vous pouvez activer la protection RDS pour un compte membre unique. Pour la désactiver, veuillez consulter Activer ou désactiver la protection RDS de manière sélective pour les comptes membres. Si vous ne souhaitez pas l'activer pour tous les nouveaux comptes qui rejoignent l'organisation, définissez `autoEnable` sur `NONE`.

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

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

  > **Note**
  >
  > Vous pouvez également transmettre une liste d'ID de compte 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 la protection RDS de manière sélective pour les comptes membres

Choisissez votre méthode d'accès préférée pour activer ou désactiver de manière sélective la surveillance de l'activité de connexion RDS 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 Activité de connexion RDS pour connaître l'état de votre compte membre.

3. Pour activer ou désactiver de manière sélective l'activité de connexion RDS

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

API/CLI

Pour activer ou désactiver la protection RDS de manière sélective pour vos comptes membres, invoquez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur*.

L'exemple suivant montre comment vous pouvez activer la protection RDS pour un compte membre unique. Pour la désactiver, remplacez `ENABLED` par `DISABLED`.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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.

Fonctionnalité de la protection RDS

Surveillance de l'activité de connexion RDS

L'activité de connexion RDS capture les tentatives de connexion réussies et infructueuses effectuées au niveau de la Bases de données Amazon Aurora et Amazon RDS prises en charge dans votre environnement AWS . Pour vous aider à protéger vos bases de données, GuardDuty RDS Protection surveille en permanence l'activité de connexion pour détecter les tentatives de connexion potentiellement suspectes. 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 protection RDS, commence GuardDuty automatiquement à surveiller l'activité de connexion RDS pour vos bases de données directement depuis le service Aurora. 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 protection RDS 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 protection RDS ne nécessite aucune configuration supplémentaire ; elle n'affecte aucune de vos configurations de base de données Amazon Aurora existantes. GuardDuty ne gère pas vos bases de données prises en charge ou votre activité de connexion RDS, et ne met pas l'activité de connexion RDS à votre disposition.

Si vous choisissez d'activer automatiquement la fonctionnalité de protection RDS 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 connexion RDS en tant que fonctionnalité, veuillez consulter Protection RDS dans GuardDuty.

Surveillance du temps d'exécution dans GuardDuty

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.

GuardDuty a initialement publié Runtime Monitoring pour prendre en charge uniquement les ressources Amazon Elastic Kubernetes Service (Amazon EKS). Toutefois, vous pouvez désormais également utiliser la fonctionnalité Runtime Monitoring pour détecter les menaces pour vos ressources AWS Fargate Amazon Elastic Container Service (Amazon ECS) et Amazon Elastic Compute Cloud (Amazon EC2).

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 Amazon EKS, Fargate, Amazon ECS et Amazon EC2.

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 (Amazon ECS 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 demandes d'API 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 instances Amazon EC2, de vos clusters Amazon ECS et de vos charges de travail Amazon EKS.
2. Gérez l' GuardDuty agent pour les ressources individuelles dont vous souhaitez surveiller le comportement d'exécution. En fonction du 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 terminaison du VPC.

> **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 instances EC2, et qu'GuardDuty il est actuellement déployé sur une instance Amazon EC2 et que vous Types d'événement d'exécution collectés le recevez de cette instance GuardDuty , l'analyse des journaux de flux VPC provenant de cette instance Amazon EC2 ne Compte AWS vous 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 la surveillance du temps d'exécution avec les instances Amazon EC2

Vos instances Amazon EC2 peuvent exécuter plusieurs types d'applications et de charges de travail dans votre environnement. AWS 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 instances Amazon EC2 existantes et dans les nouvelles instances potentielles. Cette fonctionnalité prend également en charge les instances Amazon EC2 gérées par Amazon ECS.

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 des instances Amazon EC2. GuardDuty nécessite qu'un agent de sécurité envoie les événements d'exécution de votre instance EC2 à GuardDuty.

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

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 instances Amazon EC2 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 instances EC2 uniquement, ajoutez des balises d'inclusion ou d'exclusion à vos instances EC2, selon vos besoins.

Il peut arriver que vous ne souhaitiez pas surveiller les événements d'exécution pour toutes les instances Amazon EC2 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 partir de la disponibilité de la configuration automatique des agents pour Amazon EC2, si votre instance EC2 possède une balise d'inclusion (`GuardDutyManaged:true`), cette balise GuardDuty sera respectée 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'instances EC2 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 ressources EC2.

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 association SSM pour toutes vos instances Amazon EC2 qui sont gérées par SSM et apparaissent sous Fleet Manager dans la console https://console.aws.amazon.com/systems-manager/.
- 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 instance Amazon EC2, cela signifie que vous êtes autorisé GuardDuty à gérer l'agent de sécurité en votre nom. L'association SSM 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, l'association SSM installera ensuite l'agent de sécurité dans toutes les instances EC2 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 instance Amazon EC2, 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'association SSM installe et gère l'agent de sécurité dans toutes les instances EC2, à l'exception de celles qui sont étiquetées avec la balise d'exclusion.
- GuardDuty crée des points de terminaison VPC dans tous les VPC, y compris les VPC partagés, à condition qu'il y ait au moins une instance Linux EC2 dans ce VPC qui ne soit pas dans l'état d'instance terminée ou en état d'arrêt. Pour plus d'informations sur les différents états des instances, consultez la section Cycle de vie des instances dans le guide de l'utilisateur Amazon EC2.

  GuardDuty prend également en chargeUtilisation d'un VPC partagé 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 VPC partagé pour recevoir les événements d'exécution.

> **Note**
>
> L'utilisation du point de terminaison VPC n'entraîne aucun coût supplémentaire.

Gestion manuelle de l'agent de sécurité

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

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

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

Étape suivante

Pour commencer à configurer la surveillance du temps d'exécution afin de surveiller vos instances Amazon EC2, consultez. Conditions préalables à la prise en charge des instances Amazon EC2

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

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 clusters Amazon ECS, 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.

Actuellement, Runtime Monitoring prend en charge la gestion de l'agent de sécurité pour vos clusters Amazon ECS (AWS Fargate) uniquement via GuardDuty. La gestion manuelle de l'agent de sécurité sur les clusters Amazon ECS 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 point de terminaison VPC via lequel l'agent de sécurité transmet les événements d'exécution. GuardDuty

> **Note**
>
> L'utilisation du point de terminaison VPC n'entraîne aucun coût supplémentaire.

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 ECS Fargate. 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 la surveillance du temps d'exécution avec les clusters Amazon EKS

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

Vous pouvez surveiller les événements d'exécution de vos clusters Amazon EKS au niveau du compte ou du cluster. Vous ne pouvez gérer l'agent GuardDuty de sécurité que pour les clusters

Amazon EKS 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 pour GuardDuty permettre de gérer le déploiement de l'agent de sécurité en votre nom, un point de terminaison Amazon Virtual Private Cloud (Amazon VPC) est automatiquement créé. L'agent de sécurité fournit les événements d'exécution à l'aide GuardDuty de ce point de terminaison Amazon VPC.

> **Note**
>
> L'utilisation du point de terminaison VPC n'entraîne aucun coût supplémentaire.

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

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 [1] 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.

[1] 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 plus d’informations, consultez Évaluation de la couverture d'exécution de vos ressources.

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 instances Amazon EC2, vos clusters Amazon ECS ou vos clusters Amazon EKS, elle en génère une ou plusieurs. Types 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 EKS Runtime Monitoring avant que la fonctionnalité de surveillance du temps d'exécution ne soit étendue aux instances Amazon EC2 et AWS Fargate (Amazon ECS uniquement).

J'utilise la période GuardDuty d'essai ou je n'ai jamais activé EKS Runtime Monitoring

La liste suivante explique comment fonctionne 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 EKS Runtime Monitoring :

- Lorsque vous l'activez GuardDuty pour la première fois, la surveillance du temps d'exécution et la surveillance du temps d'exécution EKS 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 la surveillance du temps d'exécution pour vos instances Amazon EC2, vous devez également configurer l'agent de sécurité pour Amazon EC2 après l'avoir activé. 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 l'instance Amazon

EC2, le cluster Amazon ECS et le cluster Amazon EKS). Dès GuardDuty réception du premier événement d'exécution pour une instance Amazon EC2, l'essai gratuit de 30 jours commence uniquement pour Amazon EC2.

- Lorsque vous souhaitez activer uniquement EKS Runtime Monitoring : lorsque vous l'activez GuardDuty pour la première fois, EKS Runtime Monitoring n'est pas activé par défaut (après la sortie de Runtime Monitoring). Vous devez activer EKS Runtime Monitoring. 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 ressource Amazon EKS.

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 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 support API/CLI pour effectuer des opérations associées à EKS Runtime Monitoring.
- Pour utiliser EKS Runtime Monitoring dans le cadre de 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, voir[Migration d'EKS Runtime Monitoring vers Runtime Monitoring](). Toutefois, cela n'aura aucune incidence sur votre essai gratuit de 30 jours pour la ressource Amazon EKS.
- 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 (instance Amazon EC2 et cluster Amazon ECS), l'essai gratuit de 30 jours commence à la GuardDuty réception du premier événement d'exécution associé à la ressource. 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 instance Amazon EC2. 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 instance Amazon EC2. Plus tard, lorsque vous déploierez l' GuardDuty agent pour Fargate (Amazon ECS 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 EKS Runtime Monitoring pour votre compte, GuardDuty cela ne réinitialise pas l'essai gratuit de 30 jours pour une ressource Amazon EKS.

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 clusters Amazon EKS et Amazon ECS.

Table des matières

Ressource Fargate (Amazon ECS 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 clusters Amazon ECS (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 tâches Amazon ECS.

Actuellement, Runtime Monitoring prend en charge la gestion de l'agent de sécurité pour vos clusters Amazon ECS (AWS Fargate) uniquement via GuardDuty. La gestion manuelle de l'agent de sécurité sur les clusters Amazon ECS 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 tâches Amazon ECS. Envisagez les approches suivantes.

Rubriques

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

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

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 clusters Amazon ECS appartenant à votre compte.

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

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

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

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

Utilisez cette approche lorsque vous GuardDuty souhaitez détecter des menaces de sécurité potentielles pour certains clusters Amazon ECS. Cette approche vous permet de surveiller le comportement d'exécution des conteneurs au sein de vos tâches Amazon ECS au niveau du cluster. Par exemple, le nombre de clusters Amazon ECS 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 clusters Amazon ECS que vous souhaitez surveiller. Pour plus d'informations, consultez Gestion de l'agent de sécurité automatisé pour Fargate (Amazon ECS uniquement).

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

GuardDuty Pour utiliser les événements d'exécution de vos clusters EKS 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, l'agent de sécurité GuardDuty sera géré sur tous les clusters EKS appartenant à un Compte AWS. Désormais, GuardDuty fournit une fonctionnalité granulaire pour vous aider à choisir les clusters EKS dans lesquels vous GuardDuty souhaitez gérer l'agent de sécurité.

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

> **Note**
>
> Quelle que soit l'approche que vous utilisez pour gérer l'agent GuardDuty de sécurité, EKS Runtime Monitoring est toujours activé 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 clusters EKS de votre compte en utilisant l'une des approches suivantes.

Rubriques

- Surveiller tous les clusters EKS
- Surveiller tous les clusters EKS et exclure certains clusters EKS
- Surveiller des clusters EKS sélectifs

Surveiller tous les clusters EKS

- Quand utiliser cette approche : utilisez cette approche lorsque vous GuardDuty souhaitez déployer et gérer l'agent de sécurité pour tous les clusters EKS de votre compte. Par défaut, l'agent de sécurité GuardDuty sera également déployé sur un cluster EKS potentiellement nouveau créé dans votre compte.
- Impact de l'utilisation de cette approche :
  - GuardDuty crée un point de terminaison Amazon Virtual Private Cloud (Amazon VPC) via lequel l'agent GuardDuty de sécurité transmet les événements d'exécution. GuardDuty La création du point de terminaison Amazon VPC 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 terminaison `guardduty-data` VPC actif. GuardDuty déploie l'agent de sécurité sur vos clusters EKS. Amazon Elastic Kubernetes Service (Amazon EKS) 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 point de terminaison VPC. Si vous utilisez des topologies réseau avancées, vous devez vérifier que la connectivité est possible.
- Considération : actuellement, lorsque vous utilisez cette option, la surveillance d'exécution EKS ne crée pas de VPC partagé.

Surveiller tous les clusters EKS et exclure certains clusters EKS

- Quand utiliser cette approche : utilisez cette approche lorsque vous souhaitez GuardDuty gérer l'agent de sécurité pour tous les clusters EKS de votre compte, mais exclure certains clusters EKS. Cette méthode utilise une approche basée sur les balises[1] dans laquelle vous pouvez étiqueter les clusters EKS 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 clusters EKS 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 clusters EKS exclus de la surveillance.

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

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

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

Surveiller des clusters EKS sélectifs

- Quand utiliser cette approche : utilisez cette approche lorsque vous souhaitez déployer et gérer les mises GuardDuty à jour de l'agent de sécurité uniquement pour certains clusters EKS de votre compte. Cette méthode utilise une approche basée sur les balises[1] dans laquelle vous pouvez étiqueter le cluster EKS pour lesquels 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 clusters EKS sélectionnés marqués « `GuardDutyManaged` - » `true` en tant que paire clé-valeur.
  - L'utilisation de cette approche aura également le même impact que celui spécifié pour Surveiller tous les clusters EKS.

- Considérations :
  - Si la valeur de la balise `GuardDutyManaged` 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 cluster EKS.
  - Pour vous assurer que vos clusters EKS sélectifs sont surveillés, vous devez empêcher la modification des balises, sauf par des identités approuvées.

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

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

[1] Pour plus d'informations sur l'étiquetage de clusters EKS sélectifs, veuillez consulter Étiquetage de vos ressources Amazon EKS dans le Guide de l'utilisateur Amazon EKS.

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 clusters EKS. Assurez-vous que la surveillance d'exécution EKS est activée pour vos comptes. L'agent GuardDuty de sécurité risque de ne pas fonctionner comme prévu si vous n'activez pas EKS Runtime Monitoring.
- Impact de l'utilisation de cette approche — Vous devrez coordonner le déploiement du logiciel de l'agent de GuardDuty sécurité au sein de vos clusters EKS sur tous les comptes et sur les Régions AWS lieux 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 plus d'informations, consultez Prérequis.

Si vous utilisiez EKS Runtime Monitoring avant le lancement de Runtime Monitoring, vous pouvez utiliser les API pour vérifier et mettre à jour la configuration existante pour EKS Runtime Monitoring. Vous pouvez également migrer votre configuration existante d'EKS Runtime Monitoring vers Runtime Monitoring. Pour plus d'informations, consultez Migration d'EKS Runtime Monitoring vers Runtime Monitoring.

> **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 des actions d'API 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 préalables à la prise en charge des instances Amazon EC2

Gérer les instances EC2 par SSM

Les instances Amazon EC2 pour lesquelles vous souhaitez GuardDuty surveiller les événements d'exécution doivent être gérées AWS Systems Manager (SSM). 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 instances Amazon EC2 avec AWS Systems Manager, consultez la section Configuration de Systems Manager pour les instances Amazon EC2 dans AWS Systems Manager le guide de 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 instances Amazon EC2 :

- 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 instances Amazon EC2.

Distribution du système d'exploitation	Version de noyau	Support du noyau	Architecture du processeur	
			64 bits (AMD64)	Graviton (ARM64)
• AL2 et AL2023 • Ubuntu 20.04 et Ubuntu 22.04 • Debian 11 et Debian 12	5,4, 5,10, 5,15, 6,1, 6,5, 6,8	eBPF, Tracepoints, Kprobe	Pris en charge	Pris en charge

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

  Pour Amazon ECS/Amazon EC2, nous vous recommandons d'utiliser les dernières AMI optimisées pour Amazon ECS (datées du 29 septembre 2023 ou version ultérieure), ou d'utiliser la version v1.77.0 de l'agent Amazon ECS.

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, assurez-vous que la politique ne refuse pas l'autorisation`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 des SCP pour votre organisation, voir Politiques de contrôle des services (SCP).

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 association SSM pour une nouvelle instance, assurez-vous que la nouvelle instance est gérée par SSM et qu'elle apparaît sous Fleet Manager dans la console https://console.aws.amazon.com/systems-manager/.
- 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 instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 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.

Limite du processeur et de la mémoire pour GuardDuty l'agent

Limite du processeur

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

Limite de mémoire

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

Le tableau suivant indique la limite de mémoire.

Mémoire de l'instance Amazon EC2	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 requises pour le AWS Fargate support (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 clusters Amazon ECS. Vous devez confirmer que vous utilisez l'une des plateformes vérifiées.

Considérations initiales :

La AWS Fargate (Fargate) plate-forme de vos clusters Amazon ECS 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 du système d'exploitation et l'architecture du processeur 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	Architecture du processeur	
		64 bits (AMD64)	Graviton (ARM64)
Linux	eBPF, Tracepoints, Kprobe	Pris en charge	Pris en charge

Fournir les autorisations ECR 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 (Amazon ECR). Vous pouvez soit utiliser la politique TaskExecutionRolePolicy gérée par AmazonECS, soit ajouter les autorisations suivantes à votre `TaskExecutionRole` politique :

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

Pour restreindre davantage les autorisations Amazon ECR, vous pouvez ajouter l'URI du référentiel Amazon ECR qui héberge l'agent GuardDuty de sécurité pour (AWS Fargate Amazon

ECS uniquement). Pour plus d'informations, consultez 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 comme entrée dans votre définition de tâche, soit créer un point de terminaison Amazon ECR VPC.

- Utilisation de l'option de définition des tâches : pour exécuter les UpdateServiceAPI CreateServiceand dans la référence d'API Amazon Elastic Container Service, vous devez transmettre les informations du sous-réseau. Pour plus d'informations, consultez les définitions des tâches Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.
- En utilisant l'option de point de terminaison VPC Amazon ECR — Fournissez le chemin réseau vers Amazon ECR — Assurez-vous que l'URI du référentiel Amazon ECR qui héberge GuardDuty l'agent 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 du téléchargement du conteneur par Fargate, consultez GuardDuty la section Utilisation d'Amazon ECR avec Amazon ECS dans le manuel Amazon Elastic Container Service Developer Guide.

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, assurez-vous que la politique ne refuse pas l'autorisation`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 des SCP pour votre organisation, voir Politiques de contrôle des services (SCP).

Limites de processeur et de mémoire

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

Valeur d'UC	Valeur de mémoire	GuardDuty limite de mémoire maximale de l'agent
256 (0,25 vCPU)	512 MiB, 1 Go, 2 Go	128 Mo
512 (0,5 vCPU)	1 Go, 2 Go, 3 Go, 4 Go	
1 024 (1 vCPU)	2 GO, 3 GO, 4 GO	
	5 GO, 6 GO, 7 GO, 8 GO	
2 048 (2 vCPU)	Entre 4 Go et 16 Go par incréments de 1 Go	
4 096 (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 cluster Amazon ECS.

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 clusters Amazon EKS

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 clusters EKS.

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 l'architecture du processeur affectent 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 d'EKS Runtime Monitoring.

Distribution du système d'exploitation	Version de noyau	Support du noyau	Architecture du processeur		Version de Kubernetes prise en charge
			64 bits (AMD64)	Graviton (ARM64) (Graviton2 et versions ultérieures) [1]	
Ubuntu AL2 AL 2023 [3]	5,4, 5,10, 5,15, 6,1 [2]	Points de trace eBPF, sonde K	Pris en charge	Pris en charge	V1.21 - V1.29
Bottlerocket					V1.23 - V1.29

1. La surveillance du temps d'exécution pour les clusters Amazon EKS ne prend pas en charge les instances Graviton de première génération telles que les types d'instances A1.
2. Actuellement, avec la version du noyau`6.1`, je ne GuardDuty peux pas générer Types de recherche liés à la surveillance du temps ceux qui sont liés àÉvénements DNS.
3. Runtime Monitoring prend en charge la norme AL2023 avec la sortie de l'agent de GuardDuty sécurité v1.6.0 et versions ultérieures. Pour plus d'informations, consultez GuardDuty agent de sécurité pour les clusters Amazon EKS.

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

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

Version de Kubernetes	Version de l'agent GuardDuty de sécurité complémentaire Amazon EKS									
	v1.6.1	v1.6.0	v1.5.0	v1.4.1	v1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1,29	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
1,28						Pris en charge	Pris en charge			
1,27								Pris en charge		
1,26									Pris en charge	
1,25										Pris en charge
1,24										
1,23										
1,22										
1,21										

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 clusters Amazon EKS.

Limites de processeur et de mémoire

Le tableau suivant indique les limites de processeur et de mémoire pour le module complémentaire Amazon EKS 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 module complémentaire Amazon EKS version 1.5.0 ou supérieure, il GuardDuty permet de configurer le schéma du module complémentaire pour les valeurs de votre processeur et de votre mémoire. Pour plus d'informations sur la plage configurable, consultezParamètres et valeurs configurables.

Une fois que vous avez activé la surveillance d'exécution EKS et évalué l'état de couverture de vos clusters EKS, vous pouvez configurer et consulter les métriques d'aperçu des conteneurs. Pour plus d'informations, consultez Configuration de la surveillance du processeur et 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 GuardDuty.

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

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

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 instance Amazon EC2, un cluster Amazon ECS ou un cluster Amazon EKS), 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'instance Amazon EC2

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

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

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

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

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 instance Amazon EC2, vous pouvez installer et utiliser l'agent sur l'hôte sous-jacent au sein d'un cluster Amazon EKS. Si vous avez déjà déployé un agent de sécurité sur ce cluster EKS, 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 d'un VPC partagé 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 VPC partagé pour Comptes AWS les personnes appartenant à la même organisation dans. AWS Organizations En votre nom, GuardDuty vous pouvez définir la politique relative aux points de terminaison Amazon VPC en fonction des détails associés au VPC partagé pour votre organisation.

Avant cette version, l'utilisation de VPC partagés était GuardDuty prise en charge uniquement lorsque vous choisissiez de gérer l'agent GuardDuty de sécurité manuellement.

Table des matières

Comment ça marche

Lorsque le compte propriétaire du VPC partagé 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)), tous les VPC partagés sont éligibles à l'installation automatique du point de terminaison Amazon VPC partagé et du groupe de sécurité associé dans le compte propriétaire du VPC partagé. GuardDuty récupère l'ID d'organisation associé à l'Amazon VPC partagé.

Désormais, ceux Comptes AWS qui appartiennent à la même organisation que le compte propriétaire Amazon VPC partagé peuvent également partager le même point de terminaison Amazon VPC. GuardDuty crée le VPC partagé lorsque le compte propriétaire du VPC partagé ou le compte participant a besoin d'un point de terminaison Amazon VPC. Parmi les exemples de besoin d'un point de terminaison Amazon VPC, citons l'activation GuardDuty, la surveillance du temps d'exécution, la surveillance du temps d'exécution EKS 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 terminaison Amazon VPC et définissent la politique du point de terminaison avec le même identifiant d'organisation que celui du compte propriétaire du VPC partagé. GuardDuty ajoute une `GuardDutyManaged` balise et lui attribue la valeur `true` pour le point de terminaison Amazon VPC qui GuardDuty le crée. Si le compte propriétaire Amazon VPC partagé n'a pas activé la surveillance du temps d'exécution ou la configuration automatique des agents pour aucune des ressources, il ne GuardDuty définira pas la politique relative aux points de terminaison Amazon VPC. 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 propriétaire du VPC partagé, consultez. Activer la surveillance du GuardDuty temps d'exécution

Chacun des comptes utilisant la même politique de point de terminaison Amazon VPC est appelé AWS compte participant du Amazon VPC partagé associé.

L'exemple suivant montre la politique de point de terminaison VPC par défaut du compte propriétaire du VPC partagé et du compte participant. Le `aws:PrincipalOrgID` affichera l'ID d'organisation associé à la ressource VPC 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 d'un VPC partagé

Conditions préalables à la configuration initiale

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

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 ressource VPC partagée — Vous pouvez créer une ressource VPC partagée à partir du compte du propriétaire. Pour plus d'informations, consultez Partager votre VPC avec d'autres comptes dans le Guide de l'utilisateur Amazon VPC.

Prérequis spécifiques à la surveillance du temps d' GuardDutyexécution

La liste suivante fournit les prérequis spécifiques à GuardDuty :

- Le compte propriétaire du VPC partagé et le 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 terminaison Amazon VPC

et un groupe de sécurité pour le VPC partagé. Pour plus d'informations sur le fonctionnement des VPC partagés, consultez Partager votre VPC avec d'autres comptes dans le guide de l'utilisateur Amazon VPC.

- Activez la surveillance du temps d'exécution ou la surveillance du temps d'exécution EKS, ainsi que la configuration GuardDuty automatique des agents pour toutes les ressources du compte propriétaire du VPC partagé et du compte participant. Pour plus d’informations, consultez 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 ressource VPC partagée associée au compte propriétaire et de sélectionner ses sous-réseaux.

Questions fréquemment posées (FAQ)

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

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

Pour plus d'informations sur les conditions requises pour créer un VPC partagé, consultez. Prérequis

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

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

En tant que propriétaire d'un VPC partagé, je souhaite que la politique de point de terminaison VPC 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 terminaison du VPC partagé.

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

Pourquoi le point de terminaison VPC partagé passe-t-il de à **`aws:PrincipalAccount`** ? **`aws:PrincipalOrgId`** Comment puis-je empêcher 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 terminaison VPC partagé. Cela empêche toute GuardDuty tentative de modification ou de remplacement de la politique de point de terminaison du VPC partagé.

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

Lorsque le compte propriétaire du VPC partagé désactive le Runtime Monitoring (GuardDuty ou EKS Runtime Monitoring), GuardDuty vérifie si un type de ressource appartenant au compte participant a utilisé le point de terminaison VPC 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 terminaison VPC et le groupe de sécurité GuardDuty ne seront pas supprimés.

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

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

En tant que compte propriétaire d'un VPC partagé, vous pouvez supprimer la ressource VPC 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 VPC partagé et sur la compréhension de son impact, consultez. To delete a VPC endpoint

Gestion des agents de sécurité doubles installés sur un hôte

Les instances Amazon EC2 peuvent prendre en charge plusieurs types de charges de travail. Lorsque vous configurez un agent de sécurité automatique sur une instance Amazon EC2, la même instance EC2 peut avoir un autre agent de sécurité via EKS.

Présentation

Imaginons un scénario dans lequel vous avez activé la surveillance du temps d'exécution. Vous pouvez désormais activer l'agent automatisé pour Amazon EKS via GuardDuty. Vous avez également activé l'agent automatique pour Amazon EC2. 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 Amazon EC2. 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, il est possible que votre compte ait besoin de deux fois plus de processeur et de mémoire. Pour plus d'informations sur les limites de processeur 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 instance EC2 entre dans le champ d'application des agents de sécurité Amazon EKS et Amazon EC2, l'agent de sécurité EKS est prioritaire. Cela ne s'applique que lorsque vous utilisez l'agent de sécurité v1.1.0 ou supérieur pour Amazon EC2. 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 instance Amazon EC2 est également gérée par SSM, 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 à EC2 et à EKS s'exécutent en même temps, GuardDuty cela peut générer des résultats dupliqués uniquement pendant la période de chevauchement.

  Cela peut se produire lorsque :

  - Les agents de sécurité pour EC2 et EKS sont configurés via GuardDuty (automatiquement), ou
  - Votre ressource Amazon EKS dispose d'un agent de sécurité automatisé.
- Lorsque l'agent de sécurité EKS est déjà en cours d'exécution, si vous déployez l'agent de sécurité EC2 manuellement sur le 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'instance Amazon EC2

> **Note**
>
> Avant de continuer, assurez-vous de suivre toutes lesConditions préalables à la prise en charge des instances Amazon EC2.

Migration d'un agent manuel Amazon EC2 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 l'association SSM

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

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

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

  Pour GuardDuty empêcher l'installation et la gestion de l'agent de sécurité, supprimez la balise d'inclusion de ces instances EC2. Pour plus d'informations, consultez la section Ajouter et supprimer des balises dans le guide de l'utilisateur Amazon EC2.
- Balises d'exclusion : lorsque vous souhaitez activer la configuration GuardDuty automatique des agents pour toutes les instances EC2 de votre compte, assurez-vous qu'aucune instance EC2 n'est étiquetée avec 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 section EC2, choisissez Enable.
5. Choisissez Enregistrer.
6. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gérera l'agent de sécurité sur toutes les ressources EC2 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 Targets pour l'association SSM (`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 instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 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'association SSM GuardDuty créée installera et gérera l'agent de sécurité uniquement sur les ressources EC2 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 Targets pour l'association SSM 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 instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

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

1. Connectez-vous à la console Amazon EC2 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 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'instance Amazon EC2.

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 section EC2, sélectionnez Activer pour tous les comptes.
- Option 2
  - Sous Configuration automatique de l'agent, dans la section EC2, sélectionnez Configurer les comptes manuellement.
  - Sous Administrateur délégué (ce compte), choisissez Activer.
- Choisissez 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 section EC2, sélectionnez Configurer les comptes manuellement.
- Sous Administrateur délégué (ce compte), choisissez Activer.
- Choisissez 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'association SSM GuardDuty créée installera et gérera l'agent de sécurité sur toutes les ressources EC2 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 Targets pour l'association SSM (`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 instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 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 EC2 sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.
3. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gérera l'agent de sécurité uniquement sur les ressources EC2 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 Targets pour l'association SSM 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 instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 lancée sans balise d'exclusion sera couverte par la configuration GuardDuty automatique des agents.

Pour configurer GuardDuty l'agent pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 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'instance Amazon EC2.

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 de l'agent pour Amazon EC2.

2. Vous pouvez vérifier que l'association SSM qui GuardDuty crée (`GuardDutyRuntimeMonitoring-do-not-delete`) installera et gérera l'agent de sécurité sur toutes les ressources EC2 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 Targets pour l'association SSM. Notez que la touche Tag apparaît sous la forme InstanceIds.

Using inclusion tag in selected instances

Pour configurer GuardDuty l'agent pour certaines instances Amazon EC2

1. Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `true` balise `GuardDutyManaged` : aux instances EC2 que vous GuardDuty souhaitez 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 EC2 sélectionnées. Il n'est pas nécessaire d'activer explicitement la configuration automatique des agents.
3. Vous pouvez vérifier que l'association SSM GuardDuty créée installera et gérera l'agent de sécurité sur toutes les ressources EC2 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 Targets pour l'association SSM (`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 instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour

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

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

1. Connectez-vous à la console Amazon EC2 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'instance Amazon EC2.

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 ressource Amazon EC2 afin de l'activer automatiquement 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 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 instances Amazon EC2 qui appartiennent à ce nouveau compte membre, assurez-vous que toutes les conditions préalables sont rempliesPour instance EC2.

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

- Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
- Ouvrez l'onglet Targets pour l'association SSM. 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 console Amazon EC2 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'association SSM GuardDuty créée installera et gérera l'agent de sécurité uniquement sur les ressources EC2 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 Targets pour l'association SSM 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 instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 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 console Amazon EC2 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'instance Amazon EC2.

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 console Amazon EC2 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 instances Amazon EC2 balisées. 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 instances Amazon EC2 avant de les lancer. Une fois que vous avez activé la configuration automatique des agents pour Amazon EC2, toute instance EC2 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 console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ec2/.
2. Ajoutez la `false` balise `GuardDutyManaged` : aux instances EC2 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'instance Amazon EC2.

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

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 instances Amazon EC2.

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

Création manuelle d'un point de terminaison Amazon VPC

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

> **Note**
>
> L'utilisation du point de terminaison VPC n'entraîne aucun coût supplémentaire.

Pour créer un point de terminaison Amazon VPC

1. Connectez-vous à la console Amazon VPC AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous Cloud privé VPC, 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`* par votre. Région AWS Il doit s'agir de la même région que l'instance Amazon EC2 associée à votre identifiant de AWS compte.
6. Choisissez Vérifier le service.
7. Une fois le nom du service vérifié avec succès, choisissez le VPC dans lequel réside votre instance. Ajoutez la politique suivante pour limiter l'utilisation des points de terminaison Amazon VPC 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 la prise en charge des points de terminaison Amazon VPC à des identifiants de compte spécifiques de votre organisation, consultez. Organization 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'ID de compte `aws:PrincipalAccount` doit correspondre au compte contenant le VPC et le point de terminaison d'un VPC. La liste suivante indique comment partager le point de terminaison VPC avec d'autres identifiants de AWS compte :

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

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

  Assurez-vous de remplacer les identifiants de AWS compte par les identifiants de compte des comptes qui doivent accéder au point de terminaison du VPC.

- Pour autoriser tous les membres d'une organisation à accéder au point de terminaison VPC, remplacez-le `"aws:PrincipalAccount: "111122223333"` par la ligne suivante :

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

  Assurez-vous de remplacer l'organisation *o-abcdef0123* par votre identifiant d'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` dans le Guide de l'utilisateur IAM.

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

8. Sous Paramètres supplémentaires, choisissez Activer le nom DNS.
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 instance Amazon EC2). 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'utilisateur Amazon EC2.

    En cas de problème lors de la restriction des autorisations entrantes sur 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 instances Amazon EC2 :

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

Méthode 1 - En utilisant AWS Systems Manager

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

AWS Systems Manager instance Amazon EC2 gérée

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

- 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 instances Amazon EC2 avec AWS Systems Manager, consultez la section Configuration de Systems Manager pour les instances Amazon EC2 dans AWS Systems Manager le guide de 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 AWS Systems Manager le guide de l'utilisateur.

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

Pour installer l' GuardDuty agent pour l'instance Amazon EC2 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 instances Amazon EC2.

6. Sélectionnez l'instance Amazon EC2 ciblée. Vous pouvez sélectionner une ou plusieurs instances Amazon EC2. 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 plus d'informations, consultez 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 des scripts RPM ou des scripts Debian. En fonction des systèmes d'exploitation, vous pouvez choisir une méthode préférée :

- Utilisez des scripts RPM pour installer l'agent de sécurité sur les distributions du système d'exploitation AL2 ou AL2023.
- 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 signature RPM de l'agent de GuardDuty sécurité avant de l'installer sur votre machine.

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

a. Préparez le modèle

Préparez les commandes avec la clé publique appropriée, la signature du fichier x86_64 tr/min, la signature du fichier arm64 tr/min et le lien d'accès correspondant aux scripts RPM 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 scripts RPM.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
publickey.pem
```

- GuardDuty signature RPM de l'agent de sécurité :

  Signature de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/
amazon-guardduty-agent-1.2.0.x86_64.sig
```

  Signature d'arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/
amazon-guardduty-agent-1.2.0.arm64.sig
```

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

  Lien d'accès pour x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/
amazon-guardduty-agent-1.2.0.x86_64.rpm
```

  Lien d'accès pour arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/
amazon-guardduty-agent-1.2.0.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 (EAU)	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 du fichier x86_64 tr/min, la signature du fichier arm64 tr/min et le lien d'accès correspondant aux scripts RPM hébergés dans les compartiments Amazon S3, assurez-vous de remplacer l'ID de compte par l'identifiant approprié Compte AWS et la région par votre région actuelle.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
x86_64/amazon-guardduty-agent-1.2.0.x86_64.rpm ./amazon-guardduty-
agent-1.2.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
x86_64/amazon-guardduty-agent-1.2.0.x86_64.sig ./amazon-guardduty-
agent-1.2.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/
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 indique que l'importation est réussie

```
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-1.2.0.x86_64.sig amazon-guardduty-
agent-1.2.0.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 de RPM.

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 sur 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 via 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-1.2.0.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, l'ID de AWS compte et la version de l' GuardDuty agent pour accéder aux scripts des paquets Debian.

   - Clé publique :

   ```
   s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/
   publickey.pem
   ```

   - GuardDuty Signature de l'agent de sécurité Debian :

Signature d'amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/amd64/
amazon-guardduty-agent-1.2.0.amd64.sig
```

Signature d'arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/
amazon-guardduty-agent-1.2.0.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/1.2.0/amd64/
  amazon-guardduty-agent-1.2.0.amd64.deb
  ```

  Lien d'accès pour arm64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/
  amazon-guardduty-agent-1.2.0.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 (EAU)	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, 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/1.2.0/
amd64/amazon-guardduty-agent-1.2.0.amd64.deb ./amazon-guardduty-
agent-1.2.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/
amd64/amazon-guardduty-agent-1.2.0.amd64.sig ./amazon-guardduty-
agent-1.2.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/
publickey.pem ./publickey.pem
```

c. Importer la clé publique dans la base de données

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

gpg indique que l'importation est réussie

```
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-1.2.0.amd64.sig amazon-guardduty-
agent-1.2.0.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 via 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-1.2.0.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 manuelle de l'agent de GuardDuty sécurité pour Amazon EC2, consultez. Résolution 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 via 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, procédez comme suit`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 ressources Amazon EC2. 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 instances Amazon EC2 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 instances Amazon EC2 ciblées est supprimé.

   Pour supprimer la configuration du point de terminaison Amazon VPC, vous devez désactiver à la fois la surveillance du temps d'exécution et la surveillance du temps d'exécution Amazon EKS.

Méthode 2 - En utilisant les gestionnaires de packages Linux

1. Connectez-vous via SSH depuis Linux ou macOS.
2. Commande de désinstallation

   La commande suivante permet de désinstaller l'agent de GuardDuty sécurité de l'instance Amazon EC2 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 terminaison Amazon VPC

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 terminaison Amazon VPC créé manuellement ()Création manuelle d'un point de terminaison Amazon VPC.

Pour supprimer le point de terminaison Amazon VPC à l'aide de la console

1. Ouvrez la console Amazon VPC 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, Delete VPC endpoints (Supprimer le point de terminaison de VPC).
5. À l'invite de confirmation, saisissez **`delete`**.
6. Sélectionnez Delete (Supprimer).

Pour supprimer le point de terminaison Amazon VPC 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 ECS uniquement)

Configuration de GuardDuty l'agent pour un compte autonome

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

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 clusters Amazon ECS (au niveau du compte)

      Choisissez Activer dans la section Configuration automatique de l'agent pour AWS Fargate (ECS uniquement). Lorsqu'une nouvelle tâche Fargate Amazon ECS est GuardDuty lancée, il gère le déploiement de l'agent de sécurité.

      - Choisissez Enregistrer.

b. Pour gérer la configuration automatisée des agents en excluant certains clusters Amazon ECS (au niveau du cluster)

   i. Ajoutez une balise au cluster Amazon ECS pour lequel 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 cluster Amazon ECS 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 cluster Amazon ECS correspondant.

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

iv. Choisissez Enregistrer.

c. Pour gérer la configuration automatisée des agents en incluant certains clusters Amazon ECS (au niveau du cluster)

i. Ajoutez une balise à un cluster Amazon ECS 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
                }
            }
        }
    ]
}
```

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 membres, et gérer la configuration automatique des agents pour les clusters Amazon ECS 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 tâches Amazon ECS 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 Enregistrer.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS 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 clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

   Dans l'onglet Configuration, choisissez Activer dans la configuration de l'agent automatisé.

   Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

6. Choisissez Enregistrer.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un cluster Amazon ECS 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 clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement l' GuardDuty agent par le biais de la configuration automatique de l'agent.

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 tâches Amazon ECS lancées.
2. Choisissez Enregistrer.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS 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 clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

   Dans l'onglet Configuration, choisissez Modifier.
6. Choisissez Activer pour tous les comptes dans la section Configuration automatique de l'agent.

Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.

7. Choisissez Enregistrer.

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 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 clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la gestion automatique des GuardDuty agents.

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 Configuration automatique de l'agent, dans la section Comptes membres actifs, sélectionnez Actions.
3. Dans Actions, choisissez Activer pour tous les comptes membres actifs existants.
4. Choisissez Confirmer.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS 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 clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS 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 clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.
7. Choisissez Confirmer.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un cluster Amazon ECS 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 clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

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 Enregistrer.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS 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 clusters Amazon ECS avant d'activer la configuration automatique des agents pour votre compte ; sinon GuardDuty , le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

   Dans l'onglet Configuration, sélectionnez Activer automatiquement pour les nouveaux comptes membres dans la section Configuration automatique de l'agent.

   Pour les clusters Amazon ECS qui n'ont pas été exclus, il GuardDuty gérera le déploiement de l'agent de sécurité dans le conteneur annexe.
6. Choisissez Enregistrer.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Ajoutez une balise à un cluster Amazon ECS 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 clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

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-Automated (ECS-Fargate). 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 automatique de l'agent Runtime Monitoring-Automated (ECS-Fargate).
3. Choisissez Confirmer.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Ajoutez une balise à ce cluster Amazon ECS 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 clusters Amazon ECS avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon GuardDuty, le conteneur annexe sera attaché à tous les conteneurs des tâches Amazon ECS lancées.

   Sur la page Comptes, sélectionnez les comptes pour lesquels vous souhaitez activer la configuration automatique de l'agent Runtime Monitoring-Automated (ECS-Fargate). Vous pouvez sélectionner plusieurs comptes. Assurez-vous que les comptes que vous sélectionnez à cette étape sont déjà activés avec Runtime Monitoring.

   Pour les clusters Amazon ECS qui n'ont pas été exclus, il 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 automatique de l'agent Runtime Monitoring-Automated (ECS-Fargate).
7. Choisissez Enregistrer.

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 clusters Amazon ECS que vous souhaitez surveiller.
2. Ajoutez une balise à un cluster Amazon ECS 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 clusters Amazon ECS, vous n'avez pas besoin d'activer explicitement la configuration automatisée des agents.

Gestion automatique de l'agent de sécurité pour les clusters Amazon EKS

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 (Surveiller tous les clusters EKS)	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 clusters EKS existants et potentiellement nouveaux de votre compte. 2. Choisissez Enregistrer.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (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 cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDuty Managed` . • Remplacez *123456789012* par l' Compte AWS ID 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"]` 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 clusters EKS avant d'activer la gestion automatique des GuardDuty agents pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. 5. Dans l'onglet Configuration, choisissez Activer dans la section de gestion des GuardDuty agents. Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité. 6. Choisissez Enregistrer.

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	Pour exclure un cluster EKS de la surveillance une fois que l'agent de GuardDuty sécurité a déjà été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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 cluster EKS. 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` .

Approche préférée pour déployer l'agent GuardDuty de sécurité	Étapes
	• Remplacez *123456789012* par l' Compte AWS ID 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. Pour arrêter de recevoir les événements d'exécuti on de ce cluster, vous devez supprimer l'agent de sécurité déployé de ce cluster EKS. 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
Surveiller des clusters EKS 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 cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `true`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés 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`* par `eks:TagResource` . • Remplacez *`ec2 : DeleteTags`* par `eks:UntagResource` . • Remplacez *`access-project`* par `GuardDutyManaged` . • Remplacez *`123456789012`* par l' Compte AWS ID 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 Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

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 clusters EKS appartenant aux comptes membres de leur 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. 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 (Surveiller tous les clusters EKS)	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 clusters EKS appartenant au compte de compte d' GuardDuty administrateur délégué ainsi que pour tous les clusters EKS 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 Enregistrer.
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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` par `pareks:TagResource` . • Remplacez `ec2 : DeleteTags` par `pareks:UntagResource` . • Remplacez `access-project par` `GuardDutyManaged` . • Remplacez `123456789012` par l' Compte AWS ID 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 clusters EKS avant d'activer la gestion automatique des GuardDuty

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	agents pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. 5. Dans l'onglet Configuration, choisissez Activer dans la section de gestion des GuardDuty agents. Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité. 6. Choisissez Enregistrer. Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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* pareks:TagResource . • Remplacez *ec2 : DeleteTags* pareks:Untag Resource . • Remplacez *access-project par* GuardDutyManaged .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes

- Remplacez *123456789012* par l' Compte AWS ID 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. Si vous avez activé l'agent automatique pour ce cluster EKS, 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 cluster EKS. 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 cluster EKS. 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 cluster EKS, consultezImpact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS 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 clusters EKS 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 Enregistrer. 3. Ajoutez une balise à votre cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `true`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés 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* pareks:TagResource . • Remplacez *ec2 : DeleteTags* pareks:Untag Resource . • Remplacez *access-project par* GuardDutyManaged . • Remplacez *123456789012* par l' Compte AWS ID 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 clusters EKS. 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 Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

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 (Surveiller tous les clusters EKS)	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 clusters EKS appartena nt au compte de compte d' GuardDuty administrateur délégué ainsi que pour tous les clusters EKS appartenant à tous les comptes membres existants et potentiellement nouveaux de l'organisation. 2. Choisissez Enregistrer.
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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* pareks:TagResource .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes

- Remplacez *ec2 : DeleteTags* par `pareks:Untag Resource` .
- Remplacez *access-project par* `GuardDutyManaged` .
- Remplacez *123456789012* par l' Compte AWS ID 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 clusters EKS avant d'activer l'agent automatisé pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS 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 clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.
7. Choisissez Enregistrer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 2. Si la configuration automatique de l'agent est activée pour ce cluster EKS, 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 cluster EKS. 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 cluster EKS. 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* pareks:TagResource . • Remplacez *ec2 : DeleteTags* pareks:Untag Resource . • Remplacez *access-project par* GuardDutyManaged .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	• Remplacez *123456789012* par l' Compte AWS ID 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"]` 4. Si vous gériez manuellement l'agent de GuardDuty sécurité pour ce cluster EKS, consultezImpact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS 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 clusters EKS 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 Enregistrer. 3. Ajoutez une balise à votre cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `true`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés 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* pareks:TagResource . • Remplacez *ec2 : DeleteTags* pareks:Untag Resource . • Remplacez *access-project par* GuardDutyManaged . • Remplacez *123456789012* par l' Compte AWS ID 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 clusters EKS. 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 Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

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 clusters EKS appartenant aux comptes de membres actifs existants de l'organisation, vous devez choisir une approche préférée pour gérer l'agent de GuardDuty sécurité pour ces clusters EKS. 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 (Surveiller tous les clusters EKS)	Pour surveiller tous les clusters EKS pour tous les comptes 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
Surveiller tous les clusters EKS, mais en exclure certains (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 cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDuty Managed` . • Remplacez *123456789012* par l' Compte AWS ID 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"]` 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 clusters EKS avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. 5. Sous l'onglet Configuration, dans le volet Configura tion automatique de l'agent, sous Comptes membres actifs, sélectionnez Actions. 6. Dans Actions, choisissez Activer pour tous les comptes membres actifs. 7. Choisissez Confirmer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Pour exclure un cluster EKS de la surveillance une fois que l'agent de GuardDuty sécurité a déjà été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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 cluster EKS. 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	• Remplacez *123456789012* par l' Compte AWS ID 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. 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 cluster EKS. 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
Surveiller des clusters EKS 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 cluster EKS 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 l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDuty Managed` . • Remplacez *123456789012* par l' Compte AWS ID 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 Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

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 (Surveiller tous les clusters EKS)	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 Enregistrer.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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* pareks:TagResource . • Remplacez *ec2 : DeleteTags* pareks:UntagResource . • Remplacez *access-project par* GuardDuty Managed . • Remplacez *123456789012* par l' Compte AWS ID de l'entité de confiance. Lorsque vous avez plusieurs entités approuvée s, 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 clusters EKS avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. 5. Dans l'onglet Configuration, sélectionnez Activer automatiquement les nouveaux comptes membres dans la section Gestion des GuardDuty agents. Pour les clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité. 6. Choisissez Enregistrer. Pour exclure un cluster EKS 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 cluster EKS avec la clé as `GuardDutyManaged` et sa valeur as`false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). Si l'agent automatisé est activé pour ce cluster EKS, 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 cluster EKS. 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 cluster EKS. 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` `pareks:TagResource` . • Remplacez `ec2 : DeleteTags` `pareks:UntagResource` .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	• Remplacez *access-project par* GuardDuty Managed . • Remplacez *123456789012* par l' Compte AWS ID 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 cluster EKS, consultezImpact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS 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 clusters EKS 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 Enregistrer. 3. Ajoutez une balise à votre cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `true`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). GuardDuty gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS sélectionnés 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* pareks:TagResource .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	• Remplacez `ec2 : DeleteTags` par `pareks:Untag Resource` . • Remplacez `access-project par` `GuardDuty Managed` . • Remplacez `123456789012` par l' Compte AWS ID 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 clusters EKS. 1. Assurez-vous de décocher la case Activer automatiq uement pour les nouveaux comptes membres dans la section Configuration automatique des agents. Conservez la configuration de surveillance du temps d'exécution identique à celle configurée à l'étape précédente. 2. Choisissez Enregistrer. 3. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

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 (Surveiller tous les clusters EKS)	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 d'exécution EKS 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 Runtime Monitoring - Configuration automatisée des agents. 3. Choisissez Confirmer.
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide de balises d'exclusion)	Dans les procédures suivantes, choisissez l'un des scénarios qui s'appliquent à vous. Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité n'a pas été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). 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* pareks:TagResource .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes

- Remplacez *ec2 : DeleteTags* par `pareks:Untag Resource` .
- Remplacez *access-project par* `GuardDutyManaged` .
- Remplacez *123456789012* par l' Compte AWS ID 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/.

   > **Note**
   >
   > Ajoutez toujours la balise d'exclusion à vos clusters EKS avant d'activer la configuration automatique de l'agent pour votre compte ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS 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 clusters EKS qui n'ont pas été exclus de la surveillance, il GuardDuty gérera le déploiement et les mises à jour de l'agent GuardDuty de sécurité.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	6. Choisissez Enregistrer. Pour exclure un cluster EKS de la surveillance lorsque l'agent GuardDuty de sécurité a été déployé sur ce cluster 1. Ajoutez une balise à ce cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `false`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). Si la configuration automatique de l'agent était précédemment activée pour ce cluster EKS, l'agent de sécurité de 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 cluster EKS. 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 cluster EKS. 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` par `eks:TagResource` . • Remplacez `ec2 : DeleteTags` par `eks:Untag Resource` .

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	• Remplacez *access-project par* GuardDutyManaged . • Remplacez *123456789012* par l' Compte AWS ID 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. Si vous gériez manuellement l'agent de GuardDuty sécurité pour ce cluster EKS, vous devez le supprimer. Pour plus d'informations, consultez Impact de la désactivation et du nettoyage des ressources.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
Surveiller des clusters EKS 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 clusters EKS appartenant aux comptes sélectionnés : 1. Assurez-vous de ne pas activer la configuration automatique de l'agent Runtime Monitoring pour les comptes sélectionnés dotés des clusters EKS que vous souhaitez surveiller. 2. Ajoutez une balise à votre cluster EKS avec la clé en tant que `GuardDutyManaged` et sa valeur en tant que `true`. Pour plus d'informations sur l'étiquetage de votre cluster Amazon EKS, veuillez consulter Gestion des balises à l'aide de la console dans le Guide de l'utilisateur Amazon EKS (langue française non garantie). Après avoir ajouté la balise, GuardDuty il gérera le déploiement et les mises à jour de l'agent de sécurité pour les clusters EKS 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* pareks:TagResource . • Remplacez *ec2 : DeleteTags* pareks:Untag Resource . • Remplacez *access-project par* GuardDutyManaged . • Remplacez *123456789012* par l' Compte AWS ID 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	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 cluster Amazon EKS.

Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS

Cette section décrit comment vous pouvez gérer votre agent complémentaire Amazon EKS (GuardDuty agent) après avoir activé la surveillance du temps d'exécution. Pour utiliser Runtime Monitoring, vous devez activer Runtime Monitoring et configurer le module complémentaire Amazon EKS,`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 clusters EKS. Avant de continuer, assurez-vous d'avoir déjà configuré la surveillance du temps d'exécution pour vos comptes. L'agent GuardDuty de sécurité (module complémentaire EKS) ne fonctionnera pas si vous ne configurez pas la surveillance du temps d'exécution. Pour plus d’informations, consultez 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 terminaison Amazon VPC.

Console

Créer un point de terminaison d'un VPC

1. Ouvrez la console Amazon VPC 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`* par la bonne région. Il doit s'agir de la même région que le cluster EKS qui appartient à votre Compte AWS identifiant.
6. Choisissez Vérifier le service.
7. Une fois le nom du service vérifié, choisissez le VPC dans lequel réside votre cluster. Ajoutez la stratégie suivante pour limiter l'utilisation de point de terminaison d'un VPC 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 prise en charge des points de terminaison d'un VPC à des identifiants de compte spécifiques de votre organisation, veuillez consulter Organization 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'ID de compte `aws:PrincipalAccount` doit correspondre au compte contenant le VPC et le point de terminaison d'un VPC. La liste suivante indique comment partager le point de terminaison d'un VPC avec d'autres ID Compte AWS :

Condition d'organisation pour restreindre l'accès à votre point de terminaison

- Pour spécifier plusieurs comptes afin d'accéder au point de terminaison d'un VPC, remplacez `"aws:PrincipalAccount": "111122223333"` par ce qui suit :

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

- Pour autoriser tous les membres d'une organisation à accéder au point de terminaison d'un VPC, remplacez `"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 le nom DNS.
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 cluster EKS). 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 sur votre VPC (ou 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`* par la bonne région. Il doit s'agir de la même région que le cluster EKS qui appartient à votre Compte AWS identifiant.
  - Pour DNSOptions, activez l'option DNS privé en la définissant sur `true`.
- Pour AWS Command Line Interface, voir create-vpc-endpoint.

Configuration des 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 Amazon EKS. 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 clusters Amazon EKS.

Pourquoi dois-je mettre à jour le schéma de configuration de l'agent de sécurité

Le schéma de configuration de l'agent GuardDuty de sécurité est le même pour tous les conteneurs de vos clusters Amazon EKS. Lorsque les valeurs par défaut ne correspondent pas aux charges de travail et à la taille de l'instance associées, envisagez de configurer les paramètres du processeur`PriorityClass`, les paramètres de mémoire et `dnsPolicy` les paramètres. Quelle que soit la façon dont vous gérez l' GuardDuty agent pour vos clusters Amazon EKS, 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 (module complémentaire EKS) en votre nom, il met à jour le module complémentaire en fonction des 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 pour ResolveConflicts est. None

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 module complémentaire Amazon EKS manuellement ou pour mettre à jour les paramètres du module complémentaire existant.

Réglages du processeur

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	1 024 milles	

Paramètres **PriorityClass**

Lorsque vous GuardDuty créez un module complémentaire Amazon EKS pour vous, le module attribué `PriorityClass` est`aws-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 politique DNS 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 politique DNS 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 clusters EKS 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 (module complémentaire EKS) 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 console Amazon EKS 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 module complémentaire EKS 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 console Amazon EKS. L'état de votre module complémentaire EKS doit être passé à Prêt à installer.
8. (Facultatif) Fourniture du schéma de configuration du module complémentaire EKS

   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, consultezConfiguration des paramètres du module complémentaire EKS.

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 dansConfiguration des paramètres du module complémentaire EKS.

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 ResolveConflicts dans le manuel Amazon EKS API Reference.

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 de module complémentaire Amazon EKS (`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 plus d’informations, consultez Configuration des paramètres du module complémentaire EKS.

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 être informé des nouvelles versions de l'agent, vous pouvez vous abonner à un flux RSS surGuardDuty 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 clusters Amazon EKS.

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 plus d'informations, consultez Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty .

Console

1. Ouvrez la console Amazon EKS 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 module complémentaire EKS 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 dansConfiguration des paramètres du module complémentaire EKS.

   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 ResolveConflicts dans le manuel Amazon EKS API Reference.

API/CLI

Pour mettre à jour l'agent GuardDuty de sécurité pour vos clusters Amazon EKS, consultez la section Mise à jour d'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, consultezConfiguration des paramètres du module complémentaire EKS.

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 module complémentaire Amazon EKS 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 plus d'informations, consultez 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 console Amazon EKS 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 Vue brute pour afficher la réponse JSON non formatée. 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 clusters Amazon EKS. Pour plus d'informations, consultez Couverture pour les clusters Amazon EKS.

Configuration de la surveillance du temps d'exécution EKS (API uniquement)

Avant de configurer la surveillance d'exécution EKS 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 EKS Runtime Monitoring dans Runtime Monitoring. GuardDuty recommande Vérification de l'état de configuration de la surveillance du temps d'exécution etMigration d'EKS Runtime Monitoring vers Runtime Monitoring.

Dans le cadre de la migration vers Runtime Monitoring, assurez-vous deDésactiver la surveillance de l'exécution EKS. Ceci est important car si vous choisissez ultérieurement de désactiver la

surveillance du temps d'exécution et que vous ne désactivez pas la surveillance du temps d'exécution EKS, vous continuerez de devoir payer des frais d'utilisation pour le suivi du temps d'exécution d'EKS.

Configuration de la surveillance d'exécution EKS pour un compte autonome

Pour les comptes associés à AWS Organizations, veuillez consulter Configuration de la surveillance d'exécution EKS pour les environnements à comptes multiples.

Choisissez votre méthode d'accès préférée pour activer la surveillance d'exécution EKS 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 clusters EKS)	1. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS de votre compte. 2. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `pareks:TagResource` . • Remplacez *ec2 : DeleteTags* par `pareks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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 cluster EKS avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI L'exemple suivant active `EKS_RUNTIME_MONITORING` 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
Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `pareks:TagResource` . • Remplacez *ec2 : DeleteTags* par `pareks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS marqués avec la `true` paire `GuardDuty Managed` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 cluster Amazon EKS.

Configuration de la surveillance d'exécution EKS pour les environnements à comptes multiples

Dans les environnements à comptes multiples, seul le compte GuardDuty administrateur délégué peut activer ou désactiver EKS Runtime Monitoring pour les comptes membres et gérer la gestion des GuardDuty agents pour les clusters EKS appartenant aux comptes membres de leur 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. Pour plus d'informations sur les environnements à comptes multiples, veuillez consulter Managing multiple accounts.

Configuration de la surveillance du temps d'exécution EKS pour le compte GuardDuty administrateur délégué

Choisissez votre méthode d'accès préférée pour activer EKS Runtime Monitoring et gérer l'agent de GuardDuty sécurité pour les clusters EKS 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 clusters EKS)	Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS de votre compte.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI 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
Surveiller tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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 cluster EKS avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI L'exemple suivant active `EKS_RUNTIME_MONITORING` 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
Surveiller des clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `pareks:TagResource` . • Remplacez *ec2 : DeleteTags* par `pareks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS marqués avec la `true` paire `GuardDuty Managed` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --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 cluster Amazon EKS.

Activer automatiquement la surveillance d'exécution EKS pour tous les comptes membres

Choisissez votre méthode d'accès préférée pour activer la surveillance d'exécution EKS 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 votre approche préférée pour gérer l'agent GuardDuty de sécurité pour les clusters EKS 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 clusters EKS)	Pour activer de manière sélective la surveillance d'exécuti on EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur* . 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 clusters Amazon EKS de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au cluster EKS 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, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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`* `pareks:TagResource` . • Remplacez *`ec2 : DeleteTags`* `pareks:UntagResource` . • Remplacez *`access-project par`* `GuardDuty Managed` . • Remplacez *`123456789012`* par l' Compte AWS ID 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 cluster EKS avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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_MANAGEM ENT", "Status" : " *ENABLED*"}]]' **Note** Vous pouvez également transmettre une liste d'ID de compte 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 clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au cluster EKS 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, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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`* `pareks:TagResource` . • Remplacez *`ec2 : DeleteTags`* `pareks:UntagResource` . • Remplacez *`access-project par`* `GuardDuty Managed` . • Remplacez *`123456789012`* par l' Compte AWS ID 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 l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	`features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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 clusters Amazon EKS marqués avec la `true` paire `GuardDutyManaged` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	lors de la modification des paramètres du détecteur pour un compte, cet ID de compte est répertorié avec un résumé du problème.
Gestion manuelle de l'agent de sécurité	1. Exécutez l'API updateDetector en utilisant votre propre ID de détecteur régional et en transmettant le nom d'objet `features` en tant que `EKS_RUNTIME_MONITORING` et l'état de l'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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 cluster Amazon EKS.

Configuration de la surveillance d'exécution EKS pour tous les comptes membres actifs existants

Choisissez votre méthode d'accès préférée pour activer EKS Runtime Monitoring 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 clusters EKS)	Pour activer de manière sélective la surveillance d'exécution EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur* . 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 clusters Amazon EKS de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au cluster EKS 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, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* pareks:TagResource . • Remplacez *ec2 : DeleteTags* pareks:UntagResource . • Remplacez *access-project par* GuardDuty Managed . • Remplacez *123456789012* par l' Compte AWS ID 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 cluster EKS avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. Pour activer de manière sélective la surveillance d'exécution EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *`ID de détecteur`* . 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 clusters Amazon EKS 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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_MANAGEM ENT", "Status" : " *ENABLED*"}]]' **Note** Vous pouvez également transmettre une liste d'ID de compte 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 clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au cluster EKS 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, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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`* `pareks:TagResource` . • Remplacez *`ec2 : DeleteTags`* `pareks:UntagResource` . • Remplacez *`access-project par`* `GuardDuty Managed` . • Remplacez *`123456789012`* par l' Compte AWS ID 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 d'exécution EKS pour vos comptes membres, exécutez l'opération

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	d'API updateMemberDetectors en utilisant votre propre *ID de détecteur* . 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 clusters Amazon EKS marqués avec la `true` paire `GuardDutyManaged` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte séparés par un espace. Lorsque le code est correctement exécuté, il renvoie une liste vide de `UnprocessedAccounts` . En cas de problème

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	lors de la modification des paramètres du détecteur pour un 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 d'exécution EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur* . 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 cluster Amazon EKS.

Activer automatiquement la surveillance d'exécution EKS pour les nouveaux membres

Le compte d' GuardDuty administrateur délégué peut activer automatiquement EKS Runtime Monitoring 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 clusters EKS)	Pour activer de manière sélective la surveillance d'exécution EKS pour vos nouveaux comptes, invoquez l'opération d'API UpdateOrganizationConfiguration à l'aide de votre propre *ID de détecteur* . 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 clusters Amazon EKS de votre compte. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte séparés par un espace.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	`detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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 cluster EKS avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte. Pour activer de manière sélective la surveillance d'exécution EKS pour vos nouveaux comptes, invoquez l'opération d'API UpdateOrganization Configuration à l'aide de votre propre *`ID de détecteur`* . 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 clusters Amazon EKS 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI L'exemple suivant active à la fois `EKS_RUNTIME_MONITORING` et `EKS_ADDON_MANAGEMENT` pour un seul compte. Vous pouvez également

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	transmettre une liste d'ID de compte séparés par un espace. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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. Pour activer de manière sélective la surveillance d'exécution EKS pour vos nouveaux comptes, invoquez l'opération d'API UpdateOrganization Configuration à l'aide de votre propre *ID de détecteur* . 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 clusters Amazon EKS marqués avec la `true` paire `GuardDuty Managed` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` pour un seul compte. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	`bc2d34e56789f0 --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
Gestion manuelle de l'agent de sécurité	1. Pour activer de manière sélective la surveillance d'exécution EKS pour vos nouveaux comptes, invoquez l'opération d'API UpdateOrganization Configuration à l'aide de votre propre *ID de détecteur* . 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI L'exemple suivant active `EKS_RUNTIME_MONITORING` et désactive `EKS_ADDON_MANAGEMENT` pour un seul compte. Vous pouvez également transmettre une liste d'ID de compte séparés par un espace. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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. 2. Pour gérer l'agent de sécurité, veuillez consulter Gestion manuelle de l'agent de sécurité pour le cluster Amazon EKS.

Activer la surveillance d'exécution EKS pour les comptes 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 clusters EKS)	Pour activer de manière sélective la surveillance d'exécution EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *`ID de détecteur`* . 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 clusters Amazon EKS de votre compte.

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 tous les clusters EKS, mais en exclure certains (à l'aide d'une balise d'exclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -false`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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 cluster EKS avant de définir le paramètre `STATUS` of `EKS_RUNTIME_MONITORING` sur `ENABLED` ; sinon, l'agent de GuardDuty sécurité sera déployé sur tous les clusters EKS de votre compte.

Pour activer de manière sélective la surveillance d'exécution EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *`ID de détecteur`* .

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 clusters Amazon EKS 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 clusters EKS sélectifs (à l'aide d'une balise d'inclusion)	1. Ajoutez une balise au cluster EKS que vous souhaitez exclure de la surveillance. La paire clé-valeur est `GuardDutyManaged -true`. Pour plus d'informations sur l'ajout de la balise, veuillez consulter Gestion des identifications à l'aide de la CLI, de l'API ou de eksctl dans le Guide de l'utilisateur Amazon EKS. 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* par `eks:TagResource` . • Remplacez *ec2 : DeleteTags* par `eks:UntagResource` . • Remplacez *access-project par* `GuardDutyManaged` . • Remplacez *123456789012* par l' Compte AWS ID 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. Pour activer de manière sélective la surveillance d'exécution EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur* . 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 clusters Amazon EKS marqués avec la `true` paire `GuardDuty Managed` -. Vous pouvez également utiliser la AWS CLI commande en utilisant votre propre identifiant de détecteur régional. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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"}] ]'`

Approche préférée pour gérer les agents GuardDuty de sécurité	Étapes
	> **Note** > Vous pouvez également transmettre une liste d'ID de compte 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
Gestion manuelle de l'agent de sécurité	1. Pour activer de manière sélective la surveillance d'exécution EKS pour vos comptes membres, exécutez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur* . 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. `detectorId` Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 cluster Amazon EKS.

Migration d'EKS Runtime Monitoring vers Runtime Monitoring

Avec le lancement de GuardDuty Runtime Monitoring, la couverture de détection des menaces a été étendue aux conteneurs Amazon ECS et aux instances Amazon EC2. L'expérience d'EKS Runtime

Monitoring est désormais consolidée dans Runtime Monitoring. Vous pouvez activer la surveillance du temps d'exécution et gérer des agents de GuardDuty sécurité individuels pour chaque type de ressource (instance Amazon EC2, cluster Amazon ECS et cluster Amazon EKS) dont vous souhaitez surveiller le comportement d'exécution.

GuardDuty a consolidé l'expérience de console pour EKS Runtime Monitoring dans Runtime Monitoring. GuardDuty recommande Vérification de l'état de configuration de la surveillance du temps d'exécution etMigration d'EKS Runtime Monitoring vers Runtime Monitoring.

Dans le cadre de la migration vers Runtime Monitoring, assurez-vous deDésactiver la surveillance de l'exécution EKS. Ceci est important car si vous choisissez ultérieurement de désactiver la surveillance du temps d'exécution et que vous ne désactivez pas la surveillance du temps d'exécution EKS, vous continuerez de devoir payer des frais d'utilisation pour le suivi du temps d'exécution d'EKS.

Pour migrer d'EKS Runtime Monitoring vers Runtime Monitoring

1. La GuardDuty console prend en charge la surveillance du temps d'exécution EKS dans le cadre de la surveillance du temps d'exécution.

   Vous pouvez commencer à utiliser la surveillance du temps d'exécution Vérification de l'état de configuration de la surveillance du temps d'exécution au niveau de votre organisation et de vos comptes.

   Assurez-vous de ne pas désactiver EKS Runtime Monitoring avant d'activer le Runtime Monitoring. Si vous désactivez EKS Runtime Monitoring, la gestion des modules complémentaires Amazon EKS 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 d'exécution d'EKS. Pour plus d’informations, consultez 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 Runtime Monitoring.
- 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 GuardDuty de l'agent de sécurité sont corrects, désactivez EKS Runtime Monitoring à l'aide de l'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 EKS Runtime Monitoring sans activer le Runtime Monitoring, consultezConfiguration de la surveillance du temps d'exécution EKS (API uniquement).

Vérification de l'état de configuration de la surveillance du temps d'exécution

Utilisez les API ou AWS CLI commandes suivantes pour vérifier l'état de configuration existant d'EKS Runtime Monitoring.

Pour vérifier l'état de la configuration EKS Runtime Monitoring existante 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. `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI

Pour vérifier l'état de la configuration EKS Runtime Monitoring existante 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 en utilisant 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. `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI

Désactiver EKS Runtime Monitoring après la migration vers Runtime Monitoring

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 temps d'exécution EKS

- Pour désactiver EKS Runtime Monitoring dans votre propre compte

  Exécutez l'UpdateDetectorAPI avec votre propre identifiant de *détecteur régional.*

  Vous pouvez également utiliser la AWS CLI commande suivante. *Remplacez 12abc34d567e8fa901bc2d34e56789f0 par votre propre identifiant de détecteur régional.*

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

- Pour désactiver EKS Runtime Monitoring pour les comptes des membres de votre organisation

  Exécutez l'UpdateMemberDetectorsAPI avec l'*identifiant de détecteur régional* du compte d' GuardDuty administrateur délégué de l'organisation.

Vous pouvez également utiliser la AWS CLI commande suivante. *Remplacez 12abc34d567e8fa901bc2d34e56789f0 par l'identifiant de détecteur régional du compte d'administrateur délégué GuardDuty de l'organisation et 111122223333 par l'ID du compte membre pour lequel vous souhaitez désactiver cette fonctionnalité.* Compte AWS

```
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 d'EKS Runtime Monitoring pour votre organisation

  Effectuez l'étape suivante uniquement si vous avez configuré les paramètres d'activation automatique d'EKS Runtime Monitoring pour les nouveaux (`NEW`) ou pour tous les (`ALL`) comptes membres de l'organisation. Si vous l'avez déjà configuré comme`NONE`, vous pouvez ignorer cette étape.

  > **Note**
  >
  > Si vous configurez la configuration d'activation automatique d'EKS Runtime Monitoring de manière à `NONE` ce qu'EKS Runtime Monitoring ne soit activé automatiquement pour aucun compte de membre existant ou lorsqu'un nouveau compte de membre rejoint votre organisation.

  Exécutez l'UpdateOrganizationConfigurationAPI avec l'*identifiant de détecteur régional* du compte d' GuardDuty administrateur délégué de l'organisation.

  Vous pouvez également utiliser la AWS CLI commande suivante. *Remplacez 12abc34d567e8fa901bc2d34e56789f0 par l'identifiant de détecteur régional du compte d'administrateur délégué de l'organisation.* GuardDuty Remplacez *EXISTING_VALUE* par 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 terminaison Amazon VPC 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 terminaison Amazon VPC et de surveiller le comportement. En cas de problème lors de la configuration de la surveillance du temps d'exécution, de la création d'un point de terminaison Amazon VPC ou du déploiement de l'agent de GuardDuty sécurité, l'état de couverture apparaît comme étant insalubre. 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'instance Amazon EC2

Pour une ressource Amazon EC2, la couverture du temps d'exécution est évaluée au niveau de l'instance. Vos instances Amazon EC2 peuvent exécuter plusieurs types d'applications et de charges de travail, entre autres, dans votre environnement. AWS Cette fonctionnalité prend également en charge les instances Amazon EC2 gérées par Amazon ECS et si vous avez des clusters Amazon ECS exécutés sur une instance Amazon EC2, les problèmes de couverture au niveau de l'instance apparaîtront dans le cadre de la couverture d'exécution Amazon EC2.

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 instances Amazon EC2 associées à vos propres comptes ou à vos comptes membres sont le pourcentage d'instances EC2 saines par rapport à toutes les instances EC2 de la sélection. 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 clusters Amazon ECS, tout problème de couverture au niveau de l'instance associé aux clusters Amazon ECS exécutés sur une instance Amazon EC2 apparaîtra comme un problème de couverture du temps d'exécution de l'instance Amazon EC2.

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 des instances EC2, vous pouvez consulter les statistiques de couverture agrégées en fonction de l'état de couverture de chaque instance Amazon EC2 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
    - ARN du cluster

- Si l'état de couverture de l'une de vos instances EC2 est considéré comme défaillant, la colonne Problème inclut des informations supplémentaires sur la raison de ce statut d'insalubrité.

API/CLI

- Exécutez l'ListCoverageAPI avec 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 API.
  - 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`
  - Lorsqu'il est `filter-criteria` inclus `RESOURCE_TYPE` en tant qu'EC2, Runtime Monitoring ne prend pas en charge l'utilisation de ISSUE en tant que`AttributeName`. Si vous l'utilisez, la réponse de l'API en résultera`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 les *`résultats maximum`* (jusqu'à 50).
  - `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 l'GetCoverageStatisticsAPI pour récupérer les statistiques agrégées de couverture sur la base de`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 clusters EKS agrégées par état 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`
  - `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 instance EC2 n'est pas satisfaisant, consultezRésolution des problèmes de couverture.

Configuration des notifications de modification de l'état de couverture

L'état de couverture de votre instance Amazon EC2 peut apparaître comme étant défectueux. 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 instance Amazon EC2 passe de `Healthy` à`Unhealthy`, *`GuardDuty Runtime Protection detail-type Unhealthy doit être indiqué`*. Pour être averti lorsque l'état 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 instance Amazon EC2 n'est pas satisfaisant, vous pouvez en connaître la raison dans la colonne Problème.

Si votre instance EC2 est associée à un cluster EKS et que l'agent de sécurité pour EKS a été installé manuellement ou via une configuration automatique de l'agent, pour résoudre le problème de couverture, consultez. Couverture pour les clusters Amazon EKS

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 d'une notification par SMS	Assurez-vous que l'instance Amazon EC2 est déjà gérée par SSM. La réception de la notification SSM peut prendre quelques minutes.
	(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 l'instance Amazon EC2.
		Si vous avez activé la configuration automatique des agents : • Votre instance EC2 est gérée par SSM.

Type de problème	Message d'émission	Étapes de résolution des problèmes
		• Consultez régulièrement le statut de votre agent de sécurité. Pour plus d'informations, consultez Validation de l'état d'installation GuardDuty de l'agent de sécurité.
		Si votre organisation dispose d'une politique de contrôle des services (SCP), assurez-vous qu'elle ne refuse pas l'`guardduty:SendSecurityTelemetry` autorisation. Pour plus d'informations, consultez Validation de la politique de contrôle des services de votre organisation.
	Agent déconnecté	• Consultez le statut de votre agent de sécurité. Pour plus d'informations, consultez 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` .
Échec de la création de l'association SSM	GuardDuty L'association SSM 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 Amazon EC2.

Type de problème	Message d'émission	Étapes de résolution des problèmes
	Votre compte comporte trop d'associations SSM	Choisissez l'une des deux options suivantes : • Supprimez toutes les associations SSM 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.
Échec de la mise à jour de l'association SSM	GuardDuty L'association SSM n'existe pas dans votre compte	GuardDuty L'association SSM n'est pas présente dans votre compte. Désactivez puis réactivez la surveillance du temps d'exécution.
Echec de la suppression de l'association SSM	GuardDuty L'association SSM n'existe pas dans votre compte	L'association SSM n'est pas présente dans votre compte. Si l'association SSM a été supprimée intentionnellement, aucune action n'est nécessaire.

Type de problème	Message d'émission	Étapes de résolution des problèmes
Échec de l'exécution de l'association d'instances SSM	Les exigences architecturales ou autres prérequis ne sont pas respectés.	Pour plus d'informations sur les distributions de systèmes d'exploitation vérifiées, consultezConditions préalables à la prise en charge des instances Amazon EC2. 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.
Échec de la création du point de terminaison VPC	La création d'un point de terminaison d'un VPC n'est pas prise en charge pour le VPC partagé *vpcId*.	La surveillance du temps d'exécution prend en charge l'utilisation d'un VPC partagé au sein d'une organisation. Pour plus d'informations, consultez Utilisation d'un VPC partagé avec des agents de sécurité automatisés.

Type de problème	Message d'émission	Étapes de résolution des problèmes
	Uniquement lors de l'utilisation d'un VPC partagé avec configuration d'agent automatisée L'ID de compte propriétaire *111122223333 pour* le VPC partagé ne permet pas d'activer la surveillance du temps *d'exécution,* la configuration automatique des agents, ou les deux	Le compte propriétaire du VPC 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 plus d'informations, consultez Prérequis spécifiques à la surveillance du temps d' GuardDuty exécution.

Type de problème	Message d'émission	Étapes de résolution des problèmes
	L'activation de DNS privé nécessite à la fois des attributs de VPC `enableDnsSupport` et `enableDnsHostnames` VPC définis sur `true` pour *`vpcId`* (Service : Ec2, Status Code:400, ID de demande : *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assurez-vous que les attributs de VPC suivants sont définis sur `true` : `enableDnsSupport` et `enableDnsHostnames` . Pour plus d'informations, veuillez consulter la rubrique Attributs DNS dans votre VPC. Si vous utilisez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/ pour créer l'Amazon VPC, assurez-vous de sélectionner à la fois Activer les noms d'hôte DNS et Activer la résolution DNS. Pour plus d'informations, veuillez consulter Options de configuration de VPC.

Type de problème	Message d'émission	Étapes de résolution des problèmes
La suppression du point de terminaison VPC partagé a échoué	*La suppression du point de terminaison VPC partagé n'est pas autorisée pour l'ID de compte 111122223333, l'identifiant de compte VPC partagé et l'ID de compte propriétaire 555555555555.*	Étapes potentielles : • La désactivation de l'état de surveillance du temps d'exécution du compte de participant VPC partagé n'a aucun impact sur la politique de point de terminaison du VPC partagé ni sur le groupe de sécurité existant dans le compte propriétaire. Pour supprimer le point de terminaison et le groupe de sécurité VPC partagés, vous devez désactiver la surveillance du temps d'exécution ou l'état de configuration automatique de l'agent dans le compte propriétaire du VPC partagé. • Le compte de participant VPC partagé ne peut pas supprimer le point de terminaison et le groupe de sécurité VPC partagés hébergés dans le compte propriétaire du VPC 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 Amazon EC2. Si le problème persiste, pensez à désactiver la surveillance du temps d'exécution pendant quelques minutes, puis réactivez-la.

Couverture pour les clusters Amazon ECS

La couverture d'exécution des clusters Amazon ECS inclut les tâches exécutées sur les instances de conteneur Amazon ECS AWS Fargate (Fargate) et les instances de conteneur [1].

Pour un cluster Amazon ECS qui s'exécute sur Fargate, la couverture d'exécution est évaluée au niveau de la tâche. La couverture du temps d'exécution des clusters ECS 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 (ECS uniquement). 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 conteneur Amazon ECS, consultez la section Création de capacités.

Table des matières

Consultation des statistiques de couverture

Les statistiques de couverture pour les ressources Amazon ECS associées à votre propre compte ou à vos comptes de membres sont le pourcentage de clusters Amazon ECS sains par rapport à tous les clusters Amazon ECS du groupe sélectionné Région AWS. Cela inclut la couverture des clusters Amazon ECS associés à la fois aux instances Fargate et Amazon EC2. L'équation suivante représente cela comme suit :

(Clusters sains/Tous les clusters) x 100

Considérations

- Les statistiques de couverture du cluster ECS incluent l'état de couverture des tâches Fargate ou des instances de conteneur ECS 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 des clusters ECS, le champ Instances de conteneur couvertes indique l'état de couverture des instances de conteneur associées à votre cluster Amazon ECS.

  Si votre cluster Amazon ECS contient uniquement des tâches Fargate, le nombre s'affiche sous la forme 0/0.
- Si votre cluster Amazon ECS est associé à une instance Amazon EC2 dépourvue d'agent de sécurité, le cluster Amazon ECS aura également un statut de couverture défaillant.

  Pour identifier et résoudre le problème de couverture de l'instance Amazon EC2 associée, Résolution des problèmes de couverture consultez la section consacrée aux instances Amazon EC2.

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 clusters ECS, vous pouvez consulter les statistiques de couverture agrégées en fonction de l'état de couverture de chaque cluster Amazon ECS 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 clusters Amazon ECS est considéré comme insalubre, la colonne Problème inclut des informations supplémentaires sur la raison de ce statut insalubre.

  Si vos clusters Amazon ECS sont associés à une instance Amazon EC2, accédez à l'onglet Couverture du temps d'exécution de l'instance EC2 et filtrez par le champ Nom du cluster pour afficher le problème associé.

API/CLI

- Exécutez l'ListCoverageAPI avec 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 API.
  - 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 cluster Amazon ECS associé ou en cas de modification de l'état de couverture correspondant.
  - Vous pouvez modifier les *`résultats maximum`* (jusqu'à 50).
  - `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 l'GetCoverageStatisticsAPI pour récupérer les statistiques agrégées de couverture sur la base de`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 clusters ECS agrégées par état 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`
- `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 cluster Amazon ECS peut apparaître comme étant défectueux. 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 l'état de couverture de votre cluster Amazon ECS passe de `Healthy` à`Unhealthy`, *`GuardDuty Runtime Protection Unhealthy detail-type doit être indiqué`*. Pour être averti lorsque l'état 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 cluster Amazon ECS n'est pas satisfaisant, vous pouvez en connaître la raison dans la colonne Problème.

Le tableau suivant fournit les étapes de dépannage recommandées pour les problèmes liés à Fargate (Amazon ECS uniquement). Pour plus d'informations sur les problèmes de couverture des instances Amazon EC2, consultez la section relative aux instances Amazon EC2. Résolution des problèmes de couverture

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 la configuration de votre point de terminaison VPC est correcte. Si votre organisation dispose d'une politique de contrôle des services (SCP), assurez-vous qu'elle ne refuse pas l'`guardduty:SendSecurityTelemetry` autorisation. Pour plus d'informations, consultez Validation de la politique de contrôle des services de votre organisation.
	`VPC_ISSUE` `; for task in TaskDefinition - '` *`TASK_DEFINITION`* `'`	Consultez les détails du problème du VPC 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 : *`RAISON`* des 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* '	

	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 (Amazon ECR) suivantes :
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		Pour plus d'informations, consultez Fournir les autorisations ECR et les détails du sous-réseau.
		Après avoir ajouté les autorisations Amazon ECR, 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
Autres ou agent non provisionné	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 ? Dans Amazon ECS, 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 Mettre à jour un service. Vous pouvez également utiliser UpdateServiceou AWS CLI. • La tâche a-t-elle été lancée après avoir exclu le cluster ECS 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 cluster ECS. • Il en manque un dans votre tâche `TaskExecutionRole` ? Il est obligatoire d'ajouter un `TaskExecutionRole` car des autorisations sont GuardDuty nécessaires pour télécharger le GuardDuty conteneur depuis le référentiel ECR. Pour plus d'informations, consultez Fournir les autorisations ECR et les détails du sous-réseau. • 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 les Amazon Resource Names (ARN) pour les ressources Amazon ECS, consultez Amazon Resource Names (ARN) and IDs.

Couverture pour les clusters Amazon EKS

Après avoir activé la surveillance du temps d'exécution et installé l'agent de GuardDuty sécurité (module complémentaire) pour EKS manuellement ou par le biais d'une configuration automatique de l'agent, vous pouvez commencer à évaluer la couverture de vos clusters EKS.

Table des matières

Consultation des statistiques de couverture

Les statistiques de couverture pour les clusters EKS associés à vos propres comptes ou à vos comptes membres sont le pourcentage de clusters EKS sains par rapport à tous les clusters EKS de la Région AWS sélectionnée. 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 du cluster EKS.
- Dans l'onglet Couverture d'exécution du cluster EKS, vous pouvez consulter les statistiques de couverture agrégées selon l'état de couverture disponible dans le tableau 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'un de vos clusters EKS a un état de couverture Non sain, la colonne Problème peut inclure des informations supplémentaires sur la raison de l'état Défectueux.

API/CLI

- Exécutez l'ListCoverageAPI avec 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 API.
  - 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 les *`résultats maximum`* (jusqu'à 50).
  - `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 l'GetCoverageStatisticsAPI pour récupérer les statistiques agrégées de couverture sur la base de`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 clusters EKS agrégées par état 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`
  - `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 cluster EKS est Défectueux, veuillez consulter Résolution des problèmes de couverture EKS.

Configuration des notifications de modification de l'état de couverture

L'état de couverture d'un cluster EKS sur votre compte peut être indiqué comme étant Défectueux. 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 l'état de couverture de votre cluster Amazon EKS passe de `Healthy` à`Unhealthy`, *`GuardDuty Runtime Protection Unhealthy detail-type doit être indiqué`*. Pour être averti lorsque l'état 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 couverture EKS

Si l'état de couverture de votre cluster EKS est le suivantUnhealthy, 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 clusters EKS de manière sélective, la synchronisation des balises peut prendre un certain temps. Cela peut avoir un impact sur l'état de couverture du cluster EKS associé. Vous pouvez réessayer de supprimer et d'ajouter la balise correspondante (inclusion ou exclusion). Pour plus d'informations, veuillez consulter Étiquetage de vos ressources Amazon EKS dans le Guide du de l'utilisateur Amazon EKS.

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 clusters EKS.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
Échec de la création de l'addon	L'addon n'`aws-guardduty-agent` est pas compatible avec la version actuelle du cluster *`ClusterName`* . Le module complémentaire 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 EKS `aws-guardduty-agent` . Pour plus d'informations, consultez Versions de Kubernetes prises en charge par l'agent de sécurité GuardDuty . Pour

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
		plus d'informations sur la mise à jour de votre version de Kubernetes, veuillez consulter la section Mise à jour d'une version Kubernetes de cluster Amazon EKS.
Échec de la création de l'addon Échec de la mise à jour de l'addon État de l'addon malsain	Problème de module complémentaire EKS : `AddonIssueCode` : `AddonIssueMessage`	Pour plus d'informations sur les étapes recommandées pour un code de problème 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.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
Échec de la création du point de terminaison VPC	*La création d'un point de terminaison VPC n'est pas prise en charge pour le VPC VPC partagé*	Runtime Monitoring prend désormais en charge l'utilisation d'un VPC partagé au sein d'une organisation. Assurez-vous que vos comptes répondent à toutes les conditions requises. Pour plus d'informations, consultez Conditions préalables à l'utilisation d'un VPC partagé.
	Uniquement lors de l'utilisation d'un VPC partagé avec configuration d'agent automatisée L'ID de compte propriétaire *111122223333 pour* le VPC partagé ne permet pas d'activer la surveillance du *temps* d'exécution, la configuration automatique des agents ou les deux.	Le compte propriétaire du VPC 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 plus d'informations, consultez Prérequis spécifiques à la surveillance du temps d' GuardDutyexécution.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
	L'activation de DNS privé nécessite à la fois des attributs de VPC `enableDnsSupport` et `enableDnsHostnames` VPC définis sur `true` pour *`vpcId`* (Service : Ec2, Status Code:400, ID de demande : *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assurez-vous que les attributs de VPC suivants sont définis sur `true` : `enableDnsSupport` et `enableDnsHostnames` . Pour plus d'informations, veuillez consulter la rubrique Attributs DNS dans votre VPC. Si vous utilisez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/ pour créer l'Amazon VPC, assurez-vous de sélectionner à la fois Activer les noms d'hôte DNS et Activer la résolution DNS. Pour plus d'informations, veuillez consulter Options de configuration de VPC.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
Échec de la suppression du point de terminaison VPC partagé	*La suppression du point de terminaison VPC partagé n'est pas autorisée pour l'ID de compte 111122223333, l'identifiant de compte VPC partagé et l'ID de compte propriétaire 555555555555.*	Étapes potentielles : • La désactivation de l'état de surveillance du temps d'exécution du compte de participant VPC partagé n'a aucun impact sur la politique de point de terminaison du VPC partagé ni sur le groupe de sécurité existant dans le compte propriétaire. Pour supprimer le point de terminaison et le groupe de sécurité VPC partagés, vous devez désactiver la surveillance du temps d'exécution ou l'état de configuration automatique de l'agent dans le compte propriétaire du VPC partagé. • Le compte de participant VPC partagé ne peut pas supprimer le point de terminaison et le groupe de sécurité VPC partagés hébergés dans le compte propriétaire du VPC partagé.

Type de problème (préfixe)	Informations supplémentaires	Étapes de dépannage recommandées
Clusters EKS locaux	Les modules complémentaires EKS ne sont pas prises en charge sur les clusters Outpost locaux.	Non exploitable. Pour de plus amples informations, veuillez consulter Amazon EKS sur AWS Outposts.
Autorisation d'activation de la surveillance d'exécution EKS 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 d'exécution EKS 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
la surveillance d'exécution EKS permet l'allocation de ressources en cours	(peut afficher ou non des informations supplémentaires)	Non exploitable. Une fois que vous avez activé la surveillance d'exécution EKS, l'état de couverture peut rester `Unhealthy` jusqu'à la fin de l'étape d'allocation 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 d'exécution EKS 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
Problème lié à l'addon EKS - `InsufficientNumberOfReplicas` : Le module complémentaire est défectueux car il 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 describe pods`à utiliser pour identifier la cause première de la défaillance du pod.

Erreur de création ou de mise à jour de l'addon	Étapes de résolution des problèmes
	Après avoir corrigé la cause première, réessayez l'étape (création ou mise à jour d'un module complémentaire).
Problème lié à l'addon EKS - `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 cluster Amazon EKS 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'Amazon EKS.
Problème lié à l'extension EKS - `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 l'API Kubernetes. 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

Problème lié à l'extension EKS - `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 cluster Amazon EKS 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
Problème lié à l'extension EKS - `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 cluster Amazon EKS. 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 (FAQ)

Table des matières

Pourquoi l'état de couverture de ma ressource **`Unhealthy`** s'applique-t-il même après avoir activé la surveillance du temps d'exécution, déployé l'agent de GuardDuty sécurité et rempli toutes les conditions préalables ?

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 bon 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.

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.

Configuration de la surveillance du processeur et 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 processeur et de mémoire de l' GuardDuty agent.

Configuration de la surveillance sur le cluster Amazon ECS

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 processeur 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 cluster Amazon EKS

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. Statistiques Amazon EKS et 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 plus d'informations, consultez Configuration des paramètres du module complémentaire EKS.

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. Si une menace potentielle est GuardDuty détectée et génère 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.
Chemin d'accès du processus	Chemin absolu de l'exécutable du processus.
ID du processus.	ID attribué au processus par le système d'exploitation.
PID de l'espace de noms	ID du processus dans un espace de noms PID secondaire différent de l'espace de noms PID 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.

Nom de champ	Description
UUID du processus	L'identifiant unique attribué au processus par GuardDuty.
GID du processus	ID de processus du groupe de processus.
EGID du processus	ID de groupe effectif du groupe de processus.
EUID du processus	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 date UTC (`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.
Process Present Working Directory (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.

Nom de champ	Description
Arguments de ligne de commande Actuellement, ce champ est limité à des versions d'agent spécifiques correspondant au type de ressource : • Fargate (Amazon ECS uniquement GuardDuty) avec agent de sécurité v1.0.0 et versions ultérieures. • Instances Amazon EC2 avec agent de GuardDuty sécurité v1.0.0 et versions ultérieures. • Clusters Amazon EKS avec agent de sécurité v1.4.0 et versions ultérieures. Pour plus d'informations, consultez 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` .
UID de conteneur	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 de champ	Description
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 (ARN) de la tâche	L'ARN de la tâche.
Nom du cluster	Nom du cluster Amazon ECS.
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 service Amazon ECS, 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'unités de processeur utilisées par la tâche, tel qu'il est indiqué 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.

Nom de champ	Description
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.

Événements DNS

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, par exemple 17 pour UDP et 6 pour TCP.
IP du point de terminaison distant DNS	Adresse IP distante de la connexion.
Port du point de terminaison distant DNS	Numéro de port de la connexion.
Adresse IP du point de terminaison local du DNS	Adresse IP locale de la connexion.
Port du point de terminaison local du DNS	Numéro de port de la connexion.
Charge utile du DNS	Charge utile des paquets DNS contenant des réponses et des requêtes DNS.

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.

Nom de champ	Description
Type de système de fichiers	Représente le type de système de fichiers monté.
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.
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.

Nom de champ	Description
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.
Type de socket	Type de socket pour indiquer la sémantique de communication. Par exemple, `SOCK_RAW`.

Nom de champ	Description
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.
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.
PID cible	ID du processus à partir duquel la mémoire est lue.
UUID du processus cible	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.
PID cible	ID du processus dans lequel la mémoire est écrite.
UUID du processus cible	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.

Événements Ptrace

Nom de champ	Description
PID cible	ID du processus cible.
UUID du processus cible	ID unique du processus cible.
Chemin d'exécutable cible	Chemin absolu du fichier exécutable du processus cible.

Nom de champ	Description
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, par exemple 17 pour UDP et 6 pour TCP.
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`.

Nom de champ	Description
Numéro de protocole	Le numéro de protocole de couche 4, par exemple 17 pour UDP et 6 pour TCP.
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.

Définir les événements UID

Nom de champ	Description
Nouvel EUID	Le nouvel ID utilisateur effectif du processus.
Nouvel 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.

Agent d'hébergement GuardDuty de référentiels Amazon ECR

Les sections suivantes répertorient les référentiels Amazon Elastic Container Registry (Amazon ECR) dans GuardDuty lesquels héberge l'agent de sécurité déployé sur vos clusters Amazon EKS et Amazon ECS.

Table des matières

Référentiel pour l'agent EKS version 1.6.0 ou supérieure

Le tableau suivant présente les référentiels Amazon ECR hébergeant l'agent complémentaire Amazon EKS version (`aws-guardduty-agent`) 1.6.0 et ultérieure, pour chacun d'entre eux. Région AWS

Région AWS	URI du référentiel Amazon ECR
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`
Canada (Centre)	`602401143452.dkr.ecr.ca-central-1.amazonaws.com`
Canada Ouest (Calgary)	`761377655185.dkr.ecr.ca-west-1.amazonaws.com`
Moyen-Orient (EAU)	`759879836304.dkr.ecr.me-central-1.amazonaws.com`

Région AWS	URI du référentiel Amazon ECR
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
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

Région AWS	URI du référentiel Amazon ECR
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'agent EKS

Le tableau suivant présente les référentiels Amazon ECR hébergeant l'agent complémentaire Amazon EKS version (`aws-guardduty-agent`) 1.5.0 et antérieures, pour chacun d'entre eux. Région AWS

Région AWS	URI du référentiel Amazon ECR
USA Ouest (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europe (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`

Région AWS	URI du référentiel Amazon ECR
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 (EAU)	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
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

Région AWS	URI du référentiel Amazon ECR
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
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 référentiels Amazon ECR qui hébergent l' GuardDuty agent pour (AWS Fargate Amazon ECS uniquement) pour chacun d'eux. Région AWS

Région AWS	URI du référentiel Amazon ECR
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 (EAU)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`
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`

Région AWS	URI du référentiel Amazon ECR
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
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

Région AWS	URI du référentiel Amazon ECR
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 l' GuardDuty agent déployé sur les instances Amazon EC2, les clusters Amazon ECS et les clusters Amazon EKS

GuardDuty agent de sécurité pour les instances Amazon EC2

Version d'agent	Notes de mise à jour	Date de disponibilité
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	26 mars 2024

Version d'agent	Notes de mise à jour	Date de disponibilité
	ue des agents dans le cadre de la surveillance du temps d'exécution pour les instances Amazon EC2 Prend en charge les nouveaux signaux de sécurité et les résultats publiés avec l'annonce de la disponibilité générale de Runtime Monitoring pour les instances EC2 Optimisation et améliorations générales des performances	
v1.0.2	Prend en charge les dernières AMI Amazon ECS.	2 février 2024
v1.0.1	Les versions de l'agent publiées avant la v1.0.2 sont incompatibles avec les AMI Amazon ECS lancées après le 31 janvier 2024. Optimisation et améliorations générales des performances	23 janvier 2024
v1.0.0	Version initiale de l'installation RPM Les versions de l'agent publiées avant la v1.0.2 sont incompatibles avec les AMI Amazon ECS lancées après le 31 janvier 2024.	26 novembre 2023

RPM S3 bucket example script

La clé publique, la signature du RPM x86_64, la signature du RPM arm64 et le lien d'accès correspondant aux scripts RPM hébergés dans les compartiments 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 RPM. Les modèles suivants incluent la dernière version de l'agent pour les instances Amazon EC2.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/publickey.pem
```

- GuardDuty signature RPM de l'agent de sécurité :

  Signature de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/amazon-guardduty-agent-1.2.0.x86_64.sig
```

  Signature d'arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.arm64.sig
```

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

  Lien d'accès pour x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/x86_64/amazon-guardduty-agent-1.2.0.x86_64.rpm
```

  Lien d'accès pour arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.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 instances Amazon EC2.

- Clé publique :

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/publickey.pem
```

- GuardDuty signature de l'agent de sécurité :

  Signature d'amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/amd64/amazon-guardduty-agent-1.2.0.amd64.sig
```

  Signature d'arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.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/1.2.0/amd64/amazon-guardduty-agent-1.2.0.amd64.deb
```

  Lien d'accès pour arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.2.0/arm64/amazon-guardduty-agent-1.2.0.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 (EAU)	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 (Amazon ECS uniquement).

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
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 Graviton (ARM64) : sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7	Prend en charge les nouveaux signaux et découvertes de sécurité Optimisation et améliorations générales des performances	01 mai 2024

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité
v1.0.1	x86_64 (AMD64) : `sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68` Graviton (ARM64) : `sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7`	Optimisation et améliorations générales des performances	26 janvier 2024
v1.0.0	x86_64 (AMD64) : `sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017` Graviton (ARM64) : `sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984`	Version initiale de l'agent de GuardDuty sécurité pour AWS Fargate (Amazon ECS uniquement).	26 novembre 2023

GuardDuty agent de sécurité pour les clusters Amazon EKS

Le tableau suivant présente l'historique des versions de l' GuardDuty agent complémentaire Amazon EKS.

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
v1.6.1	x86_64 (AMD64) : `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Graviton (ARM64) : `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Optimisation et améliorations générales des performances.	14 mai 2024	–
v1.6.0	x86_64 (AMD64) : `sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010` Graviton (ARM64) : `sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`	• Prend en charge la configuration GuardDuty automatique des agents pour les ressources EKS/EC2. • Soutient les nouveaux signaux et résultats de sécurité. Pour plus d'informations, consultez	29 avril 2024	–

Version d'agent	Image de conteneur	Notes de mise à jour	Date de disponibilité	Fin du support standard [1]
		Types d'événements d'exécution collectés qui GuardDuty utilisent et Types de recherche 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-dessousTypes d'événement d'exécution collectés. • Améliorations des performances liées à l'utilisation du processeur.	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) : `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64) : `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	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 basées sur AMD64, la version 1.2.0 prend désormais également en charge les instances basées sur ARM64. 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`	Publication initiale de l'agent de module complémentaire Amazon EKS.	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 point de terminaison VPC Compte AWS utilise ou non un point de terminaison VPC partagé GuardDuty ne supprime pas le point de terminaison VPC. Si nécessaire, vous devrez supprimer le point de terminaison du VPC manuellement.

Désactivation de la surveillance de l'exécution et de la surveillance de l'exécution EKS

Cette section s'applique à vous dans les scénarios suivants :

- Vous n'avez jamais activé EKS Runtime Monitoring séparément et vous avez maintenant désactivé le Runtime Monitoring.
- Vous désactivez à la fois la surveillance du temps d'exécution et la surveillance du temps d'exécution EKS. Si vous n'êtes pas sûr de l'état de configuration d'EKS Runtime Monitoring, consultezVérification de l'état de configuration de la surveillance du temps d'exécution.

> Désactiver la surveillance du temps d'exécution sans désactiver la surveillance du temps d'exécution EKS
>
> Dans ce scénario, à un moment donné, vous avez activé EKS Runtime Monitoring, et plus tard, vous avez également activé le Runtime Monitoring sans désactiver EKS Runtime Monitoring.
> Désormais, lorsque vous désactivez la surveillance du temps d'exécution, vous devez également désactiver la surveillance du temps d'exécution d'EKS ; dans le cas

contraire, vous continuerez à supporter des coûts d'utilisation pour le suivi du temps d'exécution d'EKS.

Si les scénarios listés précédemment s'appliquent à vous, alors vous GuardDuty effectuerez les actions suivantes sur votre compte :

- GuardDuty supprime le VPC doté de `GuardDutyManaged` la `true` balise :. Il s'agit du VPC qui GuardDuty a été créé pour gérer l'agent de sécurité automatisé.
- GuardDuty supprime le groupe de sécurité marqué comme `GuardDutyManaged` :`true`.
- Pour un VPC partagé qui a été utilisé par au moins un compte participant, GuardDuty ni le point de terminaison du VPC ni le groupe de sécurité associé à la ressource VPC partagée ne sont supprimés.
- Pour une ressource Amazon EKS, GuardDuty supprime l'agent de sécurité. Cela est indépendant du fait qu'il soit géré manuellement ou par le biais GuardDuty.

  Pour une ressource Amazon ECS, étant donné qu'une tâche ECS 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 tâche ECS commence à s'exécuter. Pour plus d'informations sur l'utilisation des tâches Fargate-ECS, consultez. Comment fonctionne la surveillance du temps d'exécution avec Fargate (Amazon ECS uniquement)

  Pour une ressource Amazon EC2, GuardDuty désinstalle l'agent de sécurité de toutes les instances Amazon EC2 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 ressource EC2, 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 terminaison Amazon VPC.

Processus de nettoyage des ressources des agents de sécurité

Pour supprimer un point de terminaison Amazon VPC

- Sans VPC partagé : lorsque vous ne souhaitez plus surveiller une ressource dans un compte, pensez à supprimer le point de terminaison Amazon VPC.
- Avec un VPC partagé : lorsqu'un compte propriétaire de VPC partagé supprime la ressource de VPC 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 d'exécution EKS) des ressources de votre compte propriétaire de VPC partagé et du compte participant peut devenir inadéquat. 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 VPC partagé : lorsque vous ne souhaitez plus surveiller un type de ressource dans un compte, pensez à supprimer le groupe de sécurité associé à Amazon VPC.
- Avec un VPC partagé : lorsque le compte propriétaire du VPC partagé supprime le groupe de sécurité, tout compte participant utilisant actuellement le groupe de sécurité associé au VPC partagé, l'état de couverture de la surveillance du temps d'exécution pour les ressources de votre compte propriétaire de VPC partagé et du compte participant peut devenir inadéquat. Pour plus d'informations, consultez 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 cluster EKS

Pour supprimer l'agent de sécurité de votre cluster EKS que vous ne souhaitez plus surveiller, reportez-vous à la section Suppression d'un module complémentaire.

La suppression de l'agent de module complémentaire EKS ne supprime pas l'espace de noms `amazon-guardduty` du cluster EKS. Pour supprimer l'espace de noms `amazon-guardduty`, veuillez consulter Suppression d'un espace de noms.

Pour supprimer l'espace de **`amazon-guardduty`** noms (cluster EKS)

La désactivation de la configuration automatique des agents ne supprime pas automatiquement l'`amazon-guarddutyespace` de noms de votre cluster EKS. Pour supprimer l'espace de noms `amazon-guardduty`, veuillez consulter Suppression d'un espace de noms.

Protection Amazon S3 sur Amazon GuardDuty

S3 Protection aide Amazon à GuardDuty surveiller les événements liés aux AWS CloudTrail données pour Amazon Simple Storage Service (Amazon S3) qui incluent des opérations d'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 opérations d'API 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 manuellement la connexion aux événements de données S3 AWS CloudTrail. 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 plus d’informations, consultez 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 plus d’informations, consultez 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 IAM (AWS Identity and Access Management) ou AWS STS (AWS Security Token Service) valides.

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.

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 plus d'informations, consultez 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**
>
> `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 plus d’informations, consultez 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 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 Enregistrer.

API/CLI

Exécutez en updateDetectorutilisant l'ID du détecteur du compte GuardDuty administrateur délégué pour la région actuelle et en transmettant l'`features`objet `name` sous forme `S3_DATA_EVENTS` ou en `status` tant que `ENABLED` ou`DISABLED`.

Vous pouvez également configurer S3 Protection en utilisant AWS Command Line Interface. *Exécutez la commande suivante et assurez-vous de remplacer 12abc34d567e8fa901bc2d34e56789f0 par l'ID du détecteur du compte administrateur délégué pour la région actuelle et 555555555555 par l'ID du compte administrateur délégué. GuardDuty* Compte AWS GuardDuty

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

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --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 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 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, invoquez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. *Assurez-vous de remplacer 12abc34d567e8fa901bc2d34e56789f0 par le compte administrateur délégué, et 111122223333. detector-id GuardDuty* Pour désactiver la protection S3, remplacez `ENABLED` par `DISABLED`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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, invoquez l'opération d'API updateMemberDetectors en utilisant votre propre *ID de détecteur*.
- L'exemple suivant montre comment vous pouvez activer la protection S3 pour un compte membre unique. *Assurez-vous de remplacer 12abc34d567e8fa901bc2d34e56789f0 par le compte administrateur délégué, et 111122223333. detector-id GuardDuty* Pour désactiver la protection S3, remplacez `ENABLED` par `DISABLED`.

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 soit la page S3 Protection, soit la page 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 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 Enregistrer.

API/CLI

- Pour activer ou désactiver la protection S3 de manière sélective pour vos comptes membres, invoquez l'opération d'API UpdateOrganizationConfiguration en utilisant votre propre *`ID de détecteur`*.
- 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 RDS de manière sélective pour 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`.

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

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

  > **Note**
  >
  > Vous pouvez également transmettre une liste d'ID de compte 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 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'opération d'API updateMemberDetectors en utilisant votre propre ID 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`.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 d'ID de compte 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 la protection S3 dans vos nouveaux comptes, vous pouvez modifier l'opération d'API createDetector avec l'objet facultatif `dataSources`, 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 le fonctionnement de l'createDetectorAPI avec l'`features`objet facultatif. 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"}]'
```

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 :

- Opérations d'API `GetObject`
- Opérations d'API `PutObject`

- Opérations d’API `ListObjects`
- Opérations d’API `DeleteObject`

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 GuardDuty Protection S3.

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 en utilisant les opérations de l'API AWS CLI or. Pour un aperçu des façons dont vous pouvez gérer les résultats, veuillez consulter Gérer les GuardDuty résultats d'Amazon.

Rubriques :

Détails d’un résultat

Découvrez les détails associés aux GuardDuty résultats générés dans votre compte.

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.

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.

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` `AccessKeyS3Bucket`, `S3ObjectKubernetes 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 exportations JSON et les sorties CLI affichent les horodatages en 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 plus d’informations, consultez 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 pour EC2 est activée, il s'agit d'un identifiant de l'analyse des programmes malveillants

exécutée sur les volumes EBS attachés à l'instance ou à la charge de travail du conteneur EC2 potentiellement compromise. Pour plus d'informations, consultez Protection contre les logiciels malveillants pour la recherche de détails dans EC2.

- Gravité : niveau de gravité attribué à un résultat : Élevée, Moyenne ou Faible. Pour plus d'informations, consultez 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 CIBLE ou ACTEUR, et indique si votre ressource était 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, S3Bucket AccessKey, S3Object, ECSCluster, Container KubernetesCluster, RDSDBInstance 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'invocation d'API sous-jacente provient d'une instance EC2 d'une autre région lors d'un appel d'API entre régions.

- ID d'instance : ID de l'instance EC2 impliquée dans l'activité qui a incité GuardDuty à générer le résultat.
- Type d'instance : type de l'instance EC2 impliquée dans le résultat.

- Heure de lancement : date et heure auxquelles l'instance a été lancée.
- Outpost ARN — Le nom de 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 de plus amples informations, veuillez consulter Élément CloudTrail userIdentity.
- 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 : ARN du compartiment impliqué dans le résultat.

- Propriétaire : ID utilisateur canonique de l'utilisateur propriétaire du compartiment impliqué dans le résultat. Pour de plus amples informations sur l'ID d'utilisateur canonique, veuillez consulter Identificateurs de compte AWS.
- 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 — Nom de ressource Amazon (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 — Nom de ressource Amazon (ARN) du compartiment S3.
- Propriétaire : identifiant canonique du propriétaire du compartiment S3.

EKSCluster

Détails du cluster Kubernetes :

- Nom : nom du cluster Kubernetes.
- ARN : l'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 exportations JSON et les sorties CLI affichent les horodatages en UTC.

- ID de VPC : ID du VPC 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 de RBAC (contrôle basé sur l'accès aux rôles) de Kubernetes de l'utilisateur qui participe à 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 rôle IAM avec les autorisations RBAC de Kubernetes.

ECSCluster

Détails du cluster ECS :

- ARN : l'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 : Amazon Resource Name (ARN) de la tâche.
  - ARN de la définition : Amazon Resource Name (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 : ID de l'instance de conteneur ou entrées ARN complètes pour 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

Détails de l'instance RDSDB :

> **Note**
>
> Cette ressource est disponible dans les résultats de protection RDS 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 compatibles avec Aurora MySQL ou compatibles avec Aurora PostgreSQL.
- 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.

- ARN de l'instance de base de données : ARN identifiant 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.
- ARN de fonction : Amazon Resource Name (ARN) de la fonction Lambda impliquée dans le résultat.
- 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.
- Configuration de VPC : configuration d'Amazon VPC, y compris l'ID VPC, le groupe de sécurité et les ID de sous-réseau associés à votre fonction Lambda.
- ID de VPC : ID d'Amazon VPC associé à la fonction Lambda impliquée dans le résultat.
- ID de sous-réseau : 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`.

Détails de l'utilisateur de base de données (DB) RDS

> **Note**
>
> Cette section s'applique aux résultats obtenus lorsque vous activez la fonctionnalité de protection RDS dans GuardDuty. Pour plus d'informations, consultez Protection RDS dans GuardDuty.

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 SSL (Secure Socket Layer) 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.
- Exécutable SHA-256 : hachage `SHA256` de l'exécutable du processus.
- PID de l'espace de noms : ID du processus dans un espace de noms PID secondaire différent de l'espace de noms PID 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.
- 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 démarré. Ce champ est au format de chaîne de date UTC (`2023-03-22T19:37:20.168Z`).
- UUID — L'identifiant unique attribué au processus par. GuardDuty

- UUID parent : identifiant 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.
  - UUID parent : identifiant unique du processus parent. Cet identifiant est attribué au processus parent par GuardDuty.
  - Heure de début : heure à laquelle le processus a démarré.
  - PID de l'espace de noms : ID du processus dans un espace de noms PID secondaire différent de l'espace de noms PID 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 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 date UTC (`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.

Détails de l'analyse des volumes EBS

> **Note**
>
> Cette section s'applique aux résultats obtenus lorsque vous activez l'analyse des programmes malveillants GuardDuty initiée par l'utilisateur. GuardDuty Protection contre les logiciels malveillants pour EC2

L'analyse des volumes EBS fournit des informations détaillées sur le volume EBS attaché à l'instance EC2 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 recherche de détails dans EC2

> **Note**
>
> Cette section s'applique aux résultats obtenus lorsque vous activez l'analyse des programmes malveillants GuardDuty initiée par l'utilisateur. GuardDuty Protection contre les logiciels malveillants pour EC2

Lorsque l'analyse Malware Protection for EC2 détecte un logiciel malveillant, vous pouvez consulter les détails de l'analyse en sélectionnant le résultat correspondant sur la page Résultats de la console https://console.aws.amazon.com/guardduty/. La gravité de votre détection de Malware Protection for EC2 dépend de la gravité de la GuardDuty découverte.

> **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.
- Hachage : SHA-256 du fichier.
- Chemin d'accès du fichier : emplacement du fichier malveillant dans le volume EBS.
- Nom du fichier : nom du fichier dans lequel la menace a été détectée.
- ARN du volume : ARN des volumes EBS analysés.

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.
  - ARN du volume : Amazon Resource Name (ARN) du volume.
  - SnapshotARN : ARN de l'instantané du volume EBS.
  - 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_REQUEST, AWS_API_CALL ou RDS_LOGIN_ATTEMPT. Les informations disponibles varient selon le type d'action :

- NETWORK_CONNECTION : indique qu'un trafic réseau a été échangé entre l'instance EC2 identifiée et l'hôte distant. Ce type d'action contient les informations supplémentaires suivantes :
  - Direction de connexion : direction de connexion réseau observée lors de 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 initié une connexion à un port local sur l'instance EC2 identifiée dans votre compte.
    - OUTBOUND : indique que l'instance EC2 identifiée a initié une connexion à un hôte distant.
    - INCONNU — 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 pod EKS par opposition à l'adresse IP de l'instance sur laquelle le pod EKS s'exécute.

  - Bloqué : indique si le port cible est bloqué.
- PORT_PROBE : indique qu'un hôte distant a fait l'objet d'une identification de l'instance EC2 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 pod EKS par opposition à l'adresse IP de l'instance sur laquelle le pod EKS s'exécute.
  - Bloqué : indique si le port cible est bloqué.
- DNS_REQUEST : indique que l'instance EC2 identifiée a interrogé 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'une API AWS a été appelée. Ce type d'action contient les informations supplémentaires suivantes :
  - API : nom de l'opération d'API qui a été invoquée et donc invitée GuardDuty à générer ce résultat.

    > **Note**
    >
    > Ces opérations peuvent également inclure des événements non API capturés par AWS CloudTrail. Pour plus d'informations, consultez la section Événements non liés à l'API capturés par CloudTrail.

  - Agent utilisateur : agent utilisateur à l'origine de la demande d'API. Cette valeur vous indique si l'appel a été effectué à partir du AWS Management Console, d'un AWS service, AWS des SDK ou du AWS CLI.
  - CODE D'ERREUR : si le résultat a été déclenché par l'échec d'un appel d'API, le code d'erreur correspondant à cet appel est affiché.
  - Nom du service : nom DNS du service qui a tenté d'effectuer l'appel d'API ayant déclenché le résultat.

- RDS_LOGIN_ATTEMPT : indique qu'une tentative de connexion a été effectuée à la base de données potentiellement compromise 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 : indique si le AWS compte de l'appelant de l'API distant est lié à votre GuardDuty environnement. Si cette valeur est `true`, l'appelant de l'API est affilié à votre compte d'une manière ou d'une autre, tandis que si cette valeur est `false`, l'appelant de l'API vient de l'extérieur 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 qui a incité GuardDuty à générer le résultat.
- Emplacement : informations de localisation de l'adresse IP impliquée dans l'activité GuardDuty à l'origine de la recherche.
- Organisation — Informations relatives à l'adresse IP associée à l'activité à l'origine de la constatation auprès de l'organisation du GuardDuty fournisseur de services Internet.
- 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. Cela peut inclure tout utilisateur, emplacement, moment, compartiment, comportement de connexion ou organisation ASN inhabituel (non observé précédemment).
- Protocole inhabituel : protocole de connexion réseau impliqué dans l'activité GuardDuty à l'origine du résultat.
- Détails de l'agent : détails sur l'agent de sécurité actuellement déployé sur le cluster EKS de votre Compte AWS. Cela ne s'applique qu'aux types de résultat de la surveillance d'exécution EKS.
  - 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 qui a généré le résultat.

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 de ML évalue toutes les demandes d'API adressées à votre compte et identifie les événements anormaux associés aux tactiques utilisées par les adversaires. Le modèle de ML suit différents

facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée.

Vous trouverez des informations sur les facteurs de la demande d'API 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'élément CloudTrail UserIdentity, et les valeurs possibles sont les suivantes :`Root`,`IAMUser`,, `AssumedRole` `FederatedUser`ou. `AWSAccount` `AWSService`

Outre les détails disponibles pour tous les GuardDuty résultats associés à l'activité de l'API, AnomalousBehaviorles résultats contiennent des informations supplémentaires qui sont décrites dans la section suivante. Ces détails peuvent être consultés dans la console et sont également disponibles dans le fichier JSON du résultat.

- API anormales : liste des demandes d'API invoquées par l'identité de l'utilisateur à proximité de la demande d'API principale associée au résultat. Ce volet détaille plus en détail l'événement d'API de la manière suivante.
  - La première API répertoriée est l'API principale, qui est la demande d'API associée à l'activité observée présentant le plus haut risque. Il s'agit de l'API qui a déclenché le résultat et qui est corrélée à la phase d'attaque du type de résultat. Il s'agit également de l'API qui est détaillée dans la section Action de la console et dans le fichier JSON du résultat.
  - Toutes les autres API répertoriées sont des API anormales supplémentaires provenant de l'identité utilisateur répertoriée observée à proximité de l'API principale. S'il n'y a qu'une seule API dans la liste, le modèle de ML n'a identifié aucune demande d'API supplémentaire provenant de cette identité d'utilisateur comme anormale.
  - La liste des API est divisée selon qu'une API a été appelée avec succès ou non, ce qui signifie qu'une réponse d'erreur a été reçue. Le type de réponse d'erreur reçue est indiqué au-dessus de chaque API appelée sans succès. 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`.
  - Les API sont classées en fonction du service qui leur est associé.

> **Note**
>
> Pour plus de contexte, choisissez API historiques pour afficher les détails des principales API, jusqu'à un maximum de 20, généralement visibles à la fois pour l'identité de l'utilisateur et pour tous les utilisateurs du compte. Les API sont marquées comme Rare

(moins d'une fois par mois), Peu fréquent (quelques fois par mois) ou Fréquent (quotidien ou hebdomadaire), selon la fréquence à laquelle elles sont utilisées dans votre compte.

- Comportement inhabituel (compte) : cette section fournit des informations supplémentaires sur le comportement profilé de votre compte. Les informations suivies dans ce panneau incluent :
  - Organisation ASN : organisation ASN à partir de laquelle l'appel d'API anormal a été effectué.
  - Nom d'utilisateur : nom de l'utilisateur qui a effectué l'appel d'API anormal.
  - Agent utilisateur : agent utilisateur utilisé pour effectuer l'appel d'API anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
  - Type d'utilisateur : type d'utilisateur qui a effectué l'appel d'API 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 cette identité d'utilisateur effectuer cet appel d'API de cette manière au cours de la période de formation. Les informations supplémentaires suivantes concernant l'identité de l'utilisateur sont disponibles :
  - Organisation ASN : organisation ASN à partir de laquelle l'appel d'API anormal a été effectué.
  - Agent utilisateur : agent utilisateur utilisé pour effectuer l'appel d'API 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 de GuardDuty machine learning n'a jamais vu d'appels d'API effectués de cette manière vers ce bucket au cours de la période de formation. Les informations suivies dans cette section incluent :
  - Organisation ASN : organisation ASN à partir de laquelle l'appel d'API anormal a été effectué.
  - Nom d'utilisateur : nom de l'utilisateur qui a effectué l'appel d'API anormal.
  - Agent utilisateur : agent utilisateur utilisé pour effectuer l'appel d'API anormal. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `aws-cli` ou `Botocore`.
  - Type d'utilisateur : type d'utilisateur qui a effectué l'appel d'API 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.
  - Organisation ASN : organisation ASN 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.

  > **Note**
  >
  > La section Comportement historique fournit plus de contexte sur les noms d'utilisateur, les organisations ASN, 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 l'API Kubernetes associée au résultat.
- Nom d'utilisateur usurpé : l'utilisateur usurpé par `username`.
- Espace de noms : espace de noms Kubernetes au sein du cluster Amazon EKS où l'action s'est produite.
- Agent utilisateur : agent utilisateur associé à l'appel d'API Kubernetes. L'agent utilisateur est la méthode utilisée pour effectuer l'appel, comme `kubectl`.
- API : l'API Kubernetes appelée par `username` au sein du cluster Amazon EKS.
- Informations ASN : informations ASN, telles que l'organisation et le fournisseur de services Internet, associées à l'adresse IP de l'utilisateur à l'origine de cet appel.
- Jour de la semaine : jour de la semaine où l'appel d'API Kubernetes a été effectué.
- Autorisation[1] : verbe et la ressource Kubernetes dont l'accès est vérifié pour indiquer si le `username` peut utiliser l'API Kubernetes.
- Nom du compte de service[1] : compte de service associé à la charge de travail Kubernetes qui fournit une identité à la charge de travail.
- Registre[1] : registre de conteneurs associé à l'image de conteneur déployée dans la charge de travail Kubernetes.
- Image[1] : image du conteneur, sans les balises et le résumé associés, déployée dans la charge de travail Kubernetes.
- Configuration du préfixe d'image[1] : préfixe d'image pour lequel la configuration de sécurité du conteneur et de la charge de travail est activée, par exemple `hostNetwork` ou `privileged`, pour le conteneur utilisant l'image.
- Nom du sujet[1] : sujets, tels que `user`, `group` ou `serviceAccountName` qui sont liés à un rôle de référence dans un `RoleBinding` ou `ClusterRoleBinding`.
- Nom du rôle[1] : nom du rôle impliqué dans la création ou la modification des rôles ou de l'API `roleBinding`.

Anomalies basées sur le volume S3

Cette section détaille les informations contextuelles relatives aux anomalies basées sur le volume S3. Le résultat basé sur le volume (Exfiltration:S3/AnomalousBehavior) surveille le nombre inhabituel d'appels d'API S3 adressés par les utilisateurs aux compartiments S3, ce qui indique une exfiltration

potentielle de données. Les appels d'API S3 suivants sont surveillés pour détecter les anomalies basées sur le volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Les métriques suivantes aideront à établir une référence du comportement habituel lorsqu'une entité IAM 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'appels d'API `s3-api-name` invoqués par l'utilisateur IAM ou le rôle IAM (selon celui qui a été émis) associés au compartiment S3 concerné au cours des dernières 24 heures.
- Nombre d'appels d'API `s3-api-name` invoqués par l'utilisateur IAM ou le rôle IAM (selon celui qui a été émis) associés à tous les compartiments S3 au cours des dernières 24 heures.
- Nombre d'appels d'API `s3-api-name` entre tous les utilisateurs IAM ou rôles IAM (selon celui qui a été émis) associés au compartiment S3 concerné au cours des dernières 24 heures.

Anomalies basées sur l'activité de connexion RDS

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 pas 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.

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.

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 un échantillon de résultats, votre liste GuardDuty de résultats actuelle est renseignée avec un échantillon de résultat 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 la recherche de types, voir le Types de résultats tableau.

Génération d'échantillons de résultats via la GuardDuty console ou l'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 exemples de résultats uniques ne peuvent être générés que par le biais de l'API.

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 via l'CreateSampleFindingsAPI. Les valeurs disponibles pour les types de recherche sont répertoriées dans le Types de résultats tableau.

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.

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

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Le titre des exemples de résultats générés par ces méthodes commence toujours par [SAMPLE] dans la console. Les exemples de résultats ont une valeur de `"sample": true` dans la section additionalInfo des détails JSON du résultat.

Pour générer des résultats courants 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 lorsque vous souhaitez comprendre certains types de GuardDuty recherche et en savoir

plus sur ceux-ci. 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 plus d'informations, consultez Utilisation de l' GuardDuty essai gratuit de 30 jours.

GuardDuty est déjà activé dans votre compte avant d'exécuter le script du testeur

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 aux journaux d'audit Amazon EC2, Amazon EKS, Amazon S3, IAM et EKS :

- 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 Services AWS 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, consultez la section 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 celui-ci. AWS CloudFormation CDK prend en charge plusieurs 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 applications CDK pour approvisionner ou mettre AWS CloudFormation 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 pile CDK 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 instances Amazon EC2 incluent également les instances EC2 qui hébergent des nœuds EKS et des clusters ECS.

> **Types d'instances**
>
> GuardDuty crée `t3.micro` pour toutes les ressources à l'exception du groupe de nœuds Amazon EKS. EKS nécessitant au moins 2 cœurs, le nœud EKS possède un type d'`t3.medium`instance. Pour plus d'informations sur les types d'instances, consultez la section Tailles disponibles dans le guide des types d'instances Amazon EC2.

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* par le code de région dans lequel vous avez déployé les ressources :

   ```
   $ REGION=us-east-1
   ```

2. Le script du testeur n'est disponible que 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 instances Amazon EC2, 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.

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

AWS CLI

- *Exécutez la AWS CLI commande suivante pour afficher les résultats générés et remplacez us-east-1 et 12ABC34D567E8FA901BC2D34Example par des valeurs appropriées :*

  ```
  aws guardduty list-findings --region us-east-1 --detector-
  id 12abc34d567e8fa901bc2d34EXAMPLE
  ```

  `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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`— Mettez à jour la AWS CDK CLI vers une version compatible avec la version d'assemblage cloud requise ou vers la dernière version disponible. Pour plus d'informations, consultez la section Compatibilité avec les AWS CDK CLI.

- `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 console Amazon EC2 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 ainsi que 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, reportez-vous describe-instance-type-offeringsà la 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 Élevée indique que la ressource en question (une instance EC2 ou un ensemble d'informations d'identification de connexion d'utilisateur IAM) est compromise et 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 instance EC2 ou mettez-y fin, ou effectuez une rotation des informations d'identification IAM. 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.

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.

Niveau de gravité	Plage de valeurs
• Vérifiez les autorisations qui sont attachées au rôle IAM impliqué, à l'utilisateur, au groupe ou à l'ensemble d'informations d'identification. 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.	

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. Cela est dû au fait que ce résultat représente un même problème de sécurité lié à l'instance indiquant que le port SSH de l'instance n'est pas correctement sécurisé contre ce type d'activité. Toutefois, si une activité d'accès SSH 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 de flux CloudTrail ou dans ceux de votre VPC.

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.

Localisation et analyse des GuardDuty résultats

Utilisez la procédure suivante pour consulter et analyser vos GuardDuty résultats.

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 plus d’informations, consultez 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 consulter son document JSON 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 du résultat et définit sa valeur à zéro. De cette façon GuardDuty , vous savez que vous pouvez ignorer ces résultats en toute sécurité.

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 Source 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 Types de recherche IAM

Les résultats suivants, spécifiques aux entités IAM et aux clés d'accès, 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 Source de données de base.

Pour tous les résultats liés à IAM, nous vous recommandons d'examiner l'entité en question et de vous assurer que ses autorisations respectent la bonne pratique 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

Une API utilisée pour accéder à un AWS environnement a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule identité d'utilisateur. L'API observée 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 API dans cette catégorie sont `GetPasswordData`, `GetSecretValue` et `GenerateDbAuthToken`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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

Une API utilisée pour contourner les mesures défensives a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule identité d'utilisateur. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de couvrir ses traces et d'éviter d'être détecté. Les API de cette catégorie sont généralement des opérations de suppression, de désactivation ou d'arrêt, telles que `DeleteFlowLogs`, `DisableAlarmActions` ou `StopLogging`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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

Une API couramment utilisée pour découvrir des ressources a été invoquée de manière anormale.

Gravité par défaut : faible

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule identité d'utilisateur. L'API observée est généralement associée à la phase de découverte d'une attaque lorsqu'un adversaire collecte des informations pour déterminer si votre AWS environnement est vulnérable à une attaque de plus grande envergure. Les API de cette catégorie sont généralement des opérations d'obtention, de description ou de liste, telles que `DescribeInstances`, `GetRolePolicy` ou `ListAccessKeys`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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

Une API couramment utilisée pour collecter des données à partir d'un AWS environnement a été invoquée de manière anormale.

Gravité par défaut : élevée

- Source de données : événement CloudTrail de gestion

Ce résultat vous informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule identité d'utilisateur. 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 en utilisant l'empaquetage et le chiffrement pour éviter d'être détecté. Les API pour ce type de résultat 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 demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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 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 informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à

proximité par une seule identité d'utilisateur. L'API observée est généralement associée à des tactiques d'impact où un adversaire tente de perturber les opérations et de manipuler, d'interrompre ou de détruire les données de votre compte. Les API pour ce type de résultat sont généralement des opérations de suppression, de mise à jour ou de saisie, telles que `DeleteSecurityGroup`, `UpdateUser` ou `PutBucketPolicy`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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 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 informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule identité d'utilisateur. L'API observée est généralement associée à la phase d'accès initiale d'une attaque lorsqu'un adversaire tente d'accéder à votre environnement. Les API de cette catégorie sont généralement des opérations d'obtention de jeton ou de session, telles que `GetFederationToken`, `StartSession` ou `GetAuthorizationToken`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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

Une API a été invoquée depuis une machine Kali Linux.

Gravité par défaut : moyenne

- Source de données : événement CloudTrail de gestion

Ce résultat vous indique qu'une machine exécutant Kali Linux effectue des appels d'API 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 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, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

PenTest:IAMUser/ParrotLinux

Une API a été invoquée par 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 effectue des appels d'API 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 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, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

PenTest:IAMUser/PentooLinux

Une API a été invoquée par 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 effectue des appels d'API 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 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, vos informations d'identification peuvent être compromises. Pour plus d'informations, consultez Corriger les informations d'identification potentiellement compromises AWS.

Persistence:IAMUser/AnomalousBehavior

Une 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 informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule identité d'utilisateur. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre environnement et tente de le conserver. Les API de cette catégorie sont généralement des opérations de création, d'importation ou de modification, telles que `CreateAccessKey`, `ImportKeyPair` ou `ModifyInstanceAttribute`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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

Une API a été invoquée à l'aide d'informations d'identification 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. Les AWS services doivent plutôt être accessibles

en utilisant les informations d'identification temporaires AWS Security Token Service (STS) dotées du moindre privilège. Lorsqu' AWS STS n'est pas pris en charge, il est recommandé d'utiliser les informations d'identification d'utilisateur IAM. Pour de plus amples informations, veuillez consulter Bonnes pratiques IAM.

> **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'appel d'API utilisé est répertorié dans les détails d'un résultat. Si la détection des menaces S3 n'est pas activée, ce résultat ne peut être déclenché que par les API du journal des événements. 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 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 informe qu'une demande d'API anormale a été observée dans votre compte. Ce résultat peut inclure une seule API ou une série de demandes d'API connexes effectuées à proximité par une seule identité d'utilisateur. L'API observée est généralement associée à des tactiques d'escalade des privilèges dans le cadre desquelles un adversaire tente d'obtenir des autorisations de niveau supérieur sur un environnement. Les API de cette catégorie impliquent généralement des opérations qui modifient les rôles, les utilisateurs et les politiques IAM, telles que `AssociateIamInstanceProfile`, `AddUserToGroup` ou `PutUserPolicy`.

Cette demande d'API a été identifiée comme anormale par GuardDuty le modèle d'apprentissage automatique (ML) de détection des 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. Le modèle de ML suit différents facteurs de la demande d'API, tels que l'utilisateur à l'origine de la demande, l'emplacement d'origine de la demande et l'API spécifique qui a été demandée. Vous trouverez des informations sur les facteurs de la demande d'API inhabituels par rapport à l'identité de l'utilisateur qui a invoqué la demande dans les détails du résultat.

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

Une API a été invoquée depuis une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API qui peut répertorier ou décrire vos ressources AWS dans un compte au sein de votre environnement a été appelée depuis 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

Une API a été invoquée depuis une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API qui peut répertorier ou décrire vos ressources AWS dans un compte au sein de votre environnement a été appelée depuis une adresse IP figurant sur une liste de menaces personnalisées. 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

Une API a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API qui peut répertorier ou décrire vos ressources AWS dans un compte au sein de votre environnement 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. 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 utilisateurs IAM. 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 vous informe que plusieurs connexions réussies à la console de la part du même utilisateur IAM ont été observées simultanément dans divers emplacements 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

Des informations d'identification qui ont été créées exclusivement pour une instance EC2 via un rôle de lancement d'instance sont utilisées depuis un autre compte au sein d' AWS.

Gravité par défaut : élevée*

> **Note**
>
> La gravité par défaut de ce résultat est élevée. Toutefois, si l'API a été invoquée 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 indique lorsque les informations d'identification de votre instance EC2 sont utilisées pour appeler des API à partir d'une adresse IP appartenant à un AWS compte différent de celui dans lequel s'exécute l'instance EC2 associée.

AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exemple, AWS applications, EC2 ou Lambda). En revanche, les utilisateurs autorisés peuvent exporter les informations d'identification de leurs instances EC2 pour effectuer des appels d'API légitimes. Si le `remoteAccountDetails.Affiliated` champ est `True` l'API a été invoquée depuis un compte associé à votre AWS environnement. Pour éviter une attaque potentielle et vérifier la légitimité de l'activité, contactez l'utilisateur IAM à qui 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'instance EC2 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 informations d'identification

EC2 pour déterminer s'il existe un cas d'utilisation permettant à 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 les détails JSON du résultat.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Des informations d'identification qui ont été créées exclusivement pour une instance EC2 via un rôle de lancement d'instance sont utilisées depuis 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 opérations d' AWS API à l'aide AWS d'informations d'identification temporaires créées sur une instance EC2 de votre AWS environnement. L'instance EC2 répertoriée est peut-être compromise et les informations d'identification temporaires de cette instance ont peut-être été exfiltrées vers un hôte distant situé à l'extérieur de. AWS AWS ne recommande pas de redistribuer les informations d'identification temporaires en dehors de l'entité qui les a créées (par exemple, AWS applications, EC2 ou Lambda). En revanche, les utilisateurs autorisés peuvent exporter les informations d'identification de leurs instances EC2 pour effectuer des appels d'API 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 la mise en réseau est configurée pour acheminer le trafic Internet de telle sorte qu'il sorte d'une passerelle sur site plutôt que d'une passerelle Internet VPC (IGW). Les configurations courantes, telles que AWS Outposts ou les connexions VPN VPC, peuvent entraîner l'acheminement 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'adresse IPv4 de l'appelant d'API avec l'adresse IP ou la plage d'adresses CIDR de votre passerelle Internet sur site. 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

Une API a été invoquée depuis une adresse IP malveillante connue.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous indique qu'une opération d'API (par exemple, une tentative de lancement d'une instance EC2, de création d'un nouvel utilisateur IAM 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

Une API a été invoquée depuis 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 opération d'API (par exemple, une tentative de lancement d'une instance EC2, de création d'un nouvel utilisateur IAM 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

Une API a été appelée depuis une adresse IP du nœud de sortie Tor.

Gravité par défaut : moyenne

- Source de données : événements CloudTrail de gestion

Ce résultat vous informe qu'une opération d'API (par exemple, une tentative de lancer une instance EC2, de créer un utilisateur IAM ou de modifier vos privilèges AWS) a été invoquée depuis une adresse IP de 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.

Types de recherche dans les journaux d'audit EKS

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'utilisateur Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'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 l'API 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'utilisateur Amazon EKS. 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 plus d’informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour accéder aux informations d'identification ou aux secrets 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API 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. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'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`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, le cas échéant, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'utilisateur Amazon EKS. 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 plus d’informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'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'action d'API 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 l'utilisateur Amazon EKS.

Pour plus d’informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/TorIPCaller

Une API couramment utilisée pour accéder aux informations d'identification ou aux secrets d'un cluster Kubernetes a été invoquée à partir d'une adresse IP de nœud de sortie Tor.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée aux tactiques d'accès aux informations d'identification lorsqu'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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour contourner les mesures défensives a été invoquée à partir d'une adresse IP malveillante connue.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API 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'évasion défensive dans lesquelles un adversaire tente de masquer 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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour contourner les mesures défensives a été invoquée depuis une adresse IP figurant sur une liste de menaces personnalisée.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API 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. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de masquer 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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour contourner les mesures défensives a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés.

L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de masquer ses actions pour éviter d'être détecté. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'action d'API 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 l'utilisateur Amazon EKS.

Pour plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

DefenseEvasion:Kubernetes/TorIPCaller

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée à des tactiques d'évasion défensive dans lesquelles un adversaire tente de masquer 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 l'API

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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/MaliciousIPCaller

Une API couramment utilisée pour découvrir des ressources dans un cluster Kubernetes a été invoquée à partir d'une adresse IP.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est couramment utilisée lors de la phase de découverte d'une attaque au cours de laquelle un pirate 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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Une API couramment utilisée pour découvrir des ressources dans 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 d'audit EKS

Ce résultat vous informe qu'une API 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. L'API observée est couramment utilisée lors de la phase de découverte d'une attaque au cours de laquelle un pirate 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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour découvrir des ressources dans un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée 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'action d'API 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 l'utilisateur Amazon EKS.

Pour plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Discovery:Kubernetes/TorIPCaller

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est couramment utilisée lors de la phase de découverte d'une attaque au cours de laquelle un pirate 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`, recherchez pourquoi l'utilisateur anonyme a été autorisé à invoquer l'API et révoquez les autorisations, si nécessaire, en suivant les instructions de la section Bonnes pratiques de sécurité pour Amazon EKS dans le guide de l'utilisateur Amazon EKS. 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 plus d'informations, consultez 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 d'audit EKS

Ce résultat vous informe qu'une commande a été exécutée dans un pod au sein de l'espace de noms `kube-system` à l'aide de l'API Kubernetes exec. L'espace de noms `kube-system` 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/MaliciousIPCaller

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API 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.

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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API 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. 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.

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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

Une API couramment utilisée pour altérer les ressources d'un cluster Kubernetes a été invoquée par un utilisateur non authentifié.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée 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'action d'API 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 l'utilisateur Amazon EKS.

Pour plus d’informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Impact:Kubernetes/TorIPCaller

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée à des tactiques d'impact où un adversaire tente de manipuler, d'interrompre ou de détruire des données au sein de votre environnement AWS . 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 l'API 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'utilisateur Amazon EKS. 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 plus d’informations, consultez 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 d'audit EKS

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 plus d’informations, consultez 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 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée à partir d'une adresse IP associée à une activité malveillante connue. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de le conserver.

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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API 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. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de le conserver.

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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API a bien été invoquée par l'utilisateur `system:anonymous`. Les appels d'API effectués par `system:anonymous` ne sont pas authentifiés. L'API observée est généralement associée aux tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster et tente de le conserver. Cette activité indique qu'un accès anonyme ou non authentifié est autorisé sur l'action d'API 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 l'utilisateur Amazon EKS.

Pour plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Persistence:Kubernetes/TorIPCaller

Une 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 d'audit EKS

Ce résultat vous informe qu'une opération d'API a été invoquée depuis une adresse IP du nœud de sortie Tor. L'API observée est généralement associée à des tactiques de persistance dans le cadre desquelles un adversaire a obtenu l'accès à votre cluster Kubernetes et tente de le conserver. 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 l'API 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'utilisateur Amazon EKS. 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 plus d'informations, consultez 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 d'audit EKS

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 plus d’informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

Policy:Kubernetes/AnonymousAccessGranted

L'utilisateur **`system:anonymous`** a obtenu l'autorisation d'API sur un cluster Kubernetes.

Gravité par défaut : élevée

- Fonctionnalité : journaux d'audit EKS

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 opérations d'API 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 l'utilisateur Amazon EKS. 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 plus d'informations, consultez 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 d'audit EKS

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 plus d'informations, consultez 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 d'audit EKS

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 plus d’informations, consultez 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 d'audit EKS

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 plus d'informations, consultez Correction des résultats de la surveillance des journaux d'audit EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Une API Kubernetes couramment utilisée pour accéder aux secrets a été invoquée de manière anormale.

Gravité par défaut : moyenne

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API anormale visant à récupérer des secrets de cluster sensibles a été invoquée par un utilisateur Kubernetes dans votre cluster. L'API observée est généralement associée 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'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster EKS et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle de ML suit plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 d'audit EKS

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'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit aussi plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 d'audit EKS

Ce résultat vous informe qu'une commande a été exécutée dans un pod à l'aide de l'API Kubernetes exec. L'API Kubernetes exec 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'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit aussi plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 d'audit EKS

Ce résultat vous informe qu'une charge de travail a été lancée avec un conteneur privilégié dans votre cluster Amazon EKS. 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 de ML évalue toutes les activités d'API utilisateur et des images de conteneur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit également plusieurs facteurs liés au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 plus d'informations, consultez 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 d'audit EKS

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 de ML évalue toutes les activités d'API utilisateur et des images de conteneur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit également plusieurs facteurs liés au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 plus d'informations, consultez 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 d'audit EKS

Ce résultat vous informe qu'une charge de travail Kubernetes a été créée ou modifiée de manière anormale, par exemple en raison d'une activité d'API, de nouvelles images de conteneur ou d'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 de ML évalue toutes les activités d'API utilisateur et des images de conteneur au sein de votre cluster EKS. Ce modèle de machine learning identifie également les événements anormaux associés aux techniques utilisées par un utilisateur non autorisé. Le modèle de ML suit également plusieurs facteurs liés au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 plus d'informations, consultez Règles de suppression.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Rôle hautement permissif ou ClusterRole créé ou modifié de manière anormale.

Gravité par défaut : faible

- Fonctionnalité : journaux d'audit EKS

Ce résultat vous informe qu'une opération d'API anormale visant à créer un `Role` ou un `ClusterRole` avec des autorisations excessives a été appelée par un utilisateur Kubernetes dans 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'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster Amazon EKS et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle de ML suit également plusieurs facteurs liés au fonctionnement de l'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'agent utilisateur utilisé, les images de conteneur observées dans votre compte et l'espace de noms

exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 d'audit EKS

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'API observée a été identifiée comme anormale par le modèle d'apprentissage automatique (ML) de détection d' GuardDuty anomalies. Le modèle de ML évalue toutes les activités d'API utilisateur au sein de votre cluster Amazon EKS et identifie les événements anormaux associés aux techniques utilisées par des utilisateurs non autorisés. Le modèle de ML suit également plusieurs facteurs de l'opération d'API, tels que l'utilisateur qui fait la demande, le lieu d'origine de la demande, l'autorisation en cours de vérification et l'espace de noms exploité par l'utilisateur. Vous pouvez trouver les détails inhabituels de la demande d'API 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 plus d'informations, consultez 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 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
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

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.

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

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 ECS potentiellement compromis.

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 ECS potentiellement compromis.

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 Bases de données Amazon Aurora et Amazon RDS 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
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin
- CredentialAccess:RDS/TorIPCaller.FailedLogin

- Discovery:RDS/TorIPCaller

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 Bases de données Amazon Aurora et Amazon RDS 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 Anomalies basées sur l'activité de connexion RDS.

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 Bases de données Amazon Aurora et Amazon RDS 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 Anomalies basées sur l'activité de connexion RDS.

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 Bases de données Amazon Aurora et Amazon RDS 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 Anomalies basées sur l'activité de connexion RDS.

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 recherche liés à la surveillance du temps

Amazon GuardDuty génère les résultats de surveillance du temps d'exécution suivants pour indiquer les menaces potentielles en fonction du comportement au niveau du système d'exploitation des hôtes et conteneurs Amazon EC2 dans vos clusters Amazon EKS, des charges de travail Fargate et Amazon ECS et des 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 coder en HTML les champs de résultat lorsque vous les affichez sur une page Web.

Rubriques

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B

- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- 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

CryptoCurrency:Runtime/BitcoinTool.B

Une instance Amazon EC2 ou un conteneur interroge une adresse IP associée à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertoriée ou un conteneur de votre environnement AWS interroge une adresse IP associée à une activité liée à une cryptomonnaie. 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 instance EC2 ou un conteneur pour exploiter ou gérer de la cryptomonnaie, ou si l'un d'eux est impliqué d'une autre manière dans une activité de blockchain, le résultat CryptoCurrency:Runtime/BitcoinTool.B 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 `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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Backdoor:Runtime/C&CActivity.B

Une instance Amazon EC2 ou un conteneur 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 informe qu'une instance Amazon EC2 répertoriée ou un conteneur de votre environnement AWS interroge un nom de domaine associé à un serveur de commande et de contrôle 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 (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.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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

UnauthorizedAccess:Runtime/TorRelay

Votre instance Amazon EC2 ou un conteneur est en train de se connecter à un réseau Tor en tant que relais Tor.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'une instance EC2 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

UnauthorizedAccess:Runtime/TorClient

Votre instance Amazon EC2 ou un conteneur est en train de se connecter à un nœud Tor Guard ou Authority.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'une instance EC2 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 instance EC2 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/BlackholeTraffic

Une instance Amazon EC2 ou un conteneur tente de communiquer avec une adresse IP d'un hôte distant qui est un trou noir connu.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une instance ou un conteneur EC2 répertorié dans 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DropPoint

Une instance ou un conteneur Amazon EC2 tente de communique 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 d'exécution

Ce résultat vous indique qu'une instance ou un conteneur EC2 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine associé à une activité de cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertoriée ou un conteneur de votre environnement AWS interroge un nom de domaine associé à une activité liée au Bitcoin ou à une autre cryptomonnaie. 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 instance EC2 ou un conteneur pour exploiter ou gérer de la cryptomonnaie, ou si l'un d'eux est impliqué d'une autre manière dans une activité de blockchain, le résultat CryptoCurrency:Runtime/BitcoinTool.B!DNS 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

Backdoor:Runtime/C&CActivity.B!DNS

Une instance Amazon EC2 ou un conteneur 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 informe qu'une instance Amazon EC2 ou le conteneur de votre environnement AWS interroge un nom de domaine associé à un serveur de commande et de contrôle connu.

L'instance EC2 ou le conteneur répertorié 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 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.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **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`.

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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/BlackholeTraffic!DNS

Une instance Amazon EC2 ou un conteneur interroge le nom d'un domaine qui est redirigé vers l'adresse IP d'un trou noir.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertoriée ou le conteneur de votre environnement AWS pourrait être compromis, car il 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.

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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DropPoint!DNS

Une instance Amazon EC2 ou un conteneur 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

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'une instance ou un conteneur EC2 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DGADomainRequest.C!DNS

Une instance Amazon EC2 ou un conteneur interroge des domaines générés par des algorithmes. Ces domaines sont couramment utilisés par des programmes malveillants et peuvent constituer une indication d'instance EC2 ou de conteneur compromis.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertoriée ou le conteneur de votre environnement AWS tente d'interroger des DGA (algorithmes de génération de noms de domaine). Votre ressource a peut-être été 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 des domaines DGA 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/DriveBySourceTraffic!DNS

Une instance Amazon EC2 ou un conteneur 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

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertorié ou le conteneur de votre environnement AWS pourrait être compromis, car il 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 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

Trojan:Runtime/PhishingDomainRequest!DNS

Une instance Amazon EC2 ou un conteneur interroge des domaines impliqués dans des attaques d'hameçonnage.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe qu'une instance EC2 ou un conteneur 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 ou le conteneur essaie peut-être de récupérer des données sensibles stockées sur un site Web d'hameçonnage ou d'en configurer un. Votre instance EC2 ou le conteneur pourrait 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/AbusedDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine de mauvaise réputation associé à des domaines abusifs connus.

Gravité par défaut : moyenne

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertoriée ou le conteneur 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 ou le conteneur peut être compromis, 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.

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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/BitcoinDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur interroge un nom de domaine de mauvaise réputation associé à une activité liée à une cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertoriée ou le conteneur de votre environnement AWS interroge un nom de domaine de mauvaise réputation associé à une activité liée au Bitcoin ou à une autre cryptomonnaie. 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 instance EC2 ou le conteneur pour exploiter ou gérer de la cryptomonnaie, ou si ces ressources sont impliquées d'une autre manière dans une activité de 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/MaliciousDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur interroge un de domaine de mauvaise réputation associé à des domaines malveillants connus.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertoriée ou le conteneur 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.

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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Une instance Amazon EC2 ou un conteneur 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

- Fonctionnalité : surveillance d'exécution

Ce résultat vous informe que l'instance EC2 répertorié ou le conteneur 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.

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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Une instance Amazon EC2 ou un conteneur effectue des recherches DNS résolues en service de métadonnées d'instance.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

> **Note**
>
> Actuellement, ce type de recherche n'est pris en charge que pour l'architecture AMD64.

Ce résultat vous indique qu'une instance ou un conteneur EC2 de votre AWS environnement interroge un domaine qui correspond à l'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.

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 ce résultat, vous devez évaluer s'il existe une application vulnérable en cours d'exécution sur l'instance EC2 ou le conteneur ou si une personne a utilisé un navigateur pour accéder au domaine identifié dans le résultat. 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 ce résultat était lié à l'un ou l'autre des cas ci-dessus, révoquez la session associée à l'instance EC2.

Certains AWS clients associent intentionnellement l'adresse IP des métadonnées à un nom de domaine sur leurs serveurs DNS 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 Domaine de demande DNS ou l'ID de l'image du conteneur. La valeur

Domaine de demande DNS doit correspondre au domaine que vous avez mappé sur 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 plus d'informations, consultez 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 être le signe d'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 plus d'informations, consultez 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 plus d'informations, consultez 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Une tentative d'évasion du conteneur via l'agent de libération de CGroups 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 plus d'informations, consultez 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 Amazon EC2.

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 plus d'informations, consultez 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 instance Amazon EC2.

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 plus d'informations, consultez 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 instance Amazon EC2.

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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/ReverseShell

Un processus dans un conteneur ou une instance Amazon EC2 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 instance Amazon EC2 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Impact:Runtime/CryptoMinerExecuted

Un conteneur ou une instance Amazon EC2 exécute un fichier binaire associé à une activité d'exploitation de cryptomonnaie.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Ce résultat vous indique qu'un conteneur ou une instance EC2 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 être le signe d'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 plus d’informations, consultez 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 plus d'informations, consultez 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 (Amazon EC2).

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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/SuspiciousTool

Un conteneur ou une instance Amazon EC2 exécute un fichier binaire ou un script fréquemment utilisé dans des scénarios de sécurité offensifs tels que l'engagement de pentests.

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 instance ou un conteneur EC2 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'instance ou le conteneur EC2 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/SuspiciousCommand

Une commande suspecte a été exécutée sur une instance Amazon EC2 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 instance Amazon EC2 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

DefenseEvasion:Runtime/SuspiciousCommand

Une commande a été exécutée sur l'instance Amazon EC2 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 plus d'informations, consultez Corriger les résultats de la surveillance de l'exécution.

DefenseEvasion:Runtime/PtraceAntiDebugging

Un processus dans un conteneur ou une instance Amazon EC2 a exécuté une mesure anti-débogage à l'aide de l'appel système ptrace.

Gravité par défaut : faible

- Fonctionnalité : surveillance d'exécution

Ce résultat montre qu'un processus exécuté sur une instance Amazon EC2 ou un conteneur au sein de votre AWS environnement a utilisé l'appel système ptrace avec l'option. `PTRACE_TRACEME` 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 plus d’informations, consultez Corriger les résultats de la surveillance de l'exécution.

Execution:Runtime/MaliciousFileExecuted

Un fichier exécutable malveillant connu a été exécuté sur une instance ou un conteneur Amazon EC2.

Gravité par défaut : élevée

- Fonctionnalité : surveillance d'exécution

Cette découverte vous indique qu'un exécutable malveillant connu a été exécuté sur une instance Amazon EC2 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 plus d'informations, voir Corriger les résultats de la surveillance de l'exécution.

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 Source 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 Protection Amazon S3 sur Amazon GuardDuty.

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
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write

- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

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.

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
- Types de recherche liés à la surveillance du temps
- Types de résultat IAM
- Types de recherche dans les journaux d'audit EKS
- Types de résultat de la protection Lambda
- 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 S3

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	Journaux DNS	Élevée
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Journaux DNS	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Journaux DNS	Medium
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Journaux DNS	Élevée
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Journaux DNS	Élevée
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Journaux DNS	Faible
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Journaux DNS	Medium
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Journaux DNS	Élevée
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Journaux DNS	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Journaux DNS	Élevée
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Journaux DNS	Élevée
Trojan:EC2/DropPoint!DNS	Amazon EC2	Journaux DNS	Medium
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Journaux DNS	Élevée
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Journaux DNS	Élevée
Execution:Container/MaliciousFile	Conteneur	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:Container/SuspiciousFile	Conteneur	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:EC2/MaliciousFile	EC2	Protection contre les logiciels malveillants EBS	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	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:ECS/MaliciousFile	ECS	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:ECS/SuspiciousFile	ECS	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:Kubernetes/MaliciousFile	Kubernetes	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
Execution:Kubernetes/SuspiciousFile	Kubernetes	Protection contre les logiciels malveillants EBS	Varie en fonction de la menace détectée
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Journaux d’audit EKS	Medium
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d’audit EKS	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Élevée
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Élevée
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Élevée
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Journaux d'audit EKS	Faible
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Medium
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Medium
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d'audit EKS	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Discovery:Kubernetes/TorIPCaller	Kubernetes	Journaux d'audit EKS	Medium
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	Journaux d'audit EKS	Medium
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Journaux d'audit EKS	Medium
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Journaux d'audit EKS	Faible
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d'audit EKS	Élevée
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d'audit EKS	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d’audit EKS	Élevée
Impact:Kubernetes/TorIPCaller	Kubernetes	Journaux d’audit EKS	Élevée
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	Journaux d’audit EKS	Medium
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Journaux d’audit EKS	Medium
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Journaux d’audit EKS	Medium
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Journaux d’audit EKS	Élevée
Persistence:Kubernetes/TorIPCaller	Kubernetes	Journaux d’audit EKS	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Journaux d'audit EKS	Élevée
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Journaux d'audit EKS	Élevée
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Journaux d'audit EKS	Medium
Policy:Kubernetes/ExposedDashboard	Kubernetes	Journaux d'audit EKS	Medium
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	Journaux d'audit EKS	Moyenne*

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	Journaux d'audit EKS	Faible
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Journaux d'audit EKS	Élevée
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Journaux d'audit EKS	Élevée
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	Journaux d'audit EKS	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	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Faible
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Élevée
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Variable*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Medium
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
CredentialAccess:RDS/TorIPCaller.FailedLogin	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Medium
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Élevée
Discovery:RDS/MaliciousIPCaller	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Medium
Discovery:RDS/TorIPCaller	Bases de données Amazon Aurora et Amazon RDS prises en charge	Surveillance de l'activité de connexion RDS	Medium
Backdoor:Runtime/C&CActivity.B	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Backdoor:Runtime/C&CActivity.B!DNS	Instance, cluster EKS, cluster ECS 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, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/FilelessExecution	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
DefenseEvasion:Runtime/ProcessInjection.Proc	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
DefenseEvasion:Runtime/PtraceAntiDebugging	Instance, cluster EKS, cluster ECS 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, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Execution:Runtime/MaliciousFileExecuted	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Execution:Runtime/NewBinaryExecuted	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Execution:Runtime/NewLibraryLoaded	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Execution:Runtime/SuspiciousCommand	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Variable
Execution:Runtime/SuspiciousTool	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Variable
Execution:Runtime/ReverseShell	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Impact:Runtime/AbusedDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Impact:Runtime/BitcoinDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Impact:Runtime/CryptoMinerExecuted	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Impact:Runtime/MaliciousDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Faible
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
PrivilegeEscalation:Runtime/RuncContainerEscape	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Object:S3/MaliciousFile	S3Object	Protection contre les logiciels malveillants pour S3	Élevée
Trojan:Runtime/BlackholeTraffic	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
Trojan:Runtime/BlackholeTraffic!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Trojan:Runtime/DropPoint	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Trojan:Runtime/DGADomainRequest.C!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Trojan:Runtime/DriveBySourceTraffic!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
Trojan:Runtime/DropPoint!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Medium
Trojan:Runtime/PhishingDomainRequest!DNS	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
UnauthorizedAccess:Runtime/TorClient	Instance, cluster EKS, cluster ECS ou conteneur	Surveillance d'exécution	Élevée
UnauthorizedAccess:Runtime/TorRelay	Instance, cluster EKS, cluster ECS 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
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

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
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
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*

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
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
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*

Type de résultat	Type de ressource	Source de données/fonctionnalité de base	Gravité du résultat
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 GuardDuty des résultats.

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. Les listes d'adresses IP fiables empêchent de générer des résultats non liés au DNS à partir d'adresses IP que vous considérez comme fiables, tandis que les listes d'informations sur les menaces vous alerteront GuardDuty en cas d'activité provenant d'adresses IP définies par l'utilisateur.

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 de protection contre les GuardDuty programmes malveillants pour EC2 et quelles sont les raisons pour lesquelles votre instance Amazon EC2 ou vos volumes Amazon EBS concernés peuvent avoir été ignorés pendant le processus de numérisation.

[Signalement des faux positifs dans GuardDuty Malware Protection for EC2]

Découvrez l'expérience faussement positive dans GuardDuty Malware Protection for EC2 et comment vous pouvez signaler les fausses détections de menaces positives.

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'aide de l'CreateFilterAPI à l'aide de JSON. 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. Choisissez Ajouter des critères de filtre au-dessus de la liste affichée de vos GuardDuty résultats.
2. Dans la liste développée d'attributs, sélectionnez l'attribut que vous souhaitez spécifier comme critères pour votre filtre, comme ID de compte ou Type d'action.

   > **Note**
   >
   > Consultez le tableau des attributs de filtre sur cette page pour obtenir la liste des attributs que vous pouvez utiliser pour créer des critères de filtre.

3. Dans le champ de texte affiché, spécifiez une valeur pour chaque attribut sélectionné, puis choisissez Appliquer.

   > **Note**
   >
   > Une fois que vous avez appliqué un filtre, vous pouvez convertir le filtre pour exclure les résultats qui correspondent au filtre en choisissant le point noir à gauche du nom du filtre. Cela permet de créer un filtre « not equals » pour l'attribut sélectionné.

4. Pour enregistrer les attributs spécifiés et leurs valeurs (critères de filtre) en tant que filtre, sélectionnez Save (Enregistrer). Saisissez le nom et la description du filtre, puis choisissez Terminé.

Attributs du filtre

Lorsque vous créez des filtres ou que vous triez des résultats à l'aide des opérations d'API, vous devez spécifier des critères de filtre au format JSON. Ces critères de filtre sont en corrélation avec le JSON détaillé 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 champs JSON 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 l'utilisez `severity` avec API AWS CLI, ou AWS CloudFormation, une valeur numérique lui est attribuée. Pour plus d'informations, consultez FindingCriteria dans le 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. Identifiant principal
Nom d’utilisateur	ressource. accessKeyDetails.Nom d'utilisateur
Type utilisateur	ressource. accessKeyDetails.Type d'utilisateur
ID de profil d'instance IAM	Resource.InstanceDetails. iamInstanceProfile .id
ID d’instance	resource.instanceDetails.instanceId
ID d'image d'instance	resource.instanceDetails.imageId

Nom de champ de console	Nom de champ JSON
Clé de balise d'instance	resource.instanceDetails.tags.key
Valeur de balise d'instance	resource.instanceDetails.tags.value
Adresse IPv6	resource.instanceDetails.networkInterfaces.ipv6Addresses
Adresse IPv4 privée	Resource.InstanceDetails.Interfaces réseau. privateIpAddresses. privateIpAddress
Nom DNS public	Resource.InstanceDetails.Interfaces réseau. publicDnsName
IP publique	resource.instanceDetails.networkInterfaces.publicIp
ID du groupe de sécurité	resource.instanceDetails.networkInterfaces.securityGroups.groupId
Nom du groupe de sécurité	resource.instanceDetails.networkInterfaces.securityGroups.groupName
ID de sous-réseau (subnet)	resource.instanceDetails.networkInterfaces.subnetId
ID du VPC	resource.instanceDetails.networkInterfaces.vpcId
ARN d'Outpost	resource.instanceDetails.outpostARN
Type de ressource	resource.resourceType
Autorisations du compartiment	resource.s3 .publicAccess.EffectivePermission BucketDetails
Nom du compartiment	resource.s3 .name BucketDetails
Clé de balise du compartiment	ressource.s3 .tags .key BucketDetails

Nom de champ de console	Nom de champ JSON
Valeur de balise de compartiment	ressource.s3 .tags .value BucketDetails
Type de compartiment	ressource.s3 .type BucketDetails
Type d'action	service.action.actionType
API appelée	service.action. awsApiCallAPI d'action
Type d'appelant d'API	service.action. awsApiCallAction. Type d'appelant
Code d'erreur d'API	service.action. awsApiCallAction. Code d'erreur
Ville de l'appelant d'API	service.action. awsApiCallAction. remoteIpDetails.ville.Nom de la ville
Pays de l'appelant d'API	service.action. awsApiCallAction. remoteIpDetails.country.CountryName
Adresse IPv4 de l'appelant d'API	service.action. awsApiCallAction. remoteIpDetails.Adresse IP v4
Adresse IPv6 de l'appelant de l'API	service.action. awsApiCallAction. remoteIpDetailsAdresse IP V6
ID ASN de l'appelant d'API	service.action. awsApiCallAction. remoteIpDetails.organisation.asn
Nom ASN de l'appelant d'API	service.action. awsApiCallAction. remoteIpDetails.Organisation.asnorg
Nom du service de l'appelant d'API	service.action. awsApiCallAction.ServiceName
Domaine de demande DNS	service.action. dnsRequestAction.domaine
Suffixe de domaine de demande DNS	service.action. dnsRequestAction. domainWithSuffix

Nom de champ de console	Nom de champ JSON
Connexion réseau bloquée	service.action. networkConnectionAction.blo qué
Direction de la connexion réseau	service.action. networkConnectionAction. Direction de connexion
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.Nom de la ville
Pays de la connexion réseau	service.action. networkConnectionAction. remoteIpDetails.country.CountryName
Adresse IPv4 distante de la connexion réseau	service.action. networkConnectionAction. remoteIpDetails.Adresse IP v4
Adresse IPv6 distante de connexion réseau	service.action. networkConnectionAction. remoteIpDetailsAdresse IP V6
ID ASN de l'adresse IP distante de la connexion réseau	service.action. networkConnectionAction. remoteIpDetails.organisation.asn
Nom ASN de l'adresse IP distante 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 IPv4 de l'appelant de l'API Kubernetes	service.action. kubernetesApiCallAction. remoteIpDetails.Adresse IP v4

Nom de champ de console	Nom de champ JSON
Adresse IPv6 de l'appelant de l'API Kubernetes	service.action. kubernetesApiCallAction. remoteIpDetailsAdresse IP V6
Espace de noms Kubernetes	service.action. kubernetesApiCallAction.Namespace
ID ASN de l'appelant de l'API Kubernetes	service.action. kubernetesApiCallAction. remoteIpDetails.organisation.asn
URI de demande d'appel d'API Kubernetes	service.action. kubernetesApiCallAction.requestURI
Code d'état de l'API Kubernetes	service.action. kubernetesApiCallCode d'état de l'action
Adresse IPv4 locale de connexion réseau	service.action. networkConnectionAction. localIpDetails.Adresse IP v4
Adresse IPv6 locale de connexion réseau	service.action. networkConnectionAction. localIpDetailsAdresse IP V6
Protocole	service.action. networkConnectionAction.protocole
Nom du service de l'appel d'API	service.action. awsApiCallAction.ServiceName
ID du compte de l'appelant d'API	service.action. awsApiCallAction. remoteAccountDetails. Identifiant du compte
Nom de la liste des menaces	Service. Informations supplémentaires. threatListName
Rôle de ressource	service.resourceRole
Nom du cluster EKS	ressource. eksClusterDetails.nom
Nom de charge de travail Kubernetes	Resource.kubernetesDétails. kubernetesWorkloadDetails.nom

Nom de champ de console	Nom de champ JSON
Espace de noms de charge de travail Kubernetes	Resource.kubernetesDétails. kubernetesWorkloadDetails.espace de noms
Nom d'utilisateur Kubernetes	Resource.kubernetesDétails. kubernetesUserDetails.nom d'utilisateur
Image de conteneur Kubernetes	Resource.kubernetesDétails. kubernetesWorkloadDetails.conteneurs.image
Préfixe de l'image de conteneur Kubernetes	Resource.kubernetesDétails. kubernetesWorkloadDetails.containers.imagePrefix
ID de numérisation	service. ebsVolumeScanDétails. ScanID
Nom de la menace EBS Volume Scan	service. ebsVolumeScanDétails. Scannez les détections. threatDetectedByName.ThreatNames.name
Nom de la menace de scan d'objets S3	service. malwareScanDetails.threats .name
Gravité de la menace	service. ebsVolumeScanDétails. Scannez les détections. threatDetectedByNom.ThreatNames.Severity
Fichier SHA	service. ebsVolumeScanDétails. Scannez les détections. threatDetectedByName.ThreatNames.FilePaths.Hash
Nom du cluster ECS	ressource. ecsClusterDetails.nom
Image de conteneur ECS	ressource. ecsClusterDetails.TaskDetails.Containers.Image
ARN de définition de tâche ECS	ressource. ecsClusterDetails.TaskDetails.DefinitionArn
Image de conteneur autonome	resource.containerDetails.image

Nom de champ de console	Nom de champ JSON
ID d'instance de base de données	ressource. rdsDbInstanceDétails. dbInstanceIdentifier
ID de cluster de base de données	ressource. rdsDbInstanceDétails. dbClusterIdentifier
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.process.executableSha256
Nom du processus	service.runtimeDetails.process.name
Chemin exécutable	service.runtimeDetails.process.executablePath
Nom de fonction Lambda	resource.lambdaDetails.functionName
ARN de fonction Lambda	resource.lambdaDetails.functionArn
Clé de balise de fonction Lambda	resource.lambdaDetails.tags.key
Valeur de balise de fonction Lambda	resource.lambdaDetails.tags.value
Domaine de demande DNS	service.action. dnsRequestAction. domainWithSuffix

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 utilisez les GuardDuty résultats via Security Hub, un SIEM tiers ou d'autres applications d'alerte et de billetterie. Si vous l'avez activéGuardDuty Protection 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 via l' GuardDuty API en utilisant l'ListFindingsAPI avec un `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 la mise en réseau de VPC est configurée de manière à acheminer le trafic Internet pour qu'il sorte d'une passerelle sur site plutôt que d'une passerelle Internet de VPC.

  Ce résultat est généré lorsque la mise en réseau est configurée pour acheminer le trafic Internet de telle sorte qu'il sorte d'une passerelle sur site plutôt que d'une passerelle Internet VPC (IGW). Les configurations courantes, telles que AWS Outposts ou les connexions VPN VPC, peuvent entraîner l'acheminement 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 filtrage. Le premier critère est le type de résultat, qui devrait être `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Le deuxième critère de filtre est l'adresse IPv4 de l'appelant d'API avec l'adresse IP ou la plage d'adresses CIDR de votre passerelle Internet sur site. L'exemple ci-dessous représente le filtre que vous utiliseriez pour supprimer ce type de résultat en fonction de l'adresse IP de l'appelant d'API.

  ```
  Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
   API caller IPv4 address: 198.51.100.6
  ```

  > **Note**
  >
  > Pour inclure plusieurs adresses IP d'appelant d'API, vous pouvez ajouter un nouveau filtre d'adresse IPv4 d'appelant d'API pour chacune d'elles.

- 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 résultat en fonction des instances avec une certaine AMI.

```
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. De même, le deuxième critère de filtre peut utiliser le champ Exécutable SHA-256 dont la valeur est égale à celle du `executableSha256` du processus dans le résultat généré.
- Les clusters Kubernetes exécutent leurs propres serveurs DNS en tant que pods, comme `coredns`. Par conséquent, pour chaque recherche DNS à partir d'un module, deux événements DNS sont GuardDuty capturés, l'un provenant du module et l'autre du module serveur. Cela peut générer des doublons pour les résultats DNS suivants :
  - 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 en double incluront les détails du pod, du conteneur et du processus correspondant à votre pod de serveur DNS. Vous pouvez définir une règle de suppression pour supprimer ces résultats en double à l'aide de ces champs. Le premier critère de filtre doit utiliser le champ Type de résultat avec une valeur égale à un type de résultat DNS figurant dans la liste des résultats

fournie plus haut dans cette section. Le deuxième critère de filtre peut être soit Chemin exécutable, avec une valeur égale à l'`executablePath` de votre serveur DNS, soit Exécutable SHA-256, avec une valeur égale à celle de l'`executableSHA256` de votre serveur DNS dans le résultat généré. En tant que troisième critère de filtre facultatif, vous pouvez utiliser le champ Image de conteneur Kubernetes avec une valeur égale à l'image de conteneur de votre pod de serveur DNS 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 l'API :

1. Vous pouvez créer des règles de suppression via l'API CreateFilter. Pour ce faire, spécifiez les critères de filtre dans un fichier JSON en suivant le format de l'exemple détaillé ci-dessous. L'exemple ci-dessous supprimera tous les résultats non archivés de faible gravité

contenant une demande DNS 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 obtenir la liste des noms de champ JSON et leur équivalent dans la console, veuillez consulter Attributs du filtre.

Pour tester vos critères de filtre, utilisez le même critère JSON dans l'API ListFindings et vérifiez que les résultats corrects ont été sélectionnés. Pour tester vos critères de filtre, AWS CLI suivez l'exemple en utilisant vos propres fichiers DetectoriD et .json.

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

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Téléchargez votre filtre à utiliser en tant que règle de suppression avec l'API CreateFilter ou via l'interface de ligne de commande AWS en suivant l'exemple ci-dessous avec votre ID de détecteur, un nom pour la règle de suppression et votre fichier .json.

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

   ```
   aws guardduty create-filter --action ARCHIVE --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
    file://criteria.json
   ```

Vous pouvez consulter la liste de vos filtres par programmation à l'aide de l'API ListFilter. Vous pouvez consulter les détails d'un filtre individuel en fournissant le nom du filtre à l'API GetFilter. Mettez à jour les filtres à l'aide de UpdateFilter ou supprimez-les avec l'API DeleteFilter.

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 l'API DeleteFilter. 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 mises en forme en *rouge* :

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 flux VPC, les journaux d' AWS CloudTrail événements et les journaux DNS. Vous pouvez personnaliser cette étendue de surveillance en la configurant de manière GuardDuty à arrêter les alertes relatives aux adresses IP fiables provenant de vos propres listes d'adresses IP fiables et à émettre des alertes sur les adresses IP malveillantes connues provenant 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 flux VPC et à tous CloudTrail les résultats, mais ne s'appliquent pas aux résultats DNS.

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 flux VPC ni de CloudTrail résultats pour les adresses IP figurant sur des listes d'adresses IP fiables. Vous pouvez inclure 2 000 adresses IP et plages CIDR au maximum dans une seule liste d'adresses IP autorisées. 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 plages d'adresses CIDR dans une seule liste de menaces. GuardDuty génère uniquement des résultats basés sur une activité impliquant des adresses IP et des plages d'adresses CIDR 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 et 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 plus d'informations, consultez Gérer 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 autorisées et listes d'adresses IP de menaces, les adresses IP et les plages CIDR doivent apparaître une par ligne. Seules les adresses IPv4 sont acceptées.

- Texte brut (TXT)

  Ce format prend en charge à la fois les blocs CIDR et les adresses IP individuelles. La liste d'exemples suivante utilise le format texte en brut (TXT).

```
192.0.2.0/24
```

```
198.51.100.1
203.0.113.1
```

- Structured Threat Information Expression (STIX)

  Ce format prend en charge à la fois les blocs CIDR et les adresses IP individuelles. La liste d'exemples suivante utilise le format STIX.

```
<?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>
```

- Open Threat Exchange (OTX)™ CSV

  Ce format prend en charge à la fois les blocs CIDR et les adresses IP individuelles. La liste d'exemples suivante utilise le format CSV 0TX™.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEyeInformations sur les menaces ™ iSight CSV

  Ce format prend en charge à la fois les blocs CIDR et les adresses IP individuelles. La liste d'exemples suivante utilise un format CSV `FireEye`™.

```
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
```

- Proofpoint™ ET Intelligence Feed CSV

  Ce format ne prend en charge que les adresses IP individuelles. La liste d'exemples suivante utilise le format CSV `Proofpoint`. 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 identités IAM 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 GuardDuty SSE-KMS côté serveur, vous devez accorder au rôle lié au service l'AWSServiceRoleForAmazonGuardDutyautorisation de déchiffrer le

fichier afin d'activer la liste. Ajoutez l'instruction suivante à la stratégie de clé KMS et remplacez l'ID 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 l'URL d'emplacement de votre liste

1. Ouvrez la console Amazon S3 sur 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 l'URI S3 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 l'URL d'emplacement

      - 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 CreateIPSet. 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/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
    activate
    ```

Pour les listes de menaces

- Exécutez 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/DOC-EXAMPLE-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 (à l'aide de l'API/la CLI) 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 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.

     `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 une 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 plus d'informations, consultez 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 clé KMS

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 clé KMS. Vous pouvez accorder les autorisations en attachant la stratégie à votre clé KMS.

Lorsque vous utilisez une clé KMS provenant 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 de l'ARN de la clé du compte propriétaire de la clé.

Pour modifier la politique de clé KMS GuardDuty afin 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 clé KMS existante ou suivez les étapes de création d'une nouvelle clé dans le guide du AWS Key Management Service développeur, que vous utiliserez pour chiffrer les résultats exportés.

   > **Note**
   >
   > Votre clé KMS et le compartiment Amazon S3 doivent être identiques. Région AWS

   Vous pouvez utiliser le même compartiment S3 et la même paire de clés KMS 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 clé KMS, 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 qui sont mises en forme en *rouge* dans l'exemple de stratégie :

   1. Remplacez l'*ARN de la clé KMS* par le nom de ressource Amazon (ARN) de la clé KMS. Pour localiser l'ARN de la clé, consultez la section Trouver l'ID et l'ARN de la clé dans le guide du AWS Key Management Service développeur.
   2. Remplacez *123456789012* par l' Compte AWS identifiant du compte qui exporte les GuardDuty résultats.
   3. Remplacez *Region2* par l' Région AWS endroit où les GuardDuty résultats sont générés.
   4. Remplacez l'*SourceDetectorID* par `detectorID` celui du GuardDuty compte dans la région spécifique où les résultats ont été générés.

      `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 syntaxe JSON de votre politique de clé KMS est valide.

   Choisissez Enregistrer.

8. (Facultatif) copiez l'ARN de la clé 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 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 syntaxe JSON de votre politique de clé KMS 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 qui sont mises en forme en *rouge* dans l'exemple de stratégie :

   1. Remplacez l'*ARN du compartiment Amazon S3* par le nom de ressource Amazon (ARN) du compartiment Amazon S3. Vous trouverez l'ARN du bucket sur la page Modifier la politique du bucket dans la console https://console.aws.amazon.com/s3/.
   2. Remplacez *123456789012* par l' Compte AWS identifiant du compte qui exporte les GuardDuty résultats.
   3. Remplacez *Region2* par l' Région AWS endroit où les GuardDuty résultats sont générés.
   4. Remplacez l'*SourceDetectorID* par `detectorID` celui du GuardDuty compte dans la région spécifique où les résultats ont été générés.

      `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'ListDetectorsAPI
   5. Remplacez la partie *[préfixe facultatif]* de la valeur d'espace réservé *ARN/[préfixe facultatif] du compartiment S3* par 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 l'*ARN de la clé KMS* par le nom de ressource Amazon (ARN) de la clé KMS associée au chiffrement des résultats exportés vers le compartiment S3. Pour localiser l'ARN de la clé, consultez la section Trouver l'ID et l'ARN de la clé dans le guide 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 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 facultatif `/AWSLogs/123456789012/GuardDuty/Region`.

Le chemin complet de l'objet S3 sera`DOC-EXAMPLE-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 clé KMS doit se trouver dans la même région que le compartiment S3.

Avant de terminer ces étapes, assurez-vous d'avoir attaché les politiques correspondantes à votre clé KMS 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 l'ARN du compartiment S3, entrez le**`bucket ARN`**. Pour trouver l'ARN du compartiment, 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 console https://console.aws.amazon.com/guardduty/.

5. Pour l'ARN de la clé KMS, entrez le **`key ARN`**. Pour localiser l'ARN de la clé, consultez la section Trouver l'ID et l'ARN de la clé dans le guide du AWS Key Management Service développeur.
6. Joindre des politiques

   - Procédez comme suit pour associer la politique du compartiment S3. Pour plus d'informations, consultez Étape 3 — Attacher une politique au compartiment Amazon S3.

   - Effectuez les étapes pour joindre la politique de clé KMS. Pour plus d'informations, consultez Étape 2 — Attacher une politique à votre clé KMS.
7. Choisissez 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
   - Update CWE and S3 every 6 hours (default) (Mettre 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 Gérer 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 plus

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.	d'informations sur les types de chiffreme nt pris GuardDuty en charge, consultez Volumes Amazon EBS pris en charge pour l'analyse des programmes malveilla nts.	

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 instance EC2 ou une charge de travail 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 instance EC2 potentiellement compromise dans votre AWS environnement :

1. Identifiez l'instance Amazon EC2 potentiellement compromise

   Recherchez dans l'instance potentiellement compromise des programmes malveillants et supprimez ceux qui sont détectés. Vous pouvez utiliser Analyse des logiciels malveillants à la demande pour identifier les logiciels malveillants dans l'instance EC2 potentiellement compromise,

ou consulter AWS Marketplace pour vérifier s'il existe des produits partenaires utiles afin d'identifier et de supprimer les logiciels malveillants.

2. Isolez l'instance Amazon EC2 potentiellement compromise

   Si possible, procédez comme suit pour isoler l'instance potentiellement compromise :

   1. Créez un groupe de sécurité dédié à l'isolation.
   2. Créez une règle unique `0.0.0.0/0 (0-65535)` pour l'ensemble du trafic dans les règles sortantes.

      Lorsque cette règle s'applique, elle convertit tout le trafic sortant existant (et nouveau) en trafic non suivi, bloquant ainsi toutes les sessions sortantes établies. Pour plus d'informations, consultez la section Connexions non suivies.
   3. Supprimez toutes les associations de groupes de sécurité actuelles de l'instance potentiellement compromise.
   4. Associez le groupe de sécurité Isolation à cette instance.

      Après l'association, supprimez la règle `0.0.0.0/0 (0-65535)` pour tout le trafic des règles sortantes du groupe de sécurité Isolation.

3. Identifiez la source de l'activité suspecte.

   Si un logiciel malveillant est détecté, identifiez et arrêtez l'activité potentiellement non autorisée sur votre instance EC2 en fonction du type de résultat 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 instance EC2 potentiellement compromise, nous vous recommandons de mettre fin à l'instance EC2 compromise et de la remplacer par une nouvelle instance si nécessaire. Les ressources supplémentaires suivantes vous permettent de sécuriser vos instances EC2 :

   - Section Sécurité et réseau de Bonnes pratiques pour Amazon EC2.
   - Groupes de sécurité Amazon EC2 pour les instances Linux et Groupes de sécurité Amazon EC2 pour les instances Windows.
   - Sécurité dans Amazon EC2
   - Conseils pour sécuriser vos instances EC2 (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'appel d'API utilisé.

   L'appel d'API utilisé est répertorié en tant qu'`API` dans les détails d'un résultat. La source sera un principal IAM (rôle IAM, 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 instance Amazon EC2, 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 utilisateur IAM était impliqué, est-il possible que ses informations d'identification aient été potentiellement compromises ? Pour plus d’informations, consultez Corriger les informations d'identification potentiellement compromises AWS.
   - Si une API a été invoquée par un principal qui n'a jamais invoqué ce type d'API, 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 appel `PreflightRequest` réussi constaté à partir du nom d'utilisateur `ANONYMOUS_PRINCIPAL` avec le type d'utilisateur `AWSAccount`, cela indique que le compartiment dispose d'une stratégie de partage des ressources entre origines multiples (CORS) définie. Ce compartiment doit-il être doté d'une stratégie CORS ? 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 CORS, veuillez consulter la section Utilisation du partage des ressources entre origines multiples (CORS) du Guide de l'utilisateur 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 données d'identification personnelle (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 console https://console.aws.amazon.com/guardduty/ vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour plus d’informations, consultez 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 afin de renforcer les autorisations et de 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 les utilisateurs IAM peuvent accéder à vos ressources ou à vos buckets. Pour plus d'informations, veuillez consulter Utilisation de stratégies de compartiment et de stratégies utilisateur.

  Vous pouvez également utiliser des points de terminaison de cloud privé virtuel (VPC) avec des stratégies de compartiment S3 pour restreindre l'accès à des points de terminaison d'un VPC spécifiques. Pour plus d'informations, veuillez consulter Exemple de stratégies de compartiment pour les points de terminaison d'un VPC pour Amazon S3 (langue française non garantie).
- Pour autoriser temporairement l'accès à vos objets S3 à des entités approuvées extérieures à votre compte, vous pouvez créer une URL présignée 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, veuillez consulter Génération d'URL présignées avec S3 (langue française non garantie).
- 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 l'accès sécurisé à vos ressources S3 à d'autres AWS comptes, vous pouvez utiliser une liste de contrôle d'accès (ACL). Pour plus d'informations, voir Gestion de l'accès S3 avec des ACL.

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 plus d’informations, consultez 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 ECS potentiellement compromis

Suivez ces étapes recommandées pour corriger un cluster Amazon ECS potentiellement compromis dans votre AWS environnement :

1. Identifiez le cluster ECS potentiellement compromis.

   La recherche GuardDuty Malware Protection for EC2 pour ECS fournit les détails du cluster ECS dans le panneau des détails de la découverte.
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 console https://console.aws.amazon.com/guardduty/ vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour plus d’informations, consultez 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'entité IAM potentiellement compromise et l'appel d'API utilisé.

   L'appel d'API utilisé est répertorié en tant qu'`API` dans les détails d'un résultat. L'entité IAM (rôle ou utilisateur IAM) et ses informations d'identification seront répertoriées dans la section Ressources des détails de la recherche. Le type de l'entité IAM impliquée peut être déterminé par le champ User Type (Type d'utilisateur), le nom de l'entité IAM se trouvant dans le champ User name (Nom d'utilisateur). Le type de l'entité IAM impliquée dans le résultat peut également être déterminé par l'Access key ID (ID de clé d'accès) utilisé.

   Pour les clés commençant par `AKIA` :

   Ce type de clé est une information d'identification à long terme gérée par le client associée à un utilisateur IAM ou à un Utilisateur racine d'un compte AWS. Pour de plus amples informations sur la gestion des clés d'accès pour les utilisateurs IAM, veuillez consulter Gestion des clés d'accès pour les utilisateurs IAM.

   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. Les rôles IAM utiliseront toujours des AWS STS informations d'identification, mais elles peuvent également être générées pour les

utilisateurs IAM. Pour plus d'informations sur AWS STS 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 IAM et les AWS STS informations dans CloudTrail.

2. Vérifiez les autorisations pour l'entité IAM.

   Ouvrez la console IAM. 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 l'entité IAM 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'opération d'API répertoriée dans le GuardDuty résultat
   - A invoqué l'opération d'API à l'heure indiquée dans le GuardDuty résultat
   - A appelé l'opération d'API 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 console https://console.aws.amazon.com/guardduty/ vous permet de configurer des règles pour supprimer complètement les résultats individuels afin qu'ils n'apparaissent plus. Pour plus d’informations, consultez 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, à savoir les informations d'identification de connexion de l'utilisateur IAM, ou éventuellement 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 volumes EBS 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 console https://console.aws.amazon.com/guardduty/ 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 plus d'informations, voir 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 Surveillance des journaux d'audit EKS. 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 activéGuardDuty Protection RDS. 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

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.

Gérer plusieurs comptes sur Amazon GuardDuty

Lorsque votre AWS environnement comporte plusieurs comptes, vous pouvez les gérer en désignant un AWS compte comme compte administrateur. Vous pouvez ensuite associer d'autres AWS comptes à ce compte administrateur en tant que comptes de membre. Ce compte GuardDuty administrateur désigné peut configurer les plans de protection. GuardDuty Il existe deux manières d'associer des comptes à un compte administrateur : créer une organisation en utilisant AWS Organizations et le compte administrateur et un ou plusieurs comptes membres appartiennent à cette organisation, ou envoyer une invitation à un AWS compte via GuardDuty.

GuardDuty recommande d'utiliser la AWS Organizations méthode. Pour de plus amples informations sur la configuration d'une organisation, veuillez consulter Création d'une organisation dans le Guide de l'utilisateur AWS Organizations .

Gérer plusieurs comptes avec AWS Organizations

Si le compte que vous souhaitez définir comme compte GuardDuty administrateur fait partie d'une organisation dans AWS Organizations, vous pouvez spécifier ce compte en tant qu'administrateur délégué de l'organisation GuardDuty. Le compte enregistré en tant qu'administrateur délégué devient automatiquement le compte GuardDuty administrateur.

Vous pouvez utiliser ce compte administrateur GuardDuty pour activer et gérer n'importe quel membre Compte AWS de l'organisation lorsque vous ajoutez ce compte en tant que compte membre.

Si vous possédez déjà un compte GuardDuty administrateur associé à des comptes de membres sur invitation, vous pouvez enregistrer ce compte en tant qu'administrateur GuardDuty délégué de l'organisation. Lorsque vous le faites, tous les comptes de membres actuellement associés restent membres, ce qui vous permet de profiter pleinement des fonctionnalités supplémentaires de gestion de vos GuardDuty comptes avec AWS Organizations.

Pour plus d'informations sur la prise en charge de plusieurs comptes GuardDuty par le biais d'une organisation, consultezGérer des GuardDuty comptes avec AWS Organizations.

Gestion de plusieurs comptes par invitation

Si les comptes que vous souhaitez associer ne font pas partie de votre organisation, vous pouvez spécifier un compte administrateur, GuardDuty puis l'utiliser pour inviter d'autres personnes

Comptes AWS à devenir des comptes membres. Lorsque le compte invité accepte l'invitation, ce compte devient un compte GuardDuty membre associé au compte administrateur.

Pour plus d'informations sur la prise en charge de plusieurs comptes sur invitation, GuardDuty voirGestion GuardDuty des comptes sur invitation.

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. Les principales fonctions que le compte administrateur peut effectuer sont les suivantes :

- Ajouter et supprimer des comptes membres associés. La procédure à suivre diffère selon que les comptes sont associés via des organisations ou une invitation.
- 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 administrateur et les comptes membres.

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'adresse s IP fiables ou les listes de menaces	Tous	–	Tous	–
Supprimer la liste d'adresse s IP fiables ou les listes de menaces	Tous	–	Tous	–
Définissez la fréquence des EventBridge notifications	Tous	–	Tous	Auto-utilisateur
Définir l'emplace ment 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 pour S3.	N’importe quel compte	–	N’importe quel compte	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	–	N° de 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 que cette action doit être effectuée pour tous les comptes associés avant d'être prise pour ce compte. Après avoir dissocié ces comptes, vous devez les supprimer. Pour plus d'informations sur l'exécution de ces tâches dans votre organisation, consultezMaintien de votre organisation au sein de GuardDuty.

Gérer des GuardDuty comptes avec AWS Organizations

Lorsque vous l'utilisez GuardDuty avec une AWS organisation, le compte de gestion de cette organisation peut désigner n'importe quel compte au sein de l'organisation comme compte d' GuardDuty administrateur délégué. Pour ce compte administrateur, GuardDuty il est activé automatiquement uniquement dans le compte désigné Région AWS. Ce compte est également autorisé à activer et à gérer tous GuardDuty les comptes de l'organisation au sein de cette région. Le compte administrateur peut voir les membres de cette AWS organisation et y ajouter des membres.

Si vous avez déjà configuré un compte GuardDuty administrateur avec des comptes membres associés sur invitation et que les comptes membres font partie de la même organisation, leur type passe de Par invitation à Via Organizations lorsque vous définissez un compte d' GuardDuty administrateur délégué pour votre organisation. Si un compte d' GuardDuty administrateur délégué a précédemment ajouté des membres sur invitation qui ne font pas partie de la même organisation, leur

type reste sur invitation. Dans les deux cas, les comptes précédemment ajoutés sont des comptes de membres associés au compte d' GuardDuty administrateur délégué de l'organisation.

Vous pouvez continuer à ajouter des comptes en tant que membres même s'ils ne font pas partie de votre organisation. Pour plus d'informations, consultez Ajout et gestion des comptes par invitation ou Désignation d'un compte d' GuardDuty administrateur délégué et gestion des membres à l'aide de la console GuardDuty .

Table des matières

Considérations et recommandations lors de la désignation d'un compte d'administrateur délégué GuardDuty

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 AWS Organizationsà GuardDuty un service régional. Les comptes GuardDuty d'administrateur délégué et leurs comptes de membre doivent être ajoutés AWS Organizations dans chaque région que vous avez GuardDuty activée. 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 l'ListMembersAPI.
- Lorsque vous travaillez avec la configuration GuardDuty d'activation automatique définie sur`NEW`, 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 sur`ALL`, 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 de l'API.

Il est recommandé à une AWS organisation d'avoir le même compte GuardDuty d'administrateur délégué pour tous les Régions AWS.

Nous vous recommandons de désigner le même compte d' GuardDuty administrateur délégué pour votre organisation sur tous les Régions AWS sites que vous avez activés GuardDuty. Si vous

désignez un compte en tant que compte d' GuardDuty administrateur délégué dans une région, il est recommandé d'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

Lorsque vous déléguez un compte d' GuardDuty administrateur délégué, vous devez disposer des autorisations nécessaires pour l'activer GuardDuty ainsi que pour certaines actions AWS Organizations d'API. Vous pouvez ajouter l'instruction suivante à la fin d'une politique IAM existante pour accorder ces autorisations :

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

En outre, si vous souhaitez désigner votre compte AWS Organizations de gestion comme compte d' GuardDuty administrateur GuardDuty délégué, cette entité aura besoin d'`CreateServiceLinkedRole`autorisations pour s'initialiser GuardDuty. Pour ce faire, ajoutez la déclaration suivante à la politique IAM et remplacez *111122223333* par l' Compte AWS ID 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' GuardDuty administrateur délégué et gestion des membres à l'aide de la console GuardDuty

Table des matières

Étape 1 — Désignez un compte GuardDuty d'administrateur délégué pour votre organisation

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 organisation AWS Organizations .

2. Si vous avez déjà activé GuardDuty le compte de gestion, ignorez cette étape et passez à l'étape suivante.

   Si vous ne l'avez pas GuardDuty encore activé, sélectionnez Commencer, puis désignez un compte d' GuardDuty administrateur délégué sur la GuardDuty page Bienvenue.

   > **Note**
   >
   > Le compte de gestion doit avoir le rôle GuardDuty lié au service (SLR) afin que le compte d' GuardDuty administrateur délégué puisse activer et gérer GuardDuty ce compte. Une fois que vous avez activé le compte de gestion GuardDuty dans une région, ce reflex est créé automatiquement.

3. Effectuez cette étape après avoir activé GuardDuty le compte de gestion. Dans le volet de navigation de la GuardDuty console, sélectionnez Paramètres. Sur la page Paramètres, entrez l' Compte AWS identifiant 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.

4. Choisisssez Delegate (Déléguer).

5. (Recommandé) Répétez l'étape précédente pour désigner le compte d' GuardDuty administrateur délégué dans chaque Région AWS cas où vous l'avez GuardDuty activé.

Étape 2 — Configuration des préférences d'activation automatique pour votre organisation

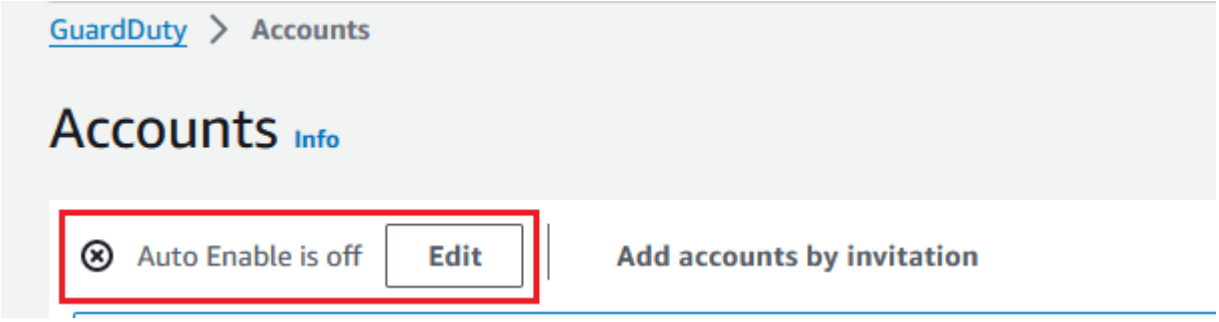
1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.

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 l'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 plus d'informations, consultez Régions et points de terminaison.

Étape 3 : ajouter des comptes en tant que membres à votre organisation

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 membre n'est pas associé au compte GuardDuty administrateur de l'organisation, le statut de ce compte membre est Non membre.

3. Sélectionnez un ou plusieurs ID de compte que vous voulez ajouter en tant que membres. Ces ID de compte doivent avec le Type Via les organisations.

   Les comptes ajoutés par invitation ne font pas partie de votre organisation. Vous pouvez gérer ces comptes individuellement. Pour plus d'informations, consultez 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. En fonction des paramètres définis dansthe section called "Étape 1 — Désignez un compte GuardDuty d'administrateur délégué pour votre 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 dans chacune d'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 dans lesquelles 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.

Étape 4 (facultative) — Configuration des plans de protection pour les comptes individuels

Vous pouvez configurer des 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.

Désignation d'un compte d' GuardDuty administrateur GuardDuty délégué et gestion des membres à l'aide de l'API

Table des matières

Étape 1 — Désignez un compte GuardDuty d'administrateur délégué pour votre AWS organisation

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* par l' Compte AWS ID du compte que vous souhaitez désigner comme compte d'administrateur délégué : GuardDuty

```
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* par la région à laquelle vous souhaitez attribuer le compte d'administrateur délégué. GuardDuty GuardDuty

```
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 l'étape précédente pour désigner le compte d' GuardDuty administrateur délégué dans chaque Région AWS cas où vous l'avez GuardDuty activé.

Étape 2 : configuration des préférences d'activation automatique pour l'organisation

1. 1. Exécutez-le à UpdateOrganizationConfigurationl'aide des 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

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

> **Note**
>
> Pour plus d'informations sur les différentes configurations d'activation automatique, consultez la section autoEnableOrganizationMembres.

2. 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.
3. 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.

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

2. (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 l'ListMembersAPI.

Étape 3 : ajouter des comptes en tant que membres à votre organisation

- 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 identifiants et adresses e-mail correspondantes) des comptes que vous souhaitez ajouter en tant que GuardDuty membres. Vous pouvez créer un ou plusieurs membres avec cette opération d'API.

  Lorsque vous gérez CreateMembers 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 membres existants.

Exécutez-le ListAccountsdans la référence d'AWS Organizations API 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.

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

Maintien de votre organisation au sein de 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 à l'aide de l'API — Exécutez 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 membre existant, la configuration de l'organisation s'applique également aux membres existants. Cela peut modifier la configuration actuelle des comptes membres existants.

  Pour afficher tous les comptes de votre organisation, exécutez ListAccountsla référence AWS Organizations d'API.

Pour maintenir l'état de configuration des comptes membres individuellement dans chaque région

- Pour afficher tous les comptes de votre organisation, exécutez ListAccountsla référence AWS Organizations d'API.
- 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 la console ou de l'API, 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-le DeregisterDelegatedAdministratordans la référence AWS Organizations d'API, 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* par le compte d'administrateur délégué existant. GuardDuty

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 l'une des méthodes d'accès suivantes :
   - Utilisation de GuardDuty la console —Étape 1 — Désignez un compte GuardDuty d'administrateur délégué pour votre organisation.
   - Utilisation de GuardDuty l'API —Étape 1 — Désignez un compte GuardDuty d'administrateur délégué pour votre AWS organisation.
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.

Pour modifier cette configuration d'organisation pour le nouveau compte d' GuardDuty administrateur délégué, utilisez l'une des méthodes d'accès suivantes :

- Utilisation de GuardDuty la console —Étape 2 — Configuration des préférences d'activation automatique pour votre organisation.
- Utilisation de GuardDuty l'API —Étape 2 : configuration des préférences d'activation automatique pour 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 opérations de l'API. Exécutez les opérations GuardDuty d'API 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'opération d'CreateMembersAPI 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 avec cette opération d'API.

   Vous pouvez également utiliser les outils de ligne de AWS commande pour désigner un compte administrateur en exécutant la commande CLI suivante. Assurez-vous d'utiliser vos propres ID de détecteur, ID de compte et adresse e-mail valides.

   `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 actuel et les identifiants des comptes dont vous souhaitez devenir GuardDuty membres. Vous pouvez inviter un ou plusieurs membres avec cette opération d'API.

   > **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 vos propres ID de détecteur et ID de compte valides pour les comptes que vous souhaitez inviter.

   `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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'opération CreateDetectorAPI 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 commande CLI suivante.

```
aws guardduty create-detector --enable
```

2. Exécutez l'opération AcceptAdministratorInvitationAPI 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 trouverez l'ID de compte du compte administrateur dans l'e-mail d'invitation ou en utilisant l'opération ListInvitations de l'API.

   Vous pouvez également accepter une invitation à l'aide des outils de ligne de AWS commande en exécutant la commande CLI suivante. Assurez-vous d'utiliser un ID de détecteur, un ID de compte administrateur et un ID d'invitation valides.

   `detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 membre toujours associé aux comptes d'administrateur préexistants.

   b. Vous pouvez également AWS Command Line Interface exécuter la commande suivante et remplacer *7777777777* par l'ID de détecteur du compte administrateur préexistant dont vous souhaitez dissocier le compte membre. Remplacez *666666666666* par l'ID Compte AWS 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 membres à l'aide d'Amazon EC2. 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 ont une dépendance sur un rôle IAM partagé avec la stratégie 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 rôle IAM dans le compte GuardDuty administrateur et associez la AWS politique gérée : AmazonGuardDutyFullAccess politique à activer GuardDuty.
2. Créez un rôle IAM dans chaque compte membre que vous souhaitez voir gérer par votre compte GuardDuty 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 fichier CSV contenant la liste des ID de compte et des adresses e-mail des comptes 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 fichier CSV doit se trouver au même emplacement que votre script `enableguardduty.py`. Vous pouvez utiliser la méthode suivante pour copier un fichier CSV existant d'Amazon S3 vers votre répertoire actuel.
>
> ```
> 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 fichier CSV comme arguments.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Estimation des GuardDuty coûts

Vous pouvez utiliser les opérations de GuardDuty console ou d'API pour estimer les coûts d'utilisation moyens quotidiens pour GuardDuty. Pendant la période d'essai gratuite de 30 jours, l'estimation des coûts prévoit estime vos coûts après la période d'essai. Si vous opérez dans un environnement multi-comptes, votre compte GuardDuty administrateur peut surveiller les statistiques de coûts pour tous les comptes membres.

> **Note**
>
> Le coût d'utilisation de Malware Protection for S3 n'est pas inclus dans la section Utilisation de la GuardDuty console. Pour plus d'informations, consultez 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.
- Source de données — Répertorie le coût estimé de la source de données spécifiée pour les types de sources de GuardDuty données suivants : journaux de flux VPC, journaux CloudTrail de gestion, événements de CloudTrail données ou journaux DNS.
- Fonctionnalités — Répertorie le coût estimé sur la source de données spécifiée pour les GuardDuty fonctionnalités suivantes : événements de CloudTrail données pour S3, surveillance du journal d'audit EKS, données de volume EBS, activité de connexion RDS, surveillance du temps d'exécution EKS, surveillance du temps d'exécution Fargate, surveillance du temps d'exécution EC2 ou surveillance 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.

> **Note**
>
> Les statistiques du compartiment S3 ne sont disponibles que si la fonction Protection S3 est activée pour le compte. Pour plus d'informations, consultez Protection Amazon S3 sur Amazon GuardDuty.

Comprendre le mode de GuardDuty calcul des 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'exécution EKS doivent être désactivées.

GuardDuty a consolidé l'expérience de console pour EKS Runtime Monitoring dans Runtime Monitoring. GuardDuty recommande Vérification de l'état de configuration de la surveillance du temps d'exécution etMigration d'EKS Runtime Monitoring vers Runtime Monitoring.

Dans le cadre de la migration vers Runtime Monitoring, assurez-vous deDésactiver la surveillance de l'exécution EKS. Ceci est important car si vous choisissez ultérieurement de désactiver la

surveillance du temps d'exécution et que vous ne désactivez pas la surveillance du temps d'exécution EKS, vous continuerez de devoir payer des frais d'utilisation pour le suivi du temps d'exécution d'EKS.

Surveillance du temps d'exécution : impact des journaux de flux VPC provenant d'instances EC2 sur les coûts d'utilisation

Lorsque vous gérez l'agent de sécurité (manuellement ou via GuardDuty) dans EKS Runtime Monitoring ou Runtime Monitoring pour les instances EC2, et qu'GuardDuty il est actuellement déployé sur une instance Amazon EC2 et que vous Types d'événement d'exécution collectés le recevez de cette instance GuardDuty , l'analyse des journaux de flux VPC provenant de cette instance Amazon EC2 ne Compte AWS vous 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 sont affectés par votre utilisation des AWS API qui se connectent à CloudTrail. Pour plus d’informations, consultez AWS CloudTrail journaux d'événements.

Révision GuardDuty des statistiques 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 de membre, 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'opération GetUsageStatisticsAPI en utilisant les informations d'identification du compte GuardDuty administrateur. Fournissez les informations suivantes pour exécuter la commande :

- (Obligatoire) Fournissez 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) Une liste des ID de compte 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.

`detectorId`Pour trouver les paramètres correspondant à votre compte et à votre région actuelle, consultez la page Paramètres de la console https://console.aws.amazon.com/guardduty/ ou exécutez l'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 Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la 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 Services AWS.
- 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 modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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 Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI 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 une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à 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 et KMS. 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 (Amazon EKS) AWS Fargate (Fargate) , Amazon Elastic Container Service (Amazon ECS) uniquement et les instances Amazon Elastic Compute Cloud (Amazon EC2) 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 événements DNS, etc. Pour plus d'informations, consultez 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 de plus amples informations, veuillez consulter FAQ sur la confidentialité des données.

GuardDuty Protection contre les logiciels malveillants

GuardDuty Malware Protection analyse et détecte les programmes malveillants contenus dans les volumes EBS attachés à votre instance Amazon EC2 et à vos charges de travail de conteneur

potentiellement compromises, ainsi que dans les fichiers récemment chargés dans les compartiments Amazon S3 que vous avez sélectionnés. Lorsque GuardDuty Malware Protection identifie un fichier de volume EBS ou un fichier S3 comme étant malveillant ou dangereux, GuardDuty Malware Protection collecte et stocke ce fichier afin de développer et d'améliorer ses détections de malwares et 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 de plus amples informations, veuillez consulter FAQ sur la confidentialité des données.

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

Surveillance du temps d'exécution dans GuardDutyutilise 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 Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser GuardDuty les ressources. IAM est un Service AWS 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 soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d’IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec GuardDuty, voirComment Amazon GuardDuty travaille avec IAM.

Administrateur IAM — Si vous êtes administrateur IAM, 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 dans IAM, 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 qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

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 (IAM Identity 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 avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. 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 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 demandes AWS d'API dans le guide de l'utilisateur IAM.

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 l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

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 Services AWS 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 vous imposent de vous connecter en tant qu’utilisateur root, consultez Tâches nécessitant des informations d’identification d’utilisateur root dans le Guide de l’utilisateur IAM.

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 Services AWS 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 Services AWS 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 obtenir des informations sur IAM Identity Center, consultez Qu’est-ce que IAM Identity Center ? dans le Guide de l’utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d’identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d’identification à long terme tels que les clés d’accès. Toutefois, si certains cas d’utilisation spécifiques nécessitent des informations d’identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d’accès. Pour plus d’informations, consultez Rotation régulière des clés d’accès pour les cas d’utilisation nécessitant des informations d’identification dans le Guide de l’utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d’utilisateurs IAM. 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

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, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- 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 obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. 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 d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS 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, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. 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 direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM 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. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS 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 la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS 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 administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

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 documents JSON. Pour plus d’informations sur la structure et le contenu des documents de politique JSON, consultez Vue d’ensemble des politiques JSON dans le Guide de l’utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON 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 octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L’administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d’une action, quelle que soit la méthode que vous utilisez pour exécuter 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 à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l’identité

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

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 découvrir comment choisir entre

une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes 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.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). 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 Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON 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 les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- 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 politiques de séance dans le Guide de l'utilisateur IAM.

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 l'utilisateur IAM.

Comment Amazon GuardDuty travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à GuardDuty, découvrez les fonctionnalités IAM disponibles. GuardDuty

Fonctionnalités IAM que vous pouvez utiliser avec Amazon GuardDuty

Fonction IAM	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
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont GuardDuty les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour GuardDuty

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles

ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et 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 découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

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 de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que 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 administrateur IAM du compte sécurisé 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, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour GuardDuty

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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 `Action` d’une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l’accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n’ont pas d’opération API correspondante. 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 les politiques AWS JSON 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 de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de 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 ARN, consultez la section Ressources définies par Amazon GuardDuty dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, 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

Clés de conditions de politique pour GuardDuty

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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 accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

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 de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

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 (ACL) dans GuardDuty

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec GuardDuty

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas 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'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec GuardDuty

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

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 Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. 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 Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour GuardDuty

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM 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. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS 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 une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour GuardDuty

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **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 à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS 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 administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant 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 d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent 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 à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l’identité IAM à l’aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l’onglet JSON dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par GuardDuty, y compris le format des ARN 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

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 politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l’utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l’exécution d’une seule 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 de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. 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 Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console GuardDuty

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 l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API 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 Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisations requises pour activer GuardDuty

Pour accorder les autorisations nécessaires aux différentes identités IAM (utilisateurs, groupes et rôles), attachez la AWS politique gérée : AmazonGuardDutyFullAccess politique requise à activer GuardDuty.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "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": "*"
        }
    ]
}
```

Politique IAM 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 rôle, à un utilisateur ou à un groupe IAM 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 rôle, à un utilisateur ou à un groupe IAM 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 politique IAM personnalisée pour limiter l'accès aux ressources GuardDuty

Pour définir l'accès d'un utilisateur en GuardDuty fonction de l'ID du détecteur, vous pouvez utiliser toutes les actions d'GuardDutyAPI dans vos politiques IAM 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 politique IAM pour définir l'accès d'un utilisateur en GuardDuty fonction de l'ID et de l'ID IPSet ThreatIntelSet :

- `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'opération `guardduty:UpdateIPSet`, à l'aide de l'ID de détecteur 1234567 et de l'ID IPSet 000000 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 plus d'informations, consultez 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'opération `guardduty:UpdateIPSet`, à l'aide de n'importe quel ID de détecteur et de l'ID IPSet 000000 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 plus d'informations, consultez 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'opération `guardduty:UpdateIPSet`, à l'aide de son ID de détecteur et de n'importe quel ID IPSet 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 plus d'informations, consultez 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 des rôles AWS Identity and Access Management liés à un service (IAM). Un rôle lié à un service (SLR) est un type unique de rôle IAM 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 comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

GuardDuty prend en charge l'utilisation de rôles liés aux services dans toutes les régions où cela GuardDuty est disponible. Pour plus d'informations, consultez 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, veuillez consulter Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM et recherchez les services ayant Oui dans la colonne Rôle lié à un 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` Le reflex permet d' GuardDuty effectuer les tâches suivantes. Cela permet également GuardDuty d'inclure les métadonnées récupérées appartenant à l'instance EC2 dans les conclusions qui GuardDuty peuvent être générées 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 les actions Amazon EC2 pour gérer et récupérer des informations sur vos instances EC2, vos images et vos composants réseau tels que les VPC, les sous-réseaux et les passerelles de transit.
- Utilisez AWS Systems Manager des actions pour gérer les associations SSM sur les instances Amazon EC2 lorsque vous GuardDuty activez la surveillance du temps d'exécution avec un agent automatisé pour Amazon EC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les instances EC2 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 les actions Amazon EKS pour gérer et récupérer des informations sur les clusters EKS et gérer les modules complémentaires Amazon EKS sur des clusters EKS. Les actions EKS récupèrent également les informations relatives aux balises associées à GuardDuty.
- Utilisez IAM pour créer la protection contre les programmes malveillants Autorisations de rôle liées à un service pour Malware Protection for EC2 après l'activation de la protection contre les logiciels malveillants pour EC2.
- Utilisez les actions Amazon ECS pour gérer et récupérer des informations sur les clusters Amazon ECS, et gérez les paramètres du compte Amazon ECS avec`guarddutyActivate`. Les actions relatives à Amazon ECS récupèrent également les informations relatives aux balises associées 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",
                "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 fil RSS 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 au service manuellement à l'aide de la console IAM, de l'API IAM ou de l' AWS CLI API IAM.

> **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 de manière à permettre à un principal IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForAmazonGuardDuty` lié au service soit correctement créé, le principal IAM que vous utilisez doit disposer GuardDuty des autorisations requises. Pour accorder les autorisations requises, attachez la stratégie suivante à cet utilisateur, groupe ou rôle :

> **Note**
>
> Remplacez l'exemple d'*`identifiant de compte`* dans l'exemple suivant par 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 de plus amples informations sur la création manuelle d'un rôle, veuillez consulter Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

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. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

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 pour EC2, la suppression `AWSServiceRoleForAmazonGuardDuty` n'est pas automatiquement supprimée. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Si vous

souhaitez effectuer une suppression`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consultez 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 plus d'informations, consultez 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 d'IAM

Utilisez la console IAM AWS CLI, ou l'API IAM pour supprimer le rôle lié au `AWSServiceRoleForAmazonGuardDuty` service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

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 for EC2

Malware Protection for EC2 utilise le rôle lié au service (SLR) nommé. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Ce SLR permet à Malware Protection for EC2 d'effectuer des analyses sans agent afin de détecter les logiciels malveillants présents dans votre compte. GuardDuty Il permet GuardDuty de créer un instantané du volume EBS dans votre compte et de partager cet instantané avec le compte de GuardDuty service. Après avoir GuardDuty évalué le snapshot, celui-ci inclut les métadonnées de charge de travail de conteneur et d'instance EC2 récupérées dans les résultats de la protection contre les malwares pour EC2. Le rôle lié à un service `AWSServiceRoleForAmazonGuardDutyMalwareProtection` fait confiance au service `malware-protection.guardduty.amazonaws.com` pour endosser le rôle.

Les politiques d'autorisation associées à ce rôle permettent à Malware Protection for EC2 d'effectuer les tâches suivantes :

- Utilisez les actions Amazon Elastic Compute Cloud (Amazon EC2) pour récupérer des informations sur vos instances, volumes et instantanés Amazon EC2. Malware Protection for EC2 fournit également l'autorisation d'accéder aux métadonnées des clusters Amazon EKS et Amazon ECS.
- Créer des instantanés pour les volumes EBS dont la balise `GuardDutyExcluded` 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 EC2 n'aura 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 Malware Protection for 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`, pour appeler `CreateGrant` pour créer et accéder à un volume EBS 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 journaux Malware Protection for EC2 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 gérée EBS. GuardDuty exécute l'`DescribeKey`action pour déterminer `key Id` la clé gérée par EBS dans votre compte.
- Récupérez l'instantané des volumes EBS chiffrés à l'aide de Clé gérée par AWS, depuis votre Compte AWS et copiez-le dans le. GuardDuty 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 prise en charge de Malware Protection for EC2 pour l'analyse des volumes EBS chiffrés avec Clé gérée par AWS peut ne pas être disponible dans tous les. Régions AWS Pour plus d'informations, consultez Disponibilité des fonctionnalités propres à la région.
- Autorisez Amazon EC2 à appeler au AWS KMS nom de Malware Protection for EC2 afin d'effectuer plusieurs actions cryptographiques sur des 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 à un service est automatiquement créé lorsque vous activez la protection contre les programmes malveillants pour EC2 pour la première fois ou lorsque vous activez la protection contre les programmes malveillants pour EC2 dans une région prise en charge où elle n'était pas activée auparavant. Vous pouvez également créer le rôle lié à un service `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manuellement, via la console IAM, la CLI IAM ou l'API IAM.

> **Note**
>
> Par défaut, si vous utilisez Amazon pour la première fois GuardDuty, Malware Protection for 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 de manière à permettre à un principal IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour que le rôle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` lié au service soit correctement créé, l'identité IAM que vous utilisez doit disposer GuardDuty 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 de plus amples informations sur la création manuelle d'un rôle, veuillez consulter Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

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 lié au `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 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. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

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 pour EC2 dans toutes les régions où elle est activée.
> Si la protection contre les programmes malveillants pour EC2 n'est pas désactivée lorsque vous essayez de supprimer le rôle lié à un service, la suppression échouera. Pour plus d'informations, consultez Pour activer ou désactiver l'analyse des programmes malveillants GuardDuty initiée.

Lorsque vous choisissez Désactiver pour arrêter le service Malware Protection for EC2, celui-ci n'`AWSServiceRoleForAmazonGuardDutyMalwareProtection`est pas automatiquement supprimé. Si vous choisissez ensuite Activer pour redémarrer le service Malware Protection for EC2, GuardDuty vous commencerez à utiliser le service existant`AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, la AWS CLI ou l'API IAM pour supprimer le rôle lié au `AWSServiceRoleForAmazonGuardDutyMalwareProtection` service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

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 pour EC2 n'est actuellement pas disponible en 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 le client IAM qui ne fournissent à votre équipe que 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 l'utilisateur IAM.

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 la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonGuardDutyFullAccess

Vous pouvez associer la politique `AmazonGuardDutyFullAccess` à vos identités IAM.

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 déterminer `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 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 politique `AmazonGuardDutyReadOnlyAccess` à vos identités IAM.

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 des opérations d'API 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 joindre de `AmazonGuardDutyServiceRolePolicy` à vos entités IAM. Cette politique AWS gérée est associée à un rôle lié à un service qui permet d' GuardDuty effectuer des actions en votre nom. Pour plus d'informations, consultez 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 flux RSS sur la page Historique du GuardDuty document.

Modification	Description	Date
AmazonGuardDutyFullAccess – Mise à jour d'une stratégie existante	Autorisation ajoutée qui vous permet de transmettre un rôle IAM GuardDuty lorsque vous activez Malware Protection pour S3. `{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow",`	10 juin 2024

Modification	Description	Date

	"Action": [
	"iam:PassRole"
	],
	"Resource":
	"arn:aws:iam::*:role/
	*",
	"Conditio
	n": {
	"StringEquals": {
	"iam:PassedToServi
	ce": "guarddut
	y.amazonaws.com"
	}
	}
	}	

AmazonGuardDutyServiceRolePolicy - Mettre à jour vers une politique existante.	Utilisez AWS Systems Manager des actions pour gérer les associations SSM sur les instances Amazon EC2 lorsque vous GuardDuty activez la surveillance du temps d'exécution avec un agent automatisé pour Amazon EC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les instances EC2 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 compte Amazon VPC partagé et définir la politique de point de terminaison Amazon VPC 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` l'une permet de `ListSnapshotBlocks` récupérer l'instantané d'un volume EBS (chiffré à l'aide Clé gérée par AWS) sur votre compte de service Compte AWS et de le copier sur le compte de GuardDuty service avant de démarrer l'analyse des logiciels malveillants.	25 janvier 2024
AmazonGuardDutyServiceRolePolicy – Mise à jour d’une politique existante	De nouvelles autorisations ont été ajoutées GuardDuty pour permettre d'ajouter des paramètres de compte `guarddutyActivate` Amazon ECS et d'effectuer des opérations de liste et de description sur les clusters Amazon ECS.	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 d'exécution d' GuardDutyEKS.	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 pour EC2. GuardDuty peut désormais effectuer l'action IAM 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 ARN mis à jour pour `iam:GetRole` to`*AWSServiceRoleForAmazonGuardDutyMalwareProtection` .	26 juillet 2022

Modification	Description	Date
AmazonGuardDutyFullAccess – Mise à jour d’une politique existante	GuardDuty a ajouté un nouveau `AWSServiceName` pour autoriser la création d'un rôle lié à un service à l'aide `iam:CreateServiceLinkedRole` du service GuardDuty Malware Protection for EC2. 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 réseau Amazon EC2 pour améliorer les résultats. GuardDuty peut désormais effectuer les actions EC2 suivantes pour obtenir des informations sur la façon dont vos instances EC2 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 IAM.

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 quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `guardduty:`*`GetWidget`* 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 Services AWS 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 utilisateur IAM 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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès 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 fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- 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 l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Validation de conformité pour Amazon GuardDuty

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS 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 Services AWS 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 sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- 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 Services AWS et décrivent 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 Service AWS 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 Service AWS 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, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS 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 dans Amazon GuardDuty

En tant que service géré, Amazon GuardDuty est protégé par la sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez des appels d'API publiés AWS pour accéder à GuardDuty via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou 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 ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

AWS intégrations de 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 format JSON standard appelé AWS Security Finding Format (ASFF). Le format ASFF comprend des informations sur la source du problème, les ressources affectées et le statut actuel du résultat. Consultez AWS Security Finding Format (ASFF) dans le Guide de l'utilisateur AWS Security Hub .

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 ASFF (AWS Security Finding Format). Dans le format ASFF, le champ `Types` fournit le type de résultat.

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 ASFF (AWS Security Finding Format). Dans le format ASFF, le champ `Types` fournit le type de résultat. Les types ASFF utilisent un schéma de dénomination différent de celui des GuardDuty types. Le tableau ci-dessous détaille

tous les types de GuardDuty recherche avec leur équivalent ASFF tels qu'ils apparaissent dans Security Hub.

> **Note**
>
> Pour certains types de GuardDuty recherche, Security Hub attribue des noms de recherche ASFF différents selon que le rôle de ressource du détail de la recherche était ACTOR ou TARGET. Pour plus d'informations, consultez Détails d'un résultat.

GuardDuty type de recherche	Type de résultat ASFF
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	Type de résultat ASFF
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: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
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

GuardDuty type de recherche	Type de résultat ASFF
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
DefenseEvasion: Je suis un utilisateur/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand

GuardDuty type de recherche	Type de résultat ASFF
Découverte : IAMuser/ AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
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
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile

GuardDuty type de recherche	Type de résultat ASFF
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/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual

GuardDuty type de recherche	Type de résultat ASFF
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
Incidence : 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	Type de résultat ASFF
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: Je suis un utilisateur/ Anomalous Behavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
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
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions

GuardDuty type de recherche	Type de résultat ASFF
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
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: Je suis un utilisateur/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
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/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape

GuardDuty type de recherche	Type de résultat ASFF
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
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

GuardDuty type de recherche	Type de résultat ASFF
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
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

GuardDuty type de recherche	Type de résultat ASFF
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
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

GuardDuty type de recherche	Type de résultat ASFF
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/Unauthorized Access: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
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

GuardDuty type de recherche	Type de résultat ASFF
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 en utilisant le format ASFF (AWS Security Finding Format).

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.

Arrêt de la publication des résultats sur Security Hub

Pour arrêter l'envoi des résultats à Security Hub, vous pouvez utiliser la console Security Hub ou l'API.

Consultez la section Désactivation et activation du flux de résultats d'une intégration (console) ou Désactivation du flux de résultats d'une intégration (API Security Hub, AWS CLI) dans le guide de l'AWS Security Hub utilisateur.

Intégration à Amazon Detective

Amazon Detective vous aide à analyser et à examiner rapidement les événements de sécurité liés à un ou plusieurs comptes AWS en générant des visualisations de données représentant le comportement et l'interaction de vos ressources au fil du temps. Detective crée des visualisations des résultats GuardDuty.

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 un Compte AWS, une ressource AWS au sein d'un compte ou une adresse IP externe qui a interagi avec vos ressources. La console GuardDuty permet de basculer vers Amazon Detective à partir des entités suivantes, en fonction du type de résultat : Compte AWS, du rôle IAM, de l'utilisateur ou de la session de rôle, de l'agent utilisateur, de l'utilisateur fédéré, de l'instance Amazon EC2 ou de l'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 GuardDuty et Detective, l'intégration est activée automatiquement. Une fois activé, Detective ingère immédiatement les données de vos résultats GuardDuty.

> **Note**
>
> GuardDuty envoie des résultats à Detective en fonction de la fréquence d'exportation des résultats GuardDuty. Par défaut, la fréquence d'exportation pour les mises à jour des résultats existants est de 6 heures. Pour que Detective reçoive les mises à jour les plus récentes de vos résultats, il est recommandé de modifier la fréquence d'exportation à 15 minutes dans chaque région dans laquelle vous utilisez Detective avec GuardDuty. Pour de plus amples informations, veuillez consulter Étape 5 — Définition de la fréquence d'exportation des résultats actifs mis à jour.

Basculement vers Amazon Detective depuis un résultat GuardDuty

1. Connectez-vous à la console à l'adresse https://console.aws.amazon.com/guardduty/.
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 un résultat GuardDuty dans la console Detective, il est également archivé dans la console GuardDuty.

Utilisation de l'intégration avec un environnement à comptes multiples GuardDuty

Si vous gérez un environnement à comptes multiples dans GuardDuty, vous devez ajouter vos comptes de membre à Amazon Detective afin de consulter les visualisations des données de Detective relatives aux résultats et aux entités dans ces comptes.

Il est recommandé d'utiliser le même compte administrateur de GuardDuty que le compte administrateur de 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 Amazon GuardDuty SNS

Cette section fournit des informations sur l'abonnement à Amazon SNS (Simple Notification Service) GuardDuty pour les annonces visant à recevoir des notifications concernant les nouveaux types de recherche, les mises à jour des types de recherche existants et d'autres modifications de fonctionnalités. Les notifications sont proposées dans tous les formats pris en charge par Amazon SNS.

Le GuardDuty SNS envoie 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 utilisateur IAM doit disposer des autorisations `sns::subscribe` pour pouvoir s'abonner à une rubrique SNS.

Vous pouvez abonner une file d'attente Amazon SQS à cette rubrique de notification, mais vous devez utiliser un ARN de rubrique se trouvant dans la même région. Pour plus d'informations, veuillez consulter Didacticiel : Abonnement d'une file d'attente Amazon SQS à une rubrique Amazon SNS 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, veuillez consulter Invocation des fonctions Lambda en utilisant des notifications Amazon SNS dans le Guide du développeur Amazon Simple Queue Service.

Les ARN de la rubrique Amazon SNS pour chaque région sont indiqués ci-après.

AWS Région	ARN de rubrique Amazon SNS
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`

AWS Région	ARN de rubrique Amazon SNS
us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

AWS Région	ARN de rubrique Amazon SNS
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	ARN de rubrique Amazon SNS
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	ARN de rubrique Amazon SNS
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	ARN de rubrique Amazon SNS
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 console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans la liste des régions, choisissez la même région que celle dans laquelle se trouve l'ARN de la rubrique à laquelle 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 ARN de la rubrique, collez l'ARN de la rubrique : `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 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 provenant de Amazon SNS.

Pour vous abonner à l'e-mail de notification de GuardDuty mise à jour avec le 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 provenant de Amazon SNS.

Format du message Amazon SNS

Voici un exemple de message de notification de GuardDuty mise à jour concernant les nouvelles découvertes :

```
{
    "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."
    }]
}
```

Voici un exemple de message de notification de GuardDuty mise à jour concernant les mises à jour des GuardDuty fonctionnalités :

```
{
    "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_cloudtrail\"}]}",
    "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_cloudtrail"
    }]
}
```

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 Service AWS. 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 Services AWSet 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 programmes malveillants pour les quotas EC2.
> - 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 Limite du processeur et de la 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

GuardDuty 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 Protection contre les malwares pour EC2 sur Amazon GuardDuty et utiliser les nouveaux plans de GuardDuty protection à

Actions/paramètres hérités	Nouvelles actions/Nouveaux paramètres	Comparison (Comparaison)
dans GuardDuty Modifications apportées à l'API 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 recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
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 ressource Amazon EC2. Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour l'instance Amazon EC2. Pour plus d'informations sur la mise à jour manuelle de l'agent de sécurité vers cette version, consultez Gestion manuelle	13 juin 2024

	de l'agent de sécurité pour l'instance Amazon EC2.	
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 rôle IAM 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	RDS Protection étend le support pour surveiller l'activité de connexion sur vos bases de données RDS pour PostgreSQL. Dans le cadre de cette extension, GuardDuty nous commencerons automatiquement à surveiller les données de connexion des bases de données RDS pour PostgreSQL pour les comptes qui ont déjà activé la protection RDS. GuardDuty Pour plus d'informations, consultez la section Protection RDS.	6 juin 2024
Fonctionnalité mise à jour dans GuardDuty Runtime Monitoring - Fargate (Amazon ECS uniquement)	Runtime Monitoring a publié une nouvelle version d'agent 1.2.0 pour les ressources 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 for EC2	Pour chaque volume Amazon EBS attaché à vos instances Amazon EC2 et à vos charges de travail de conteneur GuardDuty , Malware Protectio n for EC2 a augmenté la taille du volume EBS qu'il analyse jusqu'à 2 048 Go. Pour plus d'informations sur l'analyse des volumes Amazon EBS attachés à vos instances, consultez GuardDuty Malware Protection for EC2.	29 mai 2024
Fonctionnalité mise à jour dans Runtime Monitoring	La surveillance du temps d'exécution pour les ressource s Amazon ECS-Fargate permet désormais de détecter les menaces potentielles sur vos tâches lancées par et. AWS Batch AWS CodePipel ine Pour plus d'informations, consultez Comment fonctionn e la surveillance du temps d'exécution avec Fargate (Amazon ECS 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 les ressource s Amazon EKS. Pour plus d'informations sur les notes de mise à jour, consultez l'historique des versions de l'agent complémentaire EKS.	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 protection RDS	GuardDuty étend le support de protection RDS aux éléments suivants : Régions AWS • Canada Ouest (Calgary) • Asie-Pacifique (Hyderabad) • Europe (Espagne) • Europe (Zurich) • Moyen-Orient (EAU) • Israël (Tel Aviv) • Asie-Pacifique (Melbourne) Pour plus d'informations sur l'activation de cette fonctionn alité, consultez la section Protection RDS.	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 ressource s Amazon EKS. Pour plus d'informations sur les notes de mise à jour, consultez l'historique des versions de l'agent complémentaire EKS.	29 avril 2024
Support pour IPAddressV6	GuardDuty a ajouté le support IPAddressv6 pour les détails IP locaux et distants. Vous pouvez utiliser les attributs de filtre associés pour filtrer GuardDuty les résultats ou créer des règles de suppressi on.	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 ressource Amazon EC2. Cette version prend en charge la configuration GuardDuty automatique des agents dans Runtime Monitoring pour les instances Amazon EC2. Pour plus d'informations sur les notes de publication, consultez l'agent GuardDuty de sécurité pour l'instance Amazon EC2.	28 mars 2024

Disponibilité générale de la surveillance du temps d'exécution pour les instances Amazon EC2	GuardDuty annonce la disponibilité générale (GA) de la surveillance du temps d'exécution pour les instances Amazon EC2. 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 instances Amazon EC2 en votre nom. Avec l'agent GuardDuty automatis é, vous pouvez également utiliser des balises d'inclusi on ou d'exclusion GuardDuty pour indiquer d'installer et de gérer l'agent de sécurité uniquement sur certaines instances Amazon EC2. Pour plus d'informations, consultez Comment fonctionn e la surveillance du temps d'exécution avec les instances Amazon EC2. Liste des nouveaux types de trouvailles publiés en même temps que cette AG • Exécution : Runtime/ SuspiciousTool • Exécution : Runtime/ SuspiciousCommand	28 mars 2024

- DefenseEvasion:Temps d'exécution/ SuspiciousCommand
- 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 associations SSM sur les instances Amazon EC2 lorsque vous GuardDuty activez la surveillance du temps d'exécution avec un agent automatisé pour Amazon EC2. Lorsque la configuration GuardDuty automatique des agents est désactivée, ne GuardDuty prend en compte que les instances EC2 dotées d'une balise d'inclusion (`GuardDuty Managed :true`). • La liste suivante indique les nouvelles autorisations : `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	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 Amazon EKS, Runtime Monitoring prend désormais en charge la configuration de paramètres spécifiques de votre agent de GuardDuty sécurité, tels que les paramètres du processeur et de la mémoire, `PriorityClass` les paramètres et les paramètres de politique DNS. Pour plus d'informations, voir Configuration des paramètres GuardDuty de l'agent de sécurité (module complémentaire EKS).	7 mars 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié une nouvelle version d'agent 1.5.0 pour les ressources Amazon EKS. Pour plus d'informations sur les notes de mise à jour, consultez l'historique des versions de l'agent complémentaire EKS.	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 clusters Amazon EKS ne seront plus prises en charge à compter du 14 mai 2024. Pour plus d'informations sur les étapes à suivre avant la fin du support standard, consultez l'agent GuardDuty de sécurité pour les clusters Amazon EKS.	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 de la surveillance du temps d'exécution - Disponibilité régionale	GuardDuty Runtime Monitoring prend désormais en charge le partage d'Amazon VPC au sein de celui-ci. AWS Organizations GuardDuty le rôle lié à un service (SLR) dispose d'une nouvelle autorisation, `organizations:DescribeOrganization` qui permet de récupérer l'identifiant de l'organisation pour le compte Amazon VPC 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 terminaison Amazon VPC partagé dans le cadre de la surveillance du temps d'exécution, consultez Support pour le partage d'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 de la surveillance du temps d'exécution - Disponibilité régionale	GuardDuty Runtime Monitoring prend désormais en charge le partage d'Amazon VPC au sein de celui-ci. AWS Organizations GuardDuty le rôle lié à un service (SLR) dispose d'une nouvelle autorisation, `organizations:DescribeOrganization` qui permet de récupérer l'identifiant de l'organisation pour le compte Amazon VPC 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 terminaison Amazon VPC partagé dans le cadre de la surveillance du temps d'exécution, consultez Support pour le partage d'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 la nouvelle version Régions AWS : Malware Protection for EC2	Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS 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 la nouvelle version Régions AWS : Malware Protection for EC2	Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS chiffrés avec Clés gérées par AWS 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 instances Amazon EC2. Cette version de l'agent inclut la prise en charge des dernières AMI Amazon ECS. Pour plus d'informations sur l'historique des versions de l'agent, consultez GuardDuty la section Agent de sécurité pour les instances Amazon EC2.	2 février 2024

Fonctionnalité mise à jour avec prise en charge de la nouvelle version Régions AWS : Malware Protection for EC2	Malware Protection for EC2 prend désormais en charge l'analyse des volumes Amazon EBS chiffrés avec Clés gérées par AWS 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	Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS chiffrés avec Clés gérées par AWS les méthodes suivantes : Régions AWS • Asie-Pacifique (Jakarta) (`ap-southeast-3`) • USA Ouest (Californie du Nord) (`us-west-1`) • Moyen-Orient (EAU) (`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 for EC2	Malware Protection for EC2 prend désormais en charge l'analyse des volumes EBS chiffrés à l'aide de. Clés gérées par AWSMalware Protection for EC2 service-linked role (SLR) dispose de deux nouvelles autorisations : et. `GetSnapshotBlock` `ListSnapshotBlocks` Ces autorisations vous aideront à GuardDuty récupérer l'instantané d'un volume EBS (chiffré à l'aide de Clé gérée par AWS) sur 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 la section Agent de sécurité pour les instances Amazon EC2.	23 janvier 2024
Fonctionnalité mise à jour dans Runtime Monitoring	Runtime Monitoring a publié la version 1.4.1 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations, veuillez consulter Historique des versions de l'agent de module complémentaire EKS (langue française non garantie).	16 janvier 2024
Runtime Monitoring a publié un nouvel agent v1.4.0 pour les ressources Amazon EKS	Runtime Monitoring a publié la version 1.4.0 d'un nouvel agent pour les ressources Amazon EKS. Pour plus d'informations, veuillez consulter Historique des versions de l'agent de module complémentaire EKS (langue française non garantie).	21 décembre 2023

Ajout de types de résultats basés sur 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), en Europe (Paris), en Asie-Pacifique (Osaka), en Asie-Pacifique (Séoul), au Moyen-Orient (Bahreïn), en Europe (Espagne), en Asie-Pacifique (Hyderabad), en Asie-Pacifique (Melbourne), en Israël (Tel Aviv), en 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 clusters Amazon EKS, GuardDuty annonce la disponibilité générale de Runtime Monitoring pour détecter les menaces pesant sur vos charges de travail Amazon ECS et d'une version préliminaire pour détecter les menaces visant vos instances Amazon EC2. Pour plus d'informations sur ceux qui prennent Régions AWS actuellement en charge la surveillance du temps d'exécution, voir Régions et points de terminaison.	26 novembre 2023

Amazon GuardDuty a mis à jour le rôle lié au service (SLR)	GuardDuty a ajouté de nouvelles autorisations permettant d'utiliser les actions Amazon ECS pour gérer et récupérer des informations sur les clusters Amazon ECS, et de gérer les paramètre s du compte Amazon ECS avec`guarddutyActivate` . Les actions relatives à Amazon ECS récupèrent également les informations relatives aux balises associées 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 EKS Audit Log Monitoring.	EKS Audit 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 EKS Audit Log Monitoring.	EKS Audit 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 EKS Audit Log Monitoring.	EKS Audit Log Monitoring 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	
La surveillance d'exécution EKS a publié un nouvel agent version 1.3.1	EKS Runtime Monitoring a publié une nouvelle version d'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. Le suffixe de domaine de requête DNS fournit le domaine de deuxième et de premier niveau impliqué dans l'activité GuardDuty à l'origine de la recherche.	17 octobre 2023
La surveillance d'exécution EKS a publié un nouvel agent version 1.3.0 compatible avec Kubernetes version 1.28	EKS Runtime 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, veuillez consulter Historique des versions de l'agent de module complémentaire EKS (langue française non garantie).	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 (Émirats arabes unis)	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 (Émirats arabes unis) : • 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 EKS Runtime Monitoring introduit GuardDuty la gestion des agents de sécurité au niveau du cluster	EKS Runtime Monitoring prend en charge la gestion de l'agent de GuardDuty sécurité pour les clusters EKS individuels afin de surveiller les événements d'exécution provenant uniquement de ces clusters sélectifs. La surveillance d'exécution EKS étend cette fonctionnalité avec la prise en charge des balises.	13 septembre 2023
GuardDuty Malware Protection for EC2 étend 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) : • GuardDuty Protection EKS inclut la surveillance des journaux d'audit EKS et la surveillance d'exécution EKS. • GuardDuty Protection Lambda. • GuardDuty Protection contre les logiciels malveillants pour EC2. • GuardDuty 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

La surveillance d'exécution EKS est désormais disponible en Asie-Pacifique (Melbourne)	La surveillance du temps d'exécution GuardDuty EKS intégrée à EKS Protectio n permet de détecter les menaces d'exécution pour vos clusters Amazon EKS dans votre AWS 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 détection d'EKS Runtime Monitoring peuvent désormais invoquer une analyse des programme s malveillants GuardDuty initiée par EKS 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

La surveillance d'exécution EKS annonce trois nouveaux types de résultat.	La surveillance d'exécution EKS prend en charge trois nouveaux types de résultat 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
La surveillance d'exécution EKS a publié un nouvel agent version 1.2.0 compatible avec Kubernetes version 1.27	EKS Runtime Monitoring a publié une nouvelle version d'agent 1.2.0 qui prend également en charge les instances basées sur ARM64. Ajout de la prise en charge de Bottlerocket. Pour plus d'informations, veuillez consulter Historique des versions de l'agent de module complémentaire EKS (langue française non garantie).	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
La surveillance des journaux d'audit EKS est désormais disponible dans les régions Asie-Pacifique (Hyderabad), Asie-Pacifique (Melbourne), Europe (Zurich) et Europe (Espagne).	Activez la surveillance des journaux d'audit EKS (dans EKS Protection) pour que vos comptes surveillent les journaux d'audit EKS de vos clusters Amazon EKS et les analysent pour détecter toute activité potentiellement malveillante et suspecte.	1er juin 2023
La surveillance des journaux d'audit EKS est désormais disponible dans la région Moyen-Orient (EAU).	EKS Audit Log Monitoring est désormais disponible au Moyen-Orient (Émirats arabes unis). Activez la surveillance des journaux d'audit EKS pour vos comptes afin de surveiller les journaux d'audit EKS de vos clusters Amazon EKS et de les analyser pour détecter toute activité potentiellement malveillante et suspecte.	3 mai 2023

GuardDuty Malware Protection for EC2 annonce une analyse des programmes malveillants à la demande	Malware Protection for EC2 vous aide à détecter la présence potentielle de programmes malveillants dans les volumes Amazon EBS attachés à vos instances Amazon EC2 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 volumes Amazon EBS uniquement lorsqu'elle GuardDuty génère l'un des résultats invoquant GuardDuty une analyse des programmes malveillants initiée par cette dernière. Vous pouvez lancer une analyse des logiciels malveilla nts à la demande pour les instances Amazon EC2 de votre compte en fournissant l'Amazon Resource Name (ARN) associé à cette instance Amazon EC2. Pour plus d'informations sur les différenc es entre les deux types de scan, consultez Malware Protection for EC2. • GuardDuty-analyse des logiciels malveillants initiée	27 avril 2023

	• 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 ajout de 3 nouveaux types de résultats EC2	GuardDuty introduit de nouveaux types de recherche pour détecter l'utilisation de résolveurs DNS externes et de technologies DNS 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 d'exécution d'EKS dans EKS Protection	La surveillance du temps d'exécution EKS intégrée à EKS Protection permet de détecter les menaces d'exécution pour vos clusters Amazon EKS dans votre AWS environnement. Il utilise un agent de module complémentaire Amazon EKS (`aws-guardduty-agent`) qui collecte les événements d'exécution de vos charges de travail EKS. Après avoir GuardDuty reçu ces événements d'exécution, il les surveille et les analyse afin d'identifier les menaces de sécurité suspectes potentiel les. Pour plus d'informations, veuillez consulter les sections Détails du résultat et Types de résultat de la surveillance d'exécution EKS.	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 API suivantes sont concernées par cette nouvelle fonctionnalité : • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23 mars 2023

La fonctionnalité de protection RDS d'Amazon GuardDuty est désormais disponible pour tous	GuardDuty RDS Protection surveille et établit le profil de l'activité de connexion RDS afin d'identifier les comportements de connexion suspects sur vos instances de base de données Amazon Aurora. Pour plus d'informations sur les Régions AWS qui prennent en charge la protection RDS, veuillez consulter Régions et points de terminaison.	16 mars 2023

GuardDuty annonce l'activation de la fonctionnalité	Historiquement, l' GuardDuty API permettait de configurer à la fois les fonctionnalités et les sources de données, 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 l'API mais n'ajoutera pas de nouvelle API. L'activation des fonctionnalités affecte le comportement des API utilisées pour activer GuardDuty ou le type de protection qu'elles contiennent GuardDuty. Si vous gérez vos GuardDuty comptes via une API, un SDK ou un modèle CFN, consultez les modifications apportées à GuardDuty l'API en mars 2023.	16 mars 2023
GuardDuty La protection contre les logiciels malveillants pour EC2 est désormais disponible dans la région Moyen-Orient (EAU)	La fonctionnalité de protection contre les programmes malveillants pour EC2 GuardDuty est prise en charge dans la région du Moyen-Orient (Émirats arabes unis). 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 GuardDuty temps d'exécution d'EKS. • Utilisez les actions Amazon EKS pour gérer et récupérer des informations sur les clusters EKS, et gérer les modules complémentaires EKS sur des clusters EKS. Les actions EKS 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 pour EC2 SLR une fois que la protection contre les programmes malveillants pour EC2 a été activée.	21 février 2023

GuardDuty nécessite TLS v1.2 ou version ultérieure	Pour communiquer avec les AWS ressources, GuardDuty nécessite et prend en charge le protocole TLS v1.2 ou version ultérieure. 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 meilleures pratiques en matière d'IAM	Mise à jour du guide s’aligner sur les bonnes pratiques IAM. Pour plus d’informations, consultez Bonnes pratiques 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 RDS Protection surveille et établit le profil de l'activité de connexion RDS afin d'identifier les comportements de connexion suspects sur vos instances de base de données Amazon Aurora. Actuellement, elle est disponible 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 (EAU)	Le Moyen-Orient (EAU) a été ajouté à la liste des pays Régions AWS où GuardDuty il 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 for EC2	GuardDuty Malware Protection for EC2 est une amélioration optionnelle d'Amazon GuardDuty. Tout en GuardDuty identifiant les ressources à risque, Malware Protection for EC2 détecte les malwares susceptibles d'être à l'origine de la compromission. Lorsque Malware Protection for EC2 est activée, chaque fois qu'un comportement suspect est GuardDuty détecté sur une instance Amazon EC2 ou qu'une charge de travail de conteneur indique la présence d'un logiciel malveillant GuardDuty , Malware Protection for EC2 lance une analyse sans agent sur les volumes EBS attachés aux charges de travail d'instance ou de conteneur EC2 concernées afin de détecter la présence de logiciels malveillants. Pour plus d'informations sur le fonctionnement de Malware Protection for EC2 et sur la configuration de cette fonctionnalité, consultez GuardDuty Malware Protection for EC2. • Pour plus d'informations sur les résultats de la protection contre les programme	26 juillet 2022

	s malveillants pour EC2, consultez la section Recherche de détails. • Pour plus d'informations sur la correction de l'instanc e EC2 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 malveilla nts et les raisons pour lesquelles une ressource est ignorée lors d'une analyse de programmes malveilla nts, consultez la section Comprendre CloudWatch les journaux et les raisons des sauts. • Pour plus d'informations sur les détections de faux positifs, 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 résultat identifient si une demande d'API a invoqué une entité IAM de manière anormale. 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. 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 protection GuardDuty EKS pour GuardDuty	GuardDuty peut désormais générer des résultats pour vos ressources Amazon EKS grâce à la surveillance des journaux d'audit EKS. Pour savoir comment configurer cette fonctionnalité, consultez EKS Protection sur Amazon GuardDuty. Pour obtenir une liste des résultats que GuardDuty vous pouvez générer pour les ressources Amazon EKS, 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 recherche suivants pour identifier et hiérarchiser les problèmes liés aux CVE-2021-44228 et CVE-2021-45046 : Backdoor:EC2/C&CActivity.B ; Backdoor:EC2/C&CActivity.B ! 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
Mise à jour vers GuardDuty SLR	Le GuardDuty SLR a été mis à jour avec de nouvelles actions visant à améliorer la précision de la recherche.	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 résultat IAMUser basés sur un comportement anormal pour les principaux IAM. 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 résultats EC2 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. Un nouveau résultat EC2 a également été ajouté pour C&CActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 janvier 2021

Ajout de 4 nouveaux types de résultat.	Ajout de 3 nouveaux résultats S3 MaliciousIPCaller. Discovery:S3/MaliciousIPCallerExfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Un nouveau résultat EC2 a également été ajouté 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 accessibles via l'API.	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 associé à EMR sur une instance EC2 n'est pas bloqué et est en train d'être analysé activement. En savoir plus	8 mai 2019
Ajout de 5 nouveaux types de résultat qui détectent si vos instances EC2 sont susceptibles d'être utilisées pour les attaques Denial of Service (DoS).	Ces résultats vous informent des instances EC2 dans votre environnement qui se comportent d'une manière pouvant indiquer qu'elles sont utilisées pour réaliser des attaques Denial of 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 résultat généré sera basé sur la catégorie de l'API qui a été invoquée depuis un réseau inhabituel. En savoir plus	21 décembre 2018
Ajout de deux nouveaux types de résultat : PenTest:IAMUser/ParrotLinux et PenTest:IAMUser/PentooLinux	Le type de résultat PenTest:IAMUser/ParrotLinux vous informe qu'un ordinateur exécutant Parrot Security Linux effectue des appels d'API en utilisant les informations d'identification qui appartiennent à votre compte AWS . Le type de résultat PenTest:IAMUser/PentooLinux vous informe qu'une machine exécutant Pentoo Linux effectue des appels d'API en utilisant les informations d'identification qui appartiennent à votre compte AWS . En savoir plus	21 décembre 2018

Ajout de la prise en charge de la rubrique Amazon GuardDuty Annonces (SNS)	Vous pouvez désormais vous abonner à la rubrique SNS des GuardDuty annonces pour recevoir des notifications concernant les nouveaux types de résultats, les mises à jour des types de résultats existants et les autres modifications apportées aux fonctionnalités. Les notifications sont proposées dans tous les formats pris en charge par Amazon SNS. 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 instance EC2 de votre AWS environnement établit des connexions à un nœud Tor Guard ou Authority. UnauthorizedAccess:EC2/TorRelayfinding type vous indique qu'une instance EC2 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 instance EC2 de votre AWS environnement interroge un nom de domaine associé à 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 ultérieur es 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 automatiq uement 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 automatiq uement 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'adresse s IP fiables et des listes de menaces pour les comptes d' GuardDuty administrateur et les comptes de membres.	Avec cette version, les utilisate urs 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'adresse s 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.