aws

Guide de l’utilisateur

Amazon Inspector

Amazon Inspector: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon Inspector ?

Amazon Inspector AWS Amazon Inspector découvre et analyse automatiquement les instances Amazon EC2 en cours d'exécution, les images des conteneurs dans Amazon Elastic Container Registry (Amazon ECR) et les AWS Lambda fonctions pour détecter les vulnérabilités logicielles connues et les expositions réseau involontaires.

Amazon Inspector crée un résultat lorsqu'il découvre une vulnérabilité logicielle ou un problème de configuration réseau. Une constatation décrit la vulnérabilité, identifie la ressource affectée, évalue la gravité de la vulnérabilité et fournit des conseils pour y remédier. Vous pouvez analyser les résultats à l'aide de la console Amazon Inspector ou consulter et traiter vos résultats via une autre consoleServices AWS. Pour plus d'informations, veuillez consulter Comprendre les résultats dans Amazon Inspector.

Rubriques

Caractéristiques d'Amazon Inspector

Gérez de manière centralisée plusieurs comptes Amazon Inspector

Si votre AWS environnement comporte plusieurs comptes, vous pouvez gérer votre environnement de manière centralisée via un seul compte à l'aide de AWS Organizations. Avec cette approche, vous pouvez désigner un compte comme compte administrateur délégué Amazon Inspector

Amazon Inspector peut être activé pour l'ensemble de votre organisation en un seul clic. En outre, vous pouvez automatiser l'activation du service pour les future membres chaque fois qu'ils rejoignent votre organisation. Le compte d'administrateur délégué Amazon Inspector peut gérer les résultats, les données et certains paramètres pour les membres de l'organisation. Cela inclut l'affichage des détails des résultats agrégés pour tous les comptes des membres, l'activation ou la désactivation des scans des comptes des membres et l'examen des ressources scannées au sein de l'AWSorganisation.

Analysez en permanence votre environnement pour détecter les vulnérabilités et l'exposition du réseau

Amazon Inspector Amazon Inspector découvre automatiquement vos ressources éligibles et commence à les analyser. Amazon Inspector continue d'évaluer votre environnement tout au long

du cycle de vie de vos ressources en réanalysant automatiquement les ressources en réponse aux modifications susceptibles d'introduire une nouvelle vulnérabilité, par exemple : installation d'un nouveau package dans une instance EC2, installation d'un correctif et lors de la publication de nouvelles vulnérabilités et expositions courantes (CVE) affectant la ressource. Contrairement aux logiciels d'analyse de sécurité traditionnels, Amazon Inspector a un impact minimal sur les performances de votre parc.

Lorsque des vulnérabilités ou des chemins réseau ouverts sont identifiés, Amazon Inspector produit un résultat que vous pouvez examiner. La découverte inclut des détails complets sur la vulnérabilité, la ressource affectée et des recommandations de correction. Si vous corrigez correctement une constatation, Amazon Inspector détecte automatiquement la correction et ferme la découverte.

Évaluez les vulnérabilités avec précision grâce au score de risque d'Amazon Inspector

Au fur et à mesure qu'Amazon Inspector collecte des informations sur votre environnement par le biais d'analyses, il fournit des scores de gravité spécifiquement adaptés à votre environnement. Amazon Inspector examine les mesures de sécurité qui constituent le score de base de la National Vulnerability Database (NVD) pour une vulnérabilité et les ajuste en fonction de votre environnement informatique. Par exemple, le service peut abaisser le score Amazon Inspector d'une découverte concernant une instance Amazon EC2 si la vulnérabilité est exploitable sur le réseau mais qu'aucun chemin réseau ouvert vers Internet n'est disponible depuis l'instance. Ce score est au format CVSS et constitue une modification du score de base du Common Vulnerability Scoring System (CVSS) fourni par NVD.

Identifiez les résultats à fort impact avec le tableau de bord Amazon Inspector

Le tableau de bord Amazon Inspector offre une vue d'ensemble des résultats obtenus dans l'ensemble de votre environnement. Dans le tableau de bord, vous pouvez accéder aux détails granulaires d'une constatation. Le tableau de bord contient des informations simplifiées sur la couverture des scans dans votre environnement, vos résultats les plus critiques et les ressources ayant généré le plus de résultats. Le panneau de correction basé sur les risques du tableau de bord Amazon Inspector présente les résultats qui concernent le plus grand nombre d'instances et d'images. Ce panneau permet d'identifier plus facilement les résultats ayant le plus d'impact sur votre environnement, d'examiner les détails des résultats et d'examiner les solutions proposées.

Gérez vos résultats à l'aide de vues personnalisables

Outre le tableau de bord, la console Amazon Inspector propose une vue des résultats. Cette page répertorie tous les résultats relatifs à votre environnement et fournit les détails des résultats

individuels. Vous pouvez consulter les résultats regroupés par catégorie ou par type de vulnérabilité. Dans chaque vue, vous pouvez personnaliser davantage vos résultats à l'aide de filtres. Vous pouvez également utiliser des filtres pour créer des règles de suppression qui masquent les résultats indésirables dans vos vues.

Vous pouvez utiliser des filtres et des règles de suppression pour générer des rapports de recherche qui présentent tous les résultats ou une sélection personnalisée de résultats. Les rapports peuvent être générés au format CSV ou JSON.

Surveillez et traitez les résultats avec d'autres services et systèmes

Pour faciliter l'intégration avec d'autres services et systèmes, Amazon Inspector publie les résultats sur Amazon EventBridge sous forme d'événements de recherche. EventBridgeest un service de bus d'instance sans serveur qui peut acheminer les données de recherche vers des cibles, notamment des AWS Lambda fonctions et des rubriques Amazon Simple Notification Service (Amazon SNS). Vous pouvez ainsi surveiller et traiter les résultats en temps quasi réel dans le cadre de vos flux de travail de sécurité et de conformité existants. EventBridge

Si vous l'avez activé AWS Security Hub, Amazon Inspector publiera également les résultats sur Security Hub. Security Hub est un service qui fournit une vue complète de votre posture de sécurité dans votre AWS environnement et vous permet de vérifier votre environnement par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Avec Security Hub, vous pouvez plus facilement surveiller et traiter vos résultats dans le cadre d'une analyse plus large de la posture de sécurité de votre organisation dansAWS.

Accès à Amazon Inspector

Amazon Inspector est disponible dans la plupart des casRégions AWS. Pour voir la liste Amazon Inspector régions dans lesquelles Amazon Inspector Pour en savoir plusRégions AWS, consultez la section Gestion Régions AWS dans la référence générale d'Amazon Web Services. Dans chaque région, vous pouvez utiliser Amazon Inspector

AWSConsole de gestion

AWS Management ConsoleIl s'agit d'une interface basée sur un navigateur que vous pouvez utiliser pour créer et gérer AWS des ressources. Dans le cadre de cette console, la console Amazon Inspector permet d'accéder à votre compte et à vos ressources Amazon Inspector. Vous pouvez effectuer des Amazon Inspector

AWSOutils de ligne de commande

Avec les outils de ligne de AWS commande, vous pouvez envoyer des commandes à la ligne de commande de votre système pour effectuer des tâches Amazon L'utilisation de la ligne de commande peut être plus rapide et plus pratique que d'utiliser la console. Les outils de ligne de commande sont également utiles si vous souhaitez créer des scripts exécutant des tâches .

AWS fournit deux jeux d'outils de ligne de commande : l'AWS Command Line Interface (AWS CLI) et les AWS Tools for PowerShell. Pour plus d'informations sur l'installation et la configuration de l'interface de ligne de AWScommandeAWS CLI, veuillez consulter le Guide de l'utilisateur de l'interface de ligne de commande. Pour plus d'informations sur l'installation et la configuration des outils ToolsPowerShell, consultez le Guide de AWS Tools for PowerShell l'utilisateur.

Kits SDK AWS

AWSfournit des kits SDK composés de bibliothèques et d'exemples de code pour différentes langages et plateformes de programmation, notamment Java, Go, Python, C++ et .NET. Les kits SDK fournissent un accès pratique et programmatique à Amazon Inspector et à d'autres applications. Services AWS Ils automatisent également les tâches telles que la signature cryptographique des demandes, la gestion des erreurs et les nouvelles tentatives automatiques de demande. Pour plus d'informations sur l'installation et l'utilisation AWS des kits SDK, consultez la section Outils de développement. AWS

API REST Amazon Inspector

L'API REST Amazon Inspector vous donne un accès programmatique complet à votre compte et à vos ressources Amazon Inspector. Avec cette API, vous pouvez envoyer des requêtes HTTPS directement à Amazon Inspector. Toutefois, contrairement aux outils de ligne de AWS commande et aux kits SDK, il faut alors que votre application gère les détails de bas niveau, notamment la génération d'un hachage pour signer une demande.

Commencer à utiliser Amazon Inspector

Ce didacticiel fournit une introduction pratique à Amazon Inspector.

L'étape 1 couvre l'activation des scans Amazon Inspector pour un compte autonome ou en tant qu'administrateur délégué Amazon Inspector AWS Organizations dans un environnement multi-comptes.

L'étape 2 consiste à comprendre les résultats d'Amazon Inspector dans la console.

> **Note**
>
> Dans ce didacticiel, vous allez effectuer des tâches dans votre version actuelle Région AWS. Pour configurer Amazon Inspector dans d'autres régions, vous devez effectuer ces étapes dans chacune de ces régions.

Rubriques

Avant de commencer

Amazon Inspector est un service de gestion des vulnérabilités qui analyse en permanence vos instances Amazon EC2, les images de conteneur Amazon ECR et les AWS Lambda fonctions pour détecter les vulnérabilités logicielles et les expositions involontaires au réseau.

Avant d'activer Amazon Inspector, prenez note des points suivants :

- Amazon Inspector est un service régional et les données sont stockées Région AWS là où vous utilisez le service. Toutes les procédures de configuration que vous effectuez dans ce didacticiel doivent être répétées dans chacune des procédures Région AWS que vous souhaitez surveiller avec Amazon Inspector.
- Amazon Inspector vous donne la flexibilité d'activer l'instance Amazon EC2, l'image du conteneur Amazon ECR et AWS Lambda les fonctions de numérisation. Vous pouvez gérer les types de

numérisation depuis la page de gestion des comptes de la console Amazon Inspector ou à l'aide des API Amazon Inspector.

- Amazon Inspector peut fournir des données CVE (Common Vulnerabilities and Exposures) pour vos instances EC2 uniquement si l'agent Amazon EC2 Systems Manager (SSM) est installé et activé. Cet agent est préinstallé sur de nombreuses instances EC2, mais vous devrez peut-être l'activer manuellement. Quel que soit le statut de l'agent SSM, toutes vos instances EC2 sont analysées pour détecter tout problème d'exposition au réseau. Pour plus d'informations sur la configuration des scans pour Amazon EC2, consultez. Numérisation d'instances Amazon EC2 Amazon ECR et AWS Lambda Function Scanning ne nécessitent pas l'utilisation d'un agent.
- Une identité d'utilisateur IAM avec des autorisations d'administrateur Compte AWS peut activer Amazon Inspector. Pour des raisons de protection des données, nous vous recommandons de protéger vos informations d'identification et de configurer des utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur ne reçoit que les autorisations nécessaires pour gérer Amazon Inspector. Pour plus d'informations sur les autorisations requises pour activer Amazon Inspector, consultezAWS politique gérée : AmazonInspector2FullAccess.
- Lorsque vous activez Amazon Inspector pour la première fois dans une région, un rôle lié à un service est créé dans le monde entier pour votre compte appelé. `AWSServiceRoleForAmazonInspector2` Ce rôle inclut les autorisations et les politiques de confiance qui permettent à Amazon Inspector de collecter les détails des packages logiciels et d'analyser les configurations Amazon VPC afin de générer des découvertes de vulnérabilité. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon Inspector. Pour de plus amples informations sur les rôles liés à un service, veuillez consulter Utilisation des rôles liés à un service.

Étape 1 : activer Amazon Inspector

La première étape pour utiliser Amazon Inspector consiste à l'activer pour votre Compte AWS. Une fois que vous avez activé un type de scan Amazon Inspector, Amazon Inspector commence immédiatement à découvrir et à analyser toutes les ressources éligibles.

Si vous souhaitez gérer Amazon Inspector pour plusieurs comptes au sein de votre organisation via un compte administrateur centralisé, vous devez désigner un administrateur délégué pour Amazon Inspector. Choisissez l'une des options suivantes pour savoir comment activer Amazon Inspector pour votre environnement.

Standalone account environment

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Sélectionnez Get started (Mise en route).
3. Choisissez Activer Amazon Inspector.

Lorsque vous activez Amazon Inspector dans un compte autonome, tous les types de scan sont activés par défaut. Vous pouvez gérer les types de scan activés depuis la page de gestion des comptes de la console Amazon Inspector ou à l'aide des API Amazon Inspector. Une fois Amazon Inspector activé, il découvre et commence à analyser automatiquement toutes les ressources éligibles. Consultez les informations relatives au type de scan suivantes pour savoir quelles ressources sont éligibles par défaut :

Numérisation Amazon EC2

Pour fournir des données CVE (Common Vulnerabilities and Exposures) pour votre instance EC2, Amazon Inspector exige que l'agent AWS Systems Manager (SSM) soit installé et activé. Cet agent est préinstallé sur de nombreuses instances EC2, mais vous devrez peut-être l'activer manuellement. Quel que soit le statut de l'agent SSM, toutes vos instances EC2 seront analysées pour détecter tout problème d'exposition au réseau. Pour plus d'informations sur la configuration des scans pour Amazon EC2, consultez. Numérisation d'instances Amazon EC2 avec Amazon Inspector

Numérisation Amazon ECR

Lorsque vous activez le scan Amazon ECR, Amazon Inspector convertit tous les référentiels de conteneurs de votre registre privé qui sont configurés pour le scan de base par défaut fourni par Amazon ECR en un scan amélioré avec analyse continue. Vous pouvez également éventuellement configurer ce paramètre pour analyser uniquement en mode push ou pour analyser certains référentiels via des règles d'inclusion. Toutes les images envoyées au cours des 30 derniers jours sont programmées pour une numérisation à vie. Ce paramètre de numérisation Amazon ECR peut être modifié à tout moment. Pour plus d'informations sur la configuration des scans pour Amazon ECR, consultezNumérisation d'images de conteneurs Amazon ECR avec Amazon Inspector.

AWS Lambda fonction de numérisation

Lorsque vous activez l'analyse des AWS Lambda fonctions, Amazon Inspector découvre les fonctions Lambda de votre compte et commence immédiatement à les analyser pour détecter les vulnérabilités. Amazon Inspector analyse les nouvelles fonctions et couches Lambda lorsqu'elles sont déployées, et les réanalyse lorsqu'elles sont mises à jour ou lorsque de nouvelles vulnérabilités et expositions communes (CVE) sont publiées. Amazon Inspector propose deux niveaux différents de numérisation des fonctions Lambda. Par défaut, lorsque vous activez Amazon Inspector pour la première fois, le scan standard Lambda est activé, qui analyse les dépendances des packages dans vos fonctions. Vous pouvez également activer le scan du code Lambda pour scanner le code du développeur dans vos fonctions afin de détecter les vulnérabilités du code. Pour plus d'informations sur la configuration de l'analyse des fonctions Lambda, consultez. AWS Lambda Fonctions de numérisation avec Amazon Inspector

Multi-account environment

Important

Pour effectuer ces étapes, vous devez appartenir à la même organisation que tous les comptes que vous souhaitez gérer et avoir accès au compte de AWS Organizations gestion afin de déléguer un administrateur pour Amazon Inspector au sein de votre organisation. Des autorisations supplémentaires peuvent être nécessaires pour déléguer un administrateur. Pour de plus amples informations, veuillez consulter Autorisations requises pour désigner un administrateur délégué.

Note

Pour activer Amazon Inspector par programmation pour plusieurs comptes dans plusieurs régions, vous pouvez utiliser un script shell développé par Amazon Inspector. Pour plus d'informations sur l'utilisation de ce script, consultez l'inspector2- enablement-with-cli on. GitHub

Délégation d'un administrateur pour Amazon Inspector

1. Connectez-vous au compte de AWS Organizations gestion.

2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
3. Dans le volet Administrateur délégué, entrez l'identifiant à douze chiffres de celui Compte AWS que vous souhaitez désigner comme administrateur délégué Amazon Inspector pour l'organisation. Choisissez ensuite Déléguer. Ensuite, dans la fenêtre de confirmation, sélectionnez à nouveau Déléguer.

> **Note**
>
> Amazon Inspector est activé pour votre compte lorsque vous déléguez un administrateur.

Ajouter des comptes de membres

En tant qu'administrateur délégué, vous pouvez activer le scan pour tout membre associé au compte de gestion des Organizations. Ce flux de travail active tous les types de scan pour tous les comptes membres. Toutefois, les membres peuvent également activer Amazon Inspector pour leurs propres comptes, ou les scans d'un service peuvent être activés de manière sélective par l'administrateur délégué. Pour de plus amples informations, veuillez consulter Gestion de plusieurs comptes .

1. Connectez-vous au compte d'administrateur délégué.
2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
3. Dans le volet de navigation, choisissez Account Management. Le tableau Accounts affiche tous les comptes membres associés au compte de gestion des Organizations.
4. Sur la page Gestion des comptes, vous pouvez sélectionner Activer la numérisation pour tous les comptes dans le bandeau supérieur pour activer les instances EC2, les images des conteneurs ECR et les AWS Lambda fonctions de numérisation pour tous les comptes de votre organisation. Vous pouvez également choisir les comptes que vous souhaitez ajouter en tant que membres en les sélectionnant dans le tableau Comptes. Ensuite, dans le menu Activer, sélectionnez Toutes les numérisations.
5. (Facultatif) Activez la fonctionnalité Activation automatique de l'Inspecteur pour les nouveaux comptes membres et sélectionnez les types de scan à inclure pour activer ces scans pour tous les nouveaux comptes membres ajoutés à votre organisation.

Amazon Inspector propose actuellement des scans pour les instances EC2, les images de conteneurs ECR et AWS Lambda les fonctions. Une fois que vous avez activé Amazon Inspector, celui-ci commence automatiquement à découvrir et à analyser toutes les ressources éligibles. Consultez les informations relatives au type de scan suivantes pour savoir quelles ressources sont éligibles par défaut :

Numérisation Amazon EC2

Pour fournir des données sur les vulnérabilités CVE pour vos instances EC2, Amazon Inspector exige que l'agent AWS Systems Manager (SSM) soit installé et activé. Cet agent est préinstallé sur de nombreuses instances EC2, mais vous devrez peut-être l'activer manuellement. Quel que soit le statut de l'agent SSM, toutes vos instances EC2 seront analysées pour détecter tout problème d'exposition au réseau. Pour plus d'informations sur la configuration des scans pour Amazon EC2, consultez. Numérisation d'instances Amazon EC2 avec Amazon Inspector

Numérisation Amazon ECR

Lorsque vous activez le scan Amazon ECR, Amazon Inspector convertit tous les référentiels de conteneurs de votre registre privé qui sont configurés pour le scan de base par défaut fourni par Amazon ECR en un scan amélioré avec scan continu. Vous pouvez également éventuellement configurer ce paramètre pour analyser uniquement en mode push ou pour analyser certains référentiels via des règles d'inclusion. Toutes les images envoyées au cours des 30 derniers jours sont programmées pour une numérisation à vie. Ce paramètre de scan Amazon ECR peut être modifié à tout moment par l'administrateur délégué. Pour plus d'informations sur la configuration des scans pour Amazon ECR, consultezNumérisation d'images de conteneurs Amazon ECR avec Amazon Inspector.

AWS Lambda fonction de numérisation

Lorsque vous activez l'analyse des AWS Lambda fonctions, Amazon Inspector découvre les fonctions Lambda de votre compte et commence immédiatement à les analyser pour détecter les vulnérabilités. Amazon Inspector analyse les nouvelles fonctions et couches Lambda lorsqu'elles sont déployées, et les réanalyse lorsqu'elles sont mises à jour ou lorsque de nouvelles vulnérabilités et expositions communes (CVE) sont publiées. Pour plus d'informations sur la configuration de l'analyse des fonctions Lambda, consultez. AWS Lambda Fonctions de numérisation avec Amazon Inspector

Étape 2 : Afficher les résultats d'Amazon Inspector

Vous pouvez consulter les résultats relatifs à votre environnement dans la console Amazon Inspector ou via l'API. Tous les résultats sont également transmis à Amazon EventBridge et AWS Security Hub (s'ils sont activés). En outre, les résultats des images de conteneurs sont transmis à Amazon ECR.

La console Amazon Inspector propose différents formats d'affichage pour vos résultats. Le tableau de bord Amazon Inspector vous donne une vue d'ensemble détaillée des risques pour votre environnement, tandis que le tableau des résultats vous permet de consulter les détails d'une constatation spécifique.

Au cours de cette étape, vous allez explorer les détails d'une constatation à l'aide du tableau des résultats et du tableau de bord des résultats. Pour plus d'informations sur le tableau de bord Amazon Inspector, consultezComprendre le tableau de bord.

Pour consulter le détail des résultats relatifs à votre environnement dans la console Amazon Inspector :

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Tableau de bord. Vous pouvez sélectionner l'un des liens du tableau de bord pour accéder à une page de la console Amazon Inspector contenant plus de détails sur cet article.
3. Dans le volet de navigation, sélectionnez Résultats.
4. Par défaut, vous verrez l'onglet Tous les résultats, qui affiche toutes les instances EC2, l'image du conteneur ECR et les résultats des AWS Lambda fonctions pour votre environnement.
5. Dans la liste des résultats, choisissez un nom de recherche dans la colonne Titre pour ouvrir le volet de détails correspondant à ce résultat. Tous les résultats comportent un onglet Détails de la recherche. Vous pouvez interagir avec l'onglet Détails de recherche de différentes manières :

   - Pour plus de détails sur la vulnérabilité, suivez le lien dans la section Détails de la vulnérabilité pour ouvrir la documentation relative à cette vulnérabilité.
   - Pour étudier plus en détail votre ressource, suivez le lien ID de ressource dans la section Ressource affectée pour ouvrir la console de service de la ressource affectée.

   Les résultats relatifs aux types de vulnérabilités des packages comportent également un score d'inspecteur et un onglet de renseignement sur les vulnérabilités expliquant comment le

score Amazon Inspector a été calculé pour ce résultat et fournissant des informations sur la vulnérabilité et les exploits courants (CVE) associés à ce résultat. Pour plus de détails sur la recherche de types, consultezRecherche de types dans Amazon Inspector.

Comprendre le tableau de bord Amazon Inspector

Le tableau de bord Amazon Inspector fournit un aperçu des statistiques agrégées relatives à vos AWS ressources dans la AWS région actuelle. Ces statistiques incluent des indicateurs clés concernant la couverture des ressources et les vulnérabilités actives. Le tableau de bord affiche également des groupes de données de résultats agrégées pour votre compte, tels que les instances Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Registry (Amazon ECR) et les AWS Lambda fonctions présentant les résultats les plus critiques. Pour effectuer une analyse plus approfondie, vous pouvez consulter les données complémentaires relatives aux éléments du tableau de bord.

Si votre compte est le compte d'administrateur délégué Amazon Inspector d'une organisation, le tableau de bord inclut la couverture des comptes, des statistiques agrégées et des données de résultats pour tous les comptes de votre organisation, y compris votre propre compte.

Affichage du tableau de bord

Le tableau de bord présente une vue d'ensemble de la couverture de votre environnement et des résultats critiques.

Pour afficher le tableau de bord :

1. Ouvrez la console Amazon Inspector https://console.aws.amazon.com/inspector/v2/home.
2. Dans le panneau de navigation, sélectionnez Dashboard (Tableau de bord).
3. Vous pouvez utiliser le tableau de bord de l'une des façons suivantes :

    - Le tableau de bord est actualisé automatiquement toutes les cinq minutes. Vous pouvez toutefois actualiser les données manuellement en sélectionnant l'icône d'actualisation dans le coin supérieur droit de la page.
    - Pour afficher les données de support d'un élément sur le tableau de bord, sélectionnez l'élément.
    - Si vous gérez plusieurs comptes par le biais d'AWSorganisations en tant qu'administrateur délégué Amazon Inspector, le tableau de bord affiche des statistiques agrégées pour vos comptes de membres. Pour filtrer le tableau de bord et afficher uniquement les données d'un compte donné, entrez l'ID de compte dans la zone Compte.

Comprendre les composants du tableau de bord et interpréter les données

Chaque section du tableau de bord Amazon Inspector fournit un aperçu des indicateurs clés ou des données de résultats actifs qui peuvent vous aider à comprendre l'état actuel des vulnérabilités de vos AWS ressourcesRégion AWS.

Couverture de l'environnement

La section Couverture de l'environnement fournit des statistiques sur les ressources analysées par Amazon Inspector. Dans cette section, vous pouvez voir le nombre et le pourcentage d'instances Amazon EC2, d'images Amazon ECR et de AWS Lambda fonctions numérisées par Amazon Inspector. Si vous gérez plusieurs comptes en AWS Organizations tant qu'administrateur délégué Amazon Inspector, vous verrez également le nombre total de comptes de l'organisation, le nombre de comptes pour lesquels Amazon Inspector est activé et le pourcentage de couverture qui en résulte pour l'organisation. Vous pouvez également utiliser cette section pour déterminer quelles ressources ne sont pas couvertes par Amazon Inspector. Ces ressources peuvent contenir des vulnérabilités susceptibles d'être exploitées pour mettre votre organisation en danger. Pour en savoir plus, consultez Évaluation de la couverture de votre AWS environnement par Amazon Inspector.

Le choix d'un groupe de couverture vous amène à la page de gestion du compte correspondant au groupe que vous avez sélectionné. La page de gestion des comptes vous indique quels comptes, instances Amazon EC2 et référentiels Amazon ECR sont couverts par Amazon Inspector.

Les groupes de couverture suivants sont disponibles :

- Compte
- instances
- Référentiels de conteneurs
- Images de conteneur
- Lambda

Conclusions critiques

La section Conclusions critiques fournit un décompte des vulnérabilités critiques de votre environnement et un décompte total de toutes les découvertes de votre environnement. Dans cette section, les chiffres sont affichés par ressource et par type d'évaluation. Pour plus

d'informations sur les résultats critiques et sur la manière dont Amazon Inspector détermine la criticité, consultezComprendre les résultats dans Amazon Inspector.

Le choix d'un groupe de conclusions critiques vous amène à la page Toutes les conclusions et applique automatiquement des filtres pour afficher toutes les conclusions critiques correspondant au groupe que vous avez sélectionné.

Les groupes de résultats critiques suivants sont disponibles :

- Résultats des images des conteneurs ECR
- Résultats d'Amazon EC2
- Résultats relatifs à l'accessibilité du réseau
- AWS Lambdarésultats relatifs aux fonctions

Corrections basées sur les risques

La section Corrections basées sur les risques présente les cinq principaux packages logiciels présentant des vulnérabilités critiques qui affectent le plus de ressources de votre environnement. La correction de ces packages peut réduire de manière significative le nombre de risques critiques pour votre environnement. Choisissez le nom du package logiciel pour voir les détails des vulnérabilités associées et les ressources affectées.

Comptes présentant les résultats les plus critiques

La section Comptes présentant les résultats les plus critiques présente les cinq principaux AWS comptes de votre environnement présentant les résultats les plus critiques, ainsi que le nombre total de résultats pour ce compte. Cette section n'est visible qu'à partir du compte administrateur délégué lorsqu'Amazon Inspector est configuré pour la numérisation multi-comptes avecAWS Organizations. Cette vue permet aux administrateurs délégués de comprendre quels comptes sont les plus à risque au sein de l'organisation.

Choisissez Account ID pour voir plus d'informations sur le compte du membre concerné.

Référentiels Amazon ECR contenant les résultats les plus critiques

La section Référentiels Elastic Container Registry (ECR) présentant les résultats les plus critiques répertorie les cinq référentiels Amazon ECR les plus importants de votre environnement présentant les résultats les plus critiques en matière d'images de conteneurs. La vue affiche le nom du référentiel, l'identifiant du AWS compte, la date de création du référentiel, le nombre de vulnérabilités critiques et le nombre total de vulnérabilités. Cette vue vous permet d'identifier les référentiels susceptibles de présenter le plus de risques.

Choisissez le nom du référentiel pour obtenir plus d'informations sur le référentiel concerné.

Images des conteneurs présentant les résultats les plus critiques

La section Images de conteneurs présentant les résultats les plus critiques répertorie les cinq images de conteneurs les plus critiques de votre environnement. La vue affiche les données des balises d'image, le nom du référentiel, le résumé de l'image, l'identifiant du AWS compte, le nombre de vulnérabilités critiques et le nombre total de vulnérabilités. Cette vue aide les propriétaires d'applications à identifier les images de conteneur qui peuvent avoir besoin d'être reconstruites et relancées.

Choisissez Image du conteneur pour obtenir plus d'informations sur l'image du conteneur concernée.

Instances présentant les résultats les plus critiques

La section Instances présentant les résultats les plus critiques répertorie les cinq instances Amazon EC2 présentant les résultats les plus critiques. La vue affiche l'identifiant de l'instance, l'identifiant du AWS compte, l'identifiant Amazon Machine Image (AMI), le nombre de vulnérabilités critiques et le nombre total de vulnérabilités. Cette vue aide les propriétaires d'infrastructure à identifier les instances qui peuvent nécessiter l'application de correctifs.

Choisissez ID d'instance pour obtenir plus d'informations sur l'instance Amazon EC2 concernée.

Amazon Machine Images (AMI) avec les résultats les plus critiques

La section Amazon Machine Images (AMI) présentant les résultats les plus critiques répertorie les cinq AMI de votre environnement présentant les résultats les plus critiques. La vue montre l'identifiant de l'AMI, l'identifiant du AWS compte, le nombre d'instances EC2 affectées exécutées dans l'environnement, la date de création de l'AMI, la plate-forme du système d'exploitation de l'AMI, le nombre de vulnérabilités critiques et le nombre total de vulnérabilités. Cette vue aide les propriétaires d'infrastructures à identifier les AMI qui peuvent nécessiter une reconstruction.

Choisissez Instances affectées pour voir plus d'informations sur les instances lancées à partir de l'AMI affectée.

AWS Lambdafonctions présentant les résultats les plus critiques

La section AWS LambdaFonctions présentant les résultats les plus critiques présente les cinq principales fonctions Lambda de votre environnement présentant les résultats les plus critiques. La vue montre le nom de la fonction Lambda, l'identifiant du AWS compte, l'environnement d'exécution, le nombre de vulnérabilités critiques, le nombre de vulnérabilités élevées et le

nombre total de vulnérabilités. Cette vue aide les propriétaires d'infrastructure à identifier les fonctions Lambda qui peuvent nécessiter une correction.

Choisissez le nom de la fonction pour obtenir plus d'informations sur la AWS Lambda fonction concernée.

Comprendre les résultats dans Amazon Inspector

Une constatation est un rapport détaillé sur une vulnérabilité affectant l'une de vos AWS ressources. Les résultats sont nommés d'après les vulnérabilités détectées et fournissent des évaluations de gravité, des informations sur les ressources affectées et des détails décrivant comment remédier aux vulnérabilités signalées.

Amazon Inspector génère un résultat chaque fois qu'il détecte une vulnérabilité dans une instance Amazon EC2, une image de conteneur dans un référentiel Amazon ECR ou une fonction. AWS Lambda Amazon Inspector analyse en permanence votre environnement informatique et stocke tous vos résultats actifs jusqu'à ce que vous les corrigiez.

Lorsque vous corrigez un résultat, celui-ci est automatiquement fermé et Amazon Inspector le supprime au bout de 7 jours. Lorsque vous supprimez une ressource, Amazon Inspector supprime tout résultat associé à cette ressource au bout de 30 jours.

Si vous désactivez Amazon Inspector, les résultats sont supprimés au bout de 24 heures. En cas de AWS suspension de votre compte, les résultats sont supprimés au bout de 90 jours.

Les résultats sont classés dans l'un des états suivants :

Actif

Amazon Inspector identifie les résultats qui n'ont pas été corrigés comme actifs.

Supprimé

Amazon Inspector identifie les résultats soumis à une ou plusieurs règles de suppression comme étant supprimés. Vous pouvez trouver les résultats supprimés dans la liste des résultats supprimés. Pour de plus amples informations, veuillez consulter Suppression des résultats d'Amazon Inspector à l'aide de règles de suppression.

Fermées

Une fois que vous avez corrigé une vulnérabilité, Amazon Inspector la détecte automatiquement et change l'état de la découverte en Fermé. Les résultats fermés sont supprimés au bout de 7 jours.

Rubriques

Recherche de types dans Amazon Inspector

Amazon Inspector génère des résultats pour les instances Amazon Elastic Compute Cloud (Amazon EC2), les images de conteneurs dans les référentiels Amazon Elastic Container Registry (Amazon ECR) et les fonctions. AWS Lambda Amazon Inspector peut générer les types de résultats suivants.

Vulnérabilité du package

Les résultats relatifs aux vulnérabilités des packages identifient les packages logiciels de votre AWS environnement qui sont exposés à des vulnérabilités et à des expositions communes (CVE). Les attaquants peuvent exploiter ces vulnérabilités non corrigées pour compromettre la confidentialité, l'intégrité ou la disponibilité des données, ou pour accéder à d'autres systèmes. Le système CVE est une méthode de référence pour les vulnérabilités et les expositions de sécurité des informations connues du public. Pour plus d'informations, consultez https://www.cve.org/.

Les détections CVE pour Linux sont ajoutées à Amazon Inspector dans les 24 heures suivant leur publication par les avis de sécurité des fournisseurs. Les détections CVE pour Windows sont ajoutées à Amazon Inspector dans les 48 heures suivant leur publication par Microsoft. Vous pouvez utiliser le Recherche dans la base de données de vulnérabilités Amazon Inspector pour voir si une détection CVE est prise en charge.

Amazon Inspector peut générer des informations sur les vulnérabilités des packages pour les instances EC2, les images de conteneurs ECR et les fonctions Lambda. Les résultats relatifs à la vulnérabilité des packages comportent des informations supplémentaires propres à ce type de découverte, à savoir le score de l'Inspector et les informations sur les vulnérabilités.

vulnérabilité du code

Les découvertes de vulnérabilités dans le code identifient les lignes de votre code susceptibles d'être exploitées par des attaquants. Les vulnérabilités du code incluent des failles d'injection, des fuites de données, une cryptographie faible ou un chiffrement manquant dans votre code.

Amazon Inspector évalue le code de votre application de fonction Lambda à l'aide d'un raisonnement automatique et d'un apprentissage automatique qui analyse le code de votre application pour vérifier sa conformité globale en matière de sécurité. Il identifie les violations des politiques et les vulnérabilités sur la base de détecteurs internes développés en collaboration avec Amazon CodeGuru. Pour une liste des détections possibles, consultez la section Bibliothèque CodeGuru de détecteurs.

> **Important**
>
> Le scan de code Amazon Inspector capture des extraits de code pour mettre en évidence les vulnérabilités détectées. Ces extraits peuvent afficher des informations d'identification codées en dur ou d'autres informations sensibles en texte clair.

Amazon Inspector peut générer des informations sur les vulnérabilités du code pour les fonctions Lambda si vous les avez Numérisation du code Lambda d'Amazon Inspector activées.

Les extraits de code détectés en lien avec une vulnérabilité de code sont stockés par le CodeGuru service. Par défaut, une clé AWS détenue contrôlée par CodeGuru est utilisée pour chiffrer votre code, mais vous pouvez utiliser votre propre clé gérée par le client pour le chiffrement via l'API Amazon Inspector. Pour plus d'informations, consultez Chiffrement inexistant pour le code contenu dans vos résultats.

Accessibilité du réseau

Les résultats relatifs à l'accessibilité du réseau indiquent qu'il existe des chemins réseau ouverts vers les instances Amazon EC2 dans votre environnement. Ces résultats apparaissent lorsque vos ports TCP et UDP sont accessibles depuis les périphériques du VPC, comme une passerelle Internet (y compris les instances situées derrière des équilibreurs de charge d'application ou des équilibreurs de charge classiques), une connexion d'appairage VPC ou un VPN via une passerelle virtuelle. Ces résultats mettent en évidence des configurations réseau qui peuvent être trop permissives, telles que des groupes de sécurité mal gérés, des listes de contrôle d'accès ou des passerelles Internet, ou qui peuvent autoriser un accès potentiellement malveillant.

Amazon Inspector génère uniquement des résultats d'accessibilité au réseau pour les instances Amazon EC2. Amazon Inspector analyse les données relatives à l'accessibilité du réseau toutes les 24 heures.

Amazon Inspector évalue les configurations suivantes lors de la recherche de chemins réseau :

- Instances Amazon EC2
- Fonctions AWS Lambda
- Application Load Balancers
- Direct Connect
- Elastic Load Balancers
- Interfaces réseau Elastic
- Passerelles Internet
- Listes de contrôle d'accès au réseau
- Tables de routage
- Groupes de sécurité
- Sous-réseaux
- Clouds privés virtuels
- Passerelles privées virtuelles
- Points de terminaison d'un VPC
- Points de terminaison de la passerelle VPC
- Connexions d'appairage de VPC
- Connexions VPN

Localisation et affichage des résultats d'Amazon Inspector

Les procédures décrites dans cette section décrivent comment localiser et consulter les résultats dans Amazon Inspector via la console et l'API Amazon Inspector. Les détails de la recherche varient en fonction du type de découverte, du type de vulnérabilité et des ressources concernées. Pour de plus amples informations, veuillez consulter Amazon Inspector trouve des informations.

Console

Pour afficher les résultats dans la console

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Findings. Vous êtes dirigé vers un écran de résultats où vous pouvez consulter l'ensemble de vos résultats. Dans le tableau des résultats, vous pouvez choisir un résultat en sélectionnant le nom du résultat dans la colonne Titre.

3. (Facultatif) Vous pouvez également consulter les résultats regroupés par catégorie. Dans le volet de navigation, choisissez Findings, puis choisissez l'une des catégories suivantes :

   - Par vulnérabilité
   - Par instance

   > **Note**
   >
   > Les résultats regroupés par instance n'incluent pas d'informations sur la disponibilité du réseau.

   - Par image de conteneur
   - Par référentiel de conteneurs
   - Par fonction Lambda

API

Exécutez l'opération ListFindingsAPI. Dans la demande, vous pouvez spécifier `filterCriteria`de renvoyer des résultats spécifiques.

Amazon Inspector trouve des informations

Dans la console Amazon Inspector, vous pouvez consulter les détails de chaque résultat. Les détails de la recherche varient en fonction du type de recherche.

Pour consulter les détails d'une recherche

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home
2. Sélectionnez la région dans laquelle vous souhaitez afficher les résultats.
3. Dans le volet de navigation, choisissez Findings pour afficher la liste des résultats
4. (Facultatif) Utilisez la barre de filtre pour sélectionner un résultat spécifique. Pour de plus amples informations, veuillez consulter Filtrer les résultats d'Amazon Inspector.
5. Choisissez une recherche pour afficher son panneau de détails.

Le panneau Détails de la recherche contient les caractéristiques d'identification de base de la recherche. Cela inclut le titre de la découverte ainsi qu'une description de base de la vulnérabilité identifiée, des suggestions de mesures correctives et un score de gravité. Pour plus d'informations sur la notation, voirNiveaux de gravité des conclusions d'Amazon Inspector.

Les détails disponibles pour une recherche varient en fonction du type de recherche et de la ressource concernée.

Tous les résultats contiennent le numéro d' Compte AWS identification pour lequel le résultat a été identifié, une gravité, un type de résultat, la date à laquelle le résultat a été créé et une section affectée à la ressource avec des détails sur cette ressource.

Le type de recherche détermine les informations de correction et de renseignement sur les vulnérabilités disponibles pour la découverte. Selon le type de recherche, différents détails de recherche sont disponibles.

Vulnérabilité du package

Les résultats de vulnérabilité des packages sont disponibles pour les instances EC2, les images de conteneurs ECR et les fonctions Lambda. Pour plus d'informations, consultez Vulnérabilité du package.

Les résultats relatifs à la vulnérabilité des packages incluent égalementScore Amazon Inspector et informations sur les vulnérabilités.

Ce type de recherche comporte les détails suivants :

- Correctif disponible — Indique si la vulnérabilité est corrigée dans une version plus récente des packages concernés. Possède l'une des valeurs suivantes :
  - `YES`, ce qui signifie que tous les packages concernés ont une version fixe.
  - `NO`, ce qui signifie qu'aucun package concerné n'a de version fixe.
  - `PARTIAL`, ce qui signifie qu'un ou plusieurs (mais pas tous) des packages concernés ont une version fixe.
- Exploit disponible — Indique que la vulnérabilité comporte un exploit connu.
  - `YES`, ce qui signifie que la vulnérabilité découverte dans votre environnement comporte un exploit connu. Amazon Inspector n'a aucune visibilité sur l'utilisation des exploits dans un environnement.
  - `NO`, ce qui signifie que cette vulnérabilité ne présente aucun exploit connu.

- Packages concernés — Répertorie chaque package identifié comme vulnérable dans la recherche, ainsi que les détails de chaque package :
- Filepath : ID du volume EBS et numéro de partition associés à une recherche. Ce champ est présent dans les résultats relatifs aux instances EC2 scannées à l'aide Numérisation sans agent de.
- Version installée/Version fixe — Numéro de version du package actuellement installé pour lequel une vulnérabilité a été détectée. Comparez le numéro de version installé avec la valeur située après la barre oblique (/). La deuxième valeur est le numéro de version du package qui corrige la vulnérabilité détectée, comme indiqué dans les Common Vulnerabilities and Exposures (CVE) ou dans l'avis associé à la découverte. Si la vulnérabilité a été corrigée dans plusieurs versions, ce champ répertorie la version la plus récente incluant le correctif. Si aucun correctif n'est disponible, cette valeur est`None available`.

  > **Note**
  >
  > Si un résultat a été détecté avant qu'Amazon Inspector ne commence à inclure ce champ dans les résultats, la valeur de ce champ est vide. Cependant, un correctif est peut-être disponible.

- Gestionnaire de packages : gestionnaire de packages utilisé pour configurer ce package.
- Correction : si un correctif est disponible via un package ou une bibliothèque de programmation mis à jour, cette section inclut les commandes que vous pouvez exécuter pour effectuer la mise à jour. Vous pouvez copier la commande fournie et l'exécuter dans votre environnement.

  > **Note**
  >
  > Les commandes de correction sont fournies à partir des flux de données des fournisseurs et peuvent varier en fonction de la configuration de votre système. Consultez les références de recherche ou la documentation du système d'exploitation pour obtenir des conseils plus spécifiques.

- Informations sur la vulnérabilité : fournit un lien vers la source préférée d'Amazon Inspector pour le CVE identifiée dans le résultat, telle que la National Vulnerability Database (NVD), REDHAT ou un autre fournisseur de système d'exploitation. De plus, vous trouverez les scores de gravité du résultat. Pour plus d'informations sur le score de gravité, telles que, voirNiveaux de gravité des conclusions d'Amazon Inspector. Les scores suivants sont inclus, y compris les vecteurs de notation pour chacun :

  - Score EPSS
  - Note de l'Inspecteur
  - CVSS 3.1 d'Amazon CVE
  - CVSS 3.1 de NVD
  - CVSS 2.0 de NVD (le cas échéant, pour les anciens CVE)
- Vulnérabilités associées — Spécifie les autres vulnérabilités liées à la découverte. Il s'agit généralement d'autres CVE qui ont un impact sur la même version du package, ou d'autres CVE appartenant au même groupe que le CVE trouvé, comme déterminé par le fournisseur.

vulnérabilité du code

Les résultats de vulnérabilité du code ne sont disponibles que pour les fonctions Lambda. Pour plus d'informations, consultez vulnérabilité du code. Ce type de recherche comporte les détails suivants :

- Correctif disponible — Pour les vulnérabilités du code, cette valeur est toujours la même`YES`.
- Nom du détecteur : nom du CodeGuru détecteur utilisé pour détecter la vulnérabilité du code. Pour obtenir la liste des détections possibles, consultez la bibliothèque de CodeGuru détecteurs.
- Balises de détection : les CodeGuru balises associées au détecteur CodeGuru utilisent des balises pour classer les détections.
- CWE pertinent : les identifiants de la Common Weakness Enumeration (CWE) sont associés à la vulnérabilité du code.
- Chemin du fichier — Emplacement du fichier contenant la vulnérabilité du code.
- Emplacement de la vulnérabilité — En ce qui concerne les vulnérabilités liées au code d'analyse du code Lambda, ce champ indique les lignes de code exactes où Amazon Inspector a détecté la vulnérabilité.
- Correction suggérée — Cela suggère comment le code peut être modifié pour corriger le résultat.

Accessibilité du réseau

Les résultats relatifs à l'accessibilité du réseau ne sont disponibles que pour les instances EC2. Pour plus d'informations, consultez Accessibilité du réseau. Ce type de recherche comporte les détails suivants :

- Plage de ports ouverts : plage de ports via laquelle l'instance EC2 est accessible.

- Chemins réseau ouverts : indique le chemin d'accès libre vers l'instance EC2. Sélectionnez un élément sur le chemin pour plus d'informations.
- Correction : recommande une méthode pour fermer le chemin réseau ouvert.

Score Amazon Inspector et informations sur les vulnérabilités

Dans la console Amazon Inspector, lorsque vous sélectionnez un résultat, vous pouvez consulter le score de l'inspecteur et l'onglet Vulnerability Intelligence affiche les détails du score pour la détection de vulnérabilité d'un package, ainsi que les détails des informations sur les vulnérabilités. Ces informations ne sont disponibles que pour les Vulnérabilité du package résultats.

Note d'Amazon Inspector

Le score Amazon Inspector est un score contextualisé créé par Amazon Inspector pour chaque recherche d'instance EC2. Le score Amazon Inspector est déterminé en corrélant les informations du score CVSS v3.1 de base avec les informations collectées dans votre environnement informatique lors des analyses, telles que les résultats d'accessibilité au réseau et les données d'exploitabilité. Par exemple, le score Amazon Inspector d'une découverte peut être inférieur au score de base si la vulnérabilité est exploitable sur le réseau, mais Amazon Inspector détermine qu'aucun chemin réseau ouvert vers l'instance vulnérable n'est disponible sur Internet.

Le score de base pour un résultat est le score de base CVSS v3.1 fourni par le fournisseur. Les scores de base des fournisseurs RHEL, Debian ou Amazon sont pris en charge, pour les autres fournisseurs, ou dans les cas où le fournisseur n'a pas fourni de score. Amazon Inspector utilise le score de base de la National Vulnerability Database (NVD). Amazon Inspector utilise le calculateur Common Vulnerability Scoring System version 3.1 pour calculer le score. Vous pouvez voir la source du score de base d'une découverte individuelle dans les détails de la découverte, sous la rubrique Détails de la vulnérabilité, en tant que source de vulnérabilité (ou packageVulnerabilityDetails.source dans le fichier JSON du résultat)

> **Note**
>
> Le score Amazon Inspector n'est pas disponible pour les instances Linux exécutant Ubuntu. Cela est dû au fait qu'Ubuntu définit sa propre gravité de vulnérabilité, qui peut différer de la gravité CVE associée.

Informations détaillées sur le score d'Amazon Inspector

Lorsque vous ouvrez la page de détails d'une découverte, vous pouvez sélectionner l'onglet Score de l'inspecteur et intelligence des vulnérabilités. Ce panneau montre la différence entre le score de base et le score de l'Inspector. Cette section explique comment Amazon Inspector a attribué l'indice de gravité en se basant sur une combinaison du score Amazon Inspector et du score du fournisseur pour le package logiciel. Si les scores diffèrent, ce panneau explique pourquoi.

Dans la section des métriques du score CVSS, vous pouvez voir un tableau avec des comparaisons entre les métriques du score de base CVSS et le score de l'Inspector. Les métriques comparées sont les métriques de base définies dans le document de spécification CVSS maintenu parfirst.org. Voici un résumé des indicateurs de base :

Vecteur d'attaque

Contexte dans lequel une vulnérabilité peut être exploitée. Pour les résultats d'Amazon Inspector, il peut s'agir d'un réseau, d'un réseau adjacent ou d'un réseau local.

Complexité des attaques

Cela décrit le niveau de difficulté auquel un attaquant sera confronté lorsqu'il exploitera la vulnérabilité. Un score faible signifie que l'attaquant ne devra remplir que peu ou pas de conditions supplémentaires pour exploiter la vulnérabilité. Un score élevé signifie qu'un attaquant devra investir des efforts considérables pour mener à bien une attaque avec cette vulnérabilité.

Privilège requis

Ceci décrit le niveau de privilège dont un attaquant aura besoin pour exploiter une vulnérabilité.

Interaction avec l'utilisateur

Cette métrique indique si une attaque réussie utilisant cette vulnérabilité nécessite un utilisateur humain autre que l'attaquant.

Scope (Portée)

Cela indique si une vulnérabilité dans un composant vulnérable a un impact sur les ressources des composants situés au-delà du périmètre de sécurité du composant vulnérable. Si cette valeur est inchangée, la ressource affectée et la ressource affectée sont identiques. Si cette valeur est modifiée, le composant vulnérable peut être exploité pour avoir un impact sur les ressources gérées par différentes autorités de sécurité.

Confidentialité

Cela mesure le niveau d'impact sur la confidentialité des données au sein d'une ressource lorsque la vulnérabilité est exploitée. Cela va de Aucun, où aucune confidentialité n'est perdue, à High, où toutes les informations contenues dans une ressource sont divulguées ou des informations confidentielles telles que les mots de passe ou les clés de chiffrement peuvent être divulguées.

Intégrité

Cela mesure le niveau d'impact sur l'intégrité des données au sein de la ressource affectée si la vulnérabilité est exploitée. L'intégrité est menacée lorsque l'attaquant modifie des fichiers au sein des ressources touchées. Le score varie de Aucun, lorsque l'exploit ne permet à un attaquant de modifier aucune information, à élevé, où, si elle était exploitée, la vulnérabilité permettrait à un attaquant de modifier tout ou partie des fichiers, ou les fichiers susceptibles d'être modifiés auraient de graves conséquences.

Disponibilité

Cela mesure le niveau d'impact sur la disponibilité de la ressource affectée lorsque la vulnérabilité est exploitée. Le score varie de Aucun, lorsque la vulnérabilité n'a aucun impact sur la disponibilité, à Élevé, où, si elle est exploitée, l'attaquant peut complètement refuser la disponibilité de la ressource ou rendre un service indisponible.

Renseignements sur les vulnérabilités

Cette section résume les informations disponibles sur le CVE provenant d'Amazon ainsi que les sources de renseignement de sécurité standard telles que Recorded Future et la Cybersecurity and Infrastructure Security Agency (CISA).

> **Note**
>
> Intel de CISA, Amazon ou Recorded Future ne sera pas disponible pour tous les CVE.

Vous pouvez consulter les informations détaillées sur les vulnérabilités dans la console ou à l'aide de l'BatchGetFindingDetailsAPI. Les informations suivantes sont disponibles dans la console :

AT&CK

Cette section présente les tactiques, techniques et procédures (TTP) du MITRE associées au CVE. Les TTP associés sont affichés. S'il existe plus de deux TTP applicables, vous pouvez

sélectionner le lien pour voir une liste complète. La sélection d'une tactique ou d'une technique ouvre des informations à ce sujet sur le site Web de MITRE.

CISA

Cette section couvre les dates pertinentes associées à la vulnérabilité. La date à laquelle l'Agence de cybersécurité et de sécurité des infrastructures (CISA) a ajouté la vulnérabilité au catalogue des vulnérabilités exploitées connues, sur la base de preuves d'une exploitation active, et la date d'échéance que la CISA prévoit que les systèmes seront corrigés. Ces informations proviennent de la CISA.

Malware connu

Cette section répertorie les kits d'exploitation et les outils connus qui exploitent cette vulnérabilité.

Preuve

Cette section récapitule les événements de sécurité les plus critiques liés à cette vulnérabilité. Si plus de 3 événements ont le même niveau de criticité, les trois événements les plus récents sont affichés.

Dernière fois signalé

Cette section indique la date du dernier exploit public connu pour cette vulnérabilité.

Niveaux de gravité des conclusions d'Amazon Inspector

Lorsqu'Amazon Inspector génère une détection de vulnérabilité, il attribue automatiquement une gravité à cette découverte. La gravité d'un résultat reflète les principales caractéristiques du résultat et peut donc vous aider à évaluer et à prioriser vos résultats. La gravité d'une constatation n'implique ni n'indique le caractère critique ou l'importance que pourrait avoir une ressource affectée pour votre organisation.

L'indice de gravité d'une constatation est déterminé par un score numérique correspondant à l'un des niveaux de gravité suivants : informationnel, faible, moyen, élevé ou critique.

La méthode utilisée par Amazon Inspector pour déterminer la gravité varie en fonction du type de constatation. Consultez les sections suivantes pour en savoir plus sur la façon dont Amazon Inspector détermine l'indice de gravité de chaque type de constatation.

Gravité de la vulnérabilité des progiciels

Amazon Inspector utilise le score NVD/CVSS comme base du score de gravité des vulnérabilités des progiciels. Le score NVD/CVSS est le score de gravité de la vulnérabilité publié par le NVD et défini par le CVSS. Le score NVD/CVSS est une composition de mesures de sécurité, telles que la complexité des attaques, la maturité du code d'exploitation et les privilèges requis. Amazon Inspector produit un score numérique de 1 à 10 qui reflète la gravité de la vulnérabilité. Amazon Inspector considère ce score comme un score de base car il reflète la gravité d'une vulnérabilité en fonction de ses caractéristiques intrinsèques, qui sont constantes dans le temps. Ce score suppose également l'impact le plus défavorable raisonnable sur les différents environnements déployés. La norme CVSS v3 associe les scores CVSS aux cotes de gravité suivantes.

Score	Évaluation
0	Informational
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

La gravité des vulnérabilités détectées dans les packages peut également être considérée comme non triagée. Cela signifie que le fournisseur n'a pas encore défini de score de vulnérabilité pour la vulnérabilité détectée. Dans ce cas, nous vous recommandons d'utiliser les URL de référence pour la recherche afin de rechercher cette vulnérabilité et de réagir en conséquence.

Les résultats relatifs à la vulnérabilité des packages incluent les scores suivants et les vecteurs de notation associés dans les détails de leur découverte :

- Score EPSS
- Note de l'Inspecteur
- CVSS 3.1 d'Amazon CVE
- CVSS 3.1 de NVD
- CVSS 2.0 de NVD (le cas échéant)

Gravité de la vulnérabilité du code

Pour détecter une vulnérabilité dans le code, Amazon Inspector utilise les niveaux de gravité définis par les CodeGuru détecteurs Amazon à l'origine de la découverte. Une gravité est attribuée à chaque détecteur à l'aide du système de notation CVSS v3. Pour une explication des CodeGuru utilisations de sévérité, voir les définitions de gravité dans le CodeGuru guide. Pour obtenir une liste des détecteurs par niveau de gravité, sélectionnez l'un des langages de programmation pris en charge ci-dessous :

- Détecteurs Python par gravité
- Détecteurs Java par gravité

Sévérité de l'accessibilité du réseau

Amazon Inspector détermine la gravité d'une vulnérabilité d'accessibilité au réseau en fonction du service, des ports et des protocoles exposés et du type de chemin ouvert. Le tableau suivant définit ces niveaux de gravité. La valeur de la colonne Open path rating représente les chemins ouverts provenant de passerelles virtuelles, de VPC homologues et de réseaux. AWS Direct Connect Tous les autres services, ports et protocoles exposés ont une cote de gravité informationnelle.

Service	Ports TCP	Ports UDP	Évaluation du chemin Internet	Évaluation des chemins ouverts
DHCP	67, 68, 546, 547	67, 68, 546, 547	Medium	Informational
Elasticsearch	9300, 9200	NA	Medium	Informational
FTP	21	21	High	Medium
Global catalog LDAP	3268	NA	Medium	Informational
Global catalog LDAP over TLS	3269	NA	Medium	Informational
HTTP	80	80	Low	Informational
HTTPS	443	443	Low	Informational

Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752	Medium	Informational
LDAP	389	389	Medium	Informational
LDAP over TLS	636	NA	Medium	Informational
MongoDB	27017, 27018, 27019, 28017	NA	Medium	Informational
MySQL	3306	NA	Medium	Informational
NetBIOS	137, 139	137, 138	Medium	Informational
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110	Medium	Informational
Oracle	1521, 1630	NA	Medium	Informational
PostgreSQL	5432	NA	Medium	Informational
Print services	515	NA	High	Medium
RDP	3389	3389	Medium	Low
RPC	111, 135, 530	111, 135, 530	Medium	Informational
SMB	445	445	Medium	Informational
SSH	22	22	Medium	Low
SQL Server	1433	1434	Medium	Informational
Syslog	601	514	Medium	Informational
Telnet	23	23	High	Medium
WINS	1512, 42	1512, 42	Medium	Informational

Gestion des résultats dans Amazon Inspector

Amazon Inspector propose plusieurs méthodes pour trier, regrouper et gérer vos résultats. Ces fonctionnalités vous permettent d'adapter les résultats à votre environnement, de les agréger selon différentes vues et de vous concentrer sur les vulnérabilités propres à votre AWS environnement spécifique.

Les résultats apparaissent dans différents affichages en fonction de leur état : actif, supprimé ou fermé. Par défaut, chaque vue affiche uniquement les résultats actifs. Une découverte active représente un problème de sécurité potentiel détecté par Amazon Inspector qui indique une vulnérabilité ou une menace potentielle. Les résultats supprimés sont des résultats actifs que vous avez exclus à l'aide de règles de suppression. Amazon Inspector définit automatiquement le statut d'une recherche comme étant close lorsqu'il détecte qu'elle est corrigée. Vous ne fermez pas les résultats manuellement.

Vous pouvez également consulter les résultats dans AWS Security Hub un service qui fournit une vue complète de l'état de sécurité de votre AWS environnement. Pour de plus amples informations, veuillez consulter Intégration d'Amazon Inspector avec AWS Security Hub. Les résultats des images de conteneur sont également disponibles dans la console Amazon ECR, et vous pouvez consulter les résultats de toutes les ressources à l'aide de AWS Command Line Interface (AWS CLI) ou de l'API.

Rubriques

Afficher les résultats d'Amazon Inspector

La console Amazon Inspector affiche les résultats sous forme d'onglets en fonction de groupements connexes. Chaque vue inclut des informations qui peuvent vous aider à analyser des vulnérabilités spécifiques, à identifier vos ressources les plus vulnérables et à évaluer l'impact global des vulnérabilités dans votre environnement. Vous pouvez accéder à un autre affichage des résultats en choisissant une option dans le panneau latéral de navigation des résultats. Vous pouvez également

créer un filtre dans chaque vue afin de vous concentrer sur des types de résultats spécifiques. Pour plus d'informations sur l'utilisation des filtres, consultezFiltrer les résultats d'Amazon Inspector.

Les résultats peuvent être regroupés selon les paramètres suivants :

- Par vulnérabilité : répertorie les vulnérabilités les plus critiques détectées dans votre environnement. Choisissez le titre d'une vulnérabilité dans cette vue pour ouvrir un volet de détails contenant des informations supplémentaires.
- Par compte : répertorie vos comptes, le pourcentage de couverture scanné par Amazon Inspector pour chaque compte et le nombre total de résultats critiques et graves pour chaque compte. Ce regroupement n'est disponible que pour les administrateurs délégués.
- Par instance : répertorie les instances Amazon EC2 les plus vulnérables de votre environnement.
- Par image de conteneur — Répertorie les images de conteneurs Amazon ECR les plus vulnérables de votre environnement.
- Par référentiel de conteneurs : affiche les référentiels présentant le plus de vulnérabilités.
- Par fonction Lambda — Affiche les fonctions Lambda présentant le plus de vulnérabilités.
- Tous les résultats : affiche la liste complète des résultats pour votre environnement. Il s'agit de l'affichage par défaut lorsque vous accédez à la page Résultats. Dans cette vue, vous pouvez filtrer par résultats actifs, supprimés et fermés.

Vous pouvez créer des règles de suppression basées sur des filtres afin d'exclure les résultats des vues des résultats. Pour de plus amples informations, veuillez consulter Suppression des résultats d'Amazon Inspector à l'aide de règles de suppression.

Filtrer les résultats d'Amazon Inspector

Un filtre de recherche vous permet de visualiser uniquement les résultats correspondant aux critères que vous spécifiez. Les résultats qui ne correspondent pas aux critères du filtre sont exclus de votre affichage. Vous pouvez créer des filtres de recherche à l'aide de la console Amazon Inspector. Pour utiliser ces filtres afin de supprimer automatiquement les résultats existants et futurs, voirSuppression des résultats d'Amazon Inspector à l'aide de règles de suppression.

Création de filtres dans la console Amazon Inspector

Dans chaque vue des résultats, vous pouvez utiliser la fonctionnalité de filtrage pour localiser les résultats présentant des caractéristiques spécifiques. Les filtres sont supprimés lorsque vous passez à un autre affichage à onglets.

Un filtre est composé d'un critère de filtre, qui consiste en un attribut de filtre associé à une valeur de filtre. Les résultats qui ne correspondent pas à vos critères de filtrage sont exclus de la liste des résultats. Par exemple, pour voir tous les résultats associés à votre compte administrateur, vous pouvez choisir l'attribut ID de AWS compte et l'associer à la valeur de votre identifiant de AWS compte à douze chiffres.

Certains critères de filtrage s'appliquent à tous les résultats, tandis que d'autres sont disponibles pour des types de ressources spécifiques ou uniquement pour des types de recherche.

Pour appliquer un filtre à la vue des résultats

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, choisissez Conclusions. La vue par défaut affiche tous les résultats ayant le statut Actif.
3. Pour filtrer les résultats par critère, sélectionnez la barre Ajouter un filtre pour afficher la liste de tous les critères de filtre applicables à cette vue. Différents critères de filtre sont disponibles dans différents affichages.
4. Choisissez un critère sur lequel vous souhaitez filtrer dans la liste.
5. Dans le volet de saisie des critères, entrez les valeurs de filtre souhaitées pour définir ce critère.
6. Choisissez Appliquer pour appliquer ce critère de filtre à vos résultats actuels. Vous pouvez continuer à ajouter d'autres critères de filtre en sélectionnant à nouveau la barre de saisie du filtre.
7. (Facultatif) Pour afficher vos résultats supprimés ou fermés, choisissez Actif dans la barre de filtre, puis choisissez Supprimé ou Fermé. Choisissez Afficher tout pour afficher les résultats actifs, supprimés et fermés dans la même vue.

Suppression des résultats d'Amazon Inspector à l'aide de règles de suppression

Utilisez les règles de suppression pour exclure les résultats correspondant aux critères. Par exemple, vous pouvez créer une règle qui supprime tous les résultats présentant un faible score de vulnérabilité, afin de vous concentrer uniquement sur les résultats les plus critiques.

> **Note**
>
> Les règles de suppression ne sont utilisées que pour filtrer votre liste de résultats et n'ont aucun impact sur les résultats et n'empêchent Amazon Inspector de générer des résultats.

Si Amazon Inspector génère des résultats qui correspondent à une règle de suppression, ils sont définis sur Supprimé. Les résultats correspondant à une règle de suppression n'apparaissent pas dans votre liste par défaut.

Amazon Inspector conserve les résultats supprimés jusqu'à ce qu'ils soient corrigés. Amazon Inspector détecte les résultats corrigés. Lorsqu'Amazon Inspector détecte un résultat corrigé, il le définit sur Fermé et le stocke pendant 7 jours.

Les résultats supprimés sont publiés sur Amazon AWS Security Hub et publiés EventBridge sous forme d'événements. Vous pouvez supprimer automatiquement les résultats indésirables dans Security Hub en modifiant le statut des résultats à l'aide d'une EventBridge règle. Pour plus d'informations, consultez Comment créer des règles de suppression automatique dans AWS Security Hub.

Vous ne pouvez pas créer de règle de suppression qui ferme ou corrige les résultats. Vous ne pouvez créer une règle de suppression que pour filtrer les résultats qui apparaissent dans votre liste. Vous pouvez consulter les résultats supprimés à tout moment dans la console Amazon Inspector.

> **Note**
>
> Les comptes membres d'une organisation ne peuvent pas créer ou gérer de règles de suppression.

Création d'une règle de suppression

Vous pouvez créer des règles de suppression pour filtrer la liste des résultats affichés par défaut. Vous pouvez créer une règle de suppression par programmation en utilisant l'CreateFilterAPI et en spécifiant `SUPRESS` comme valeur pour. `action`

> **Note**
>
> Seuls les comptes autonomes et les administrateurs délégués d'Amazon Inspector peuvent créer et gérer des règles de suppression. Les membres d'une organisation ne verront aucune option concernant les règles de suppression dans le volet de navigation.

Pour créer une règle de suppression (console)

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Règles de suppression. Puis, choisissez Create rule (Créer une règle).
3. Pour chaque critère, procédez comme suit :
   - Sélectionnez la barre de filtre pour afficher la liste des critères de filtre que vous pouvez ajouter à votre règle de suppression.
   - Sélectionnez les critères de filtre pour votre règle de suppression.
4. Lorsque vous avez fini d'ajouter des critères, entrez le nom de la règle et une description facultative.
5. Choisissez Enregistrer la règle. Amazon Inspector applique immédiatement la nouvelle règle de suppression et masque tous les résultats correspondant aux critères.

Affichage des résultats supprimés

Par défaut, Amazon Inspector n'affiche pas les résultats supprimés dans la console Amazon Inspector. Toutefois, vous pouvez consulter les résultats supprimés par une règle particulière.

Pour afficher les résultats supprimés

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Règles de suppression.
3. Dans la liste des règles de suppression, sélectionnez le titre de la règle.

Modification des règles de suppression

Vous pouvez modifier les règles de suppression à tout moment.

Pour modifier les règles de suppression

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home
2. Dans le volet de navigation, sélectionnez Règles de suppression.
3. Sélectionnez le titre de la règle de suppression que vous souhaitez modifier.
4. Apportez les modifications souhaitées, puis choisissez Enregistrer pour mettre à jour la règle.

Suppression de règles de suppression

Vous pouvez supprimer les règles de suppression. Si vous supprimez une règle de suppression, Amazon Inspector arrête de supprimer les occurrences nouvelles et existantes de découvertes qui répondent aux critères de la règle et qui ne sont pas supprimées par d'autres règles.

Une fois que vous avez supprimé une règle de suppression, les occurrences nouvelles et existantes de résultats répondant aux critères de la règle ont le statut Actif. Cela signifie qu'ils apparaissent par défaut sur la console Amazon Inspector. En outre, Amazon Inspector publie ces résultats sur AWS Security Hub et Amazon EventBridge sous forme d'événements.

Pour supprimer une règle de suppression

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Règles de suppression.
3. Cochez la case à côté du titre de la règle de suppression que vous souhaitez supprimer.
4. Choisissez Supprimer, puis confirmez votre choix de supprimer définitivement la règle.

Exportation de rapports de résultats depuis Amazon Inspector

Outre l'envoi des résultats à Amazon EventBridge AWS Security Hub, vous pouvez éventuellement les exporter vers un compartiment Amazon Simple Storage Service (Amazon S3) sous forme de rapport de résultats. Un rapport de résultats est un fichier CSV ou JSON qui contient les détails des

résultats que vous choisissez d'inclure dans le rapport. Il fournit un aperçu détaillé de vos résultats à un moment précis. Pour chaque découverte, le fichier inclut des informations telles que le nom de ressource Amazon (ARN) de la ressource affectée, la date et l'heure de création de la découverte, l'identifiant CVE (Common Vulnerabilities and Exposures) associé, ainsi que la gravité, le statut et les scores Amazon Inspector et CVSS de la découverte.

Lorsque vous configurez un rapport de résultats, vous commencez par spécifier les résultats à inclure dans le rapport. Par défaut, Amazon Inspector inclut les données relatives à toutes les découvertes Région AWS que vous avez actuellement enregistrées et dont le statut est Actif. Si vous êtes l'administrateur délégué d'Amazon Inspector pour une organisation, cela inclut les données de résultats pour tous les comptes membres de votre organisation.

Vous pouvez éventuellement personnaliser un rapport en filtrant les données. Les filtres vous permettent d'inclure ou d'exclure des données pour des résultats présentant des caractéristiques spécifiques, par exemple, tous les résultats critiques créés pendant une période spécifique, tous les résultats actifs pour une ressource particulière ou tous les résultats critiques d'un type spécifique. Si vous êtes l'administrateur Amazon Inspector d'une organisation, vous pouvez utiliser des filtres pour créer un rapport qui inclut les résultats relatifs Compte AWS à un membre spécifique de votre organisation, par exemple tous les résultats critiques d'un compte dont le statut est Actif et pour lesquels un correctif est disponible. Vous pouvez ensuite partager le rapport avec le propriétaire du compte à des fins de correction.

> **Note**
>
> Lorsque vous exportez un rapport de résultats à l'aide de l'CreateFindingsReportAPI, seuls les résultats actifs s'affichent par défaut. Pour voir les résultats supprimés ou fermés, vous devez spécifier `SUPPRESSED` ou `CLOSED` sous forme de valeurs pour les critères de filtre FindingStatus.

Lorsque vous exportez un rapport de résultats, Amazon Inspector chiffre les données à l'aide d'une clé AWS Key Management Service (AWS KMS) que vous spécifiez et ajoute le rapport dans un compartiment S3 que vous spécifiez également. La clé de chiffrement doit être une clé de chiffrement symétrique AWS Key Management Service (AWS KMS) gérée par le client et figurant dans la version actuelleRégion AWS. En outre, la politique relative aux clés doit autoriser Amazon Inspector à utiliser la clé. Le compartiment S3 doit également se trouver dans la région actuelle, et la politique du compartiment doit autoriser Amazon Inspector à ajouter des objets au compartiment.

Une fois qu'Amazon Inspector a fini de chiffrer et de stocker votre rapport, vous pouvez le télécharger depuis le compartiment S3 que vous avez spécifié ou le déplacer vers un autre emplacement. Vous pouvez également conserver le rapport dans le même compartiment S3 et utiliser ce compartiment comme référentiel pour les rapports de résultats que vous exportez ultérieurement.

Cette rubrique vous explique comment utiliser le AWS Management Console pour exporter un rapport de résultats. Le processus consiste à vérifier que vous disposez des autorisations nécessaires, à configurer les ressources dont vous avez besoin, puis à configurer et à exporter le rapport.

> **Note**
>
> Vous ne pouvez exporter qu'un seul rapport de résultats à la fois. Si une exportation est en cours, attendez qu'elle soit terminée avant d'essayer d'exporter un autre rapport.

Tâches

Après avoir exporté un rapport de résultats pour la première fois, les étapes 1 à 3 peuvent être facultatives. Cela dépend principalement du fait que vous souhaitez utiliser le même compartiment S3 et AWS KMS key pour les rapports suivants.

Si vous préférez exporter un rapport par programmation après les étapes 1 à 3, utilisez l'API CreateFindingsReportAmazon Inspector.

Étape 1 : Vérifier vos autorisations

Avant d'exporter un rapport de résultats depuis Amazon Inspector, vérifiez que vous disposez des autorisations nécessaires pour exporter les rapports de résultats et configurer les ressources nécessaires au chiffrement et au stockage des rapports. Pour vérifier vos autorisations, utilisez AWS Identity and Access Management (IAM) pour passer en revue les politiques IAM associées à votre identité IAM. Comparez ensuite les informations contenues dans ces politiques à la liste suivante des actions que vous devez être autorisé à effectuer pour exporter un rapport de résultats.

Amazon Inspector

Pour Amazon Inspector, vérifiez que vous êtes autorisé à effectuer les actions suivantes :

- `inspector2:ListFindings`
- `inspector2:CreateFindingsReport`

Ces actions vous permettent de récupérer les données de résultats pour votre compte et d'exporter ces données dans des rapports de résultats.

Si vous envisagez d'exporter des rapports volumineux par programmation, vous pouvez également vérifier que vous êtes autorisé à effectuer les actions suivantes : `inspector2:GetFindingsReportStatus` vérifier le statut des rapports et `inspector2:CancelFindingsReport` annuler les exportations en cours.

AWS KMS

PourAWS KMS, vérifiez que vous êtes autorisé à effectuer les actions suivantes :

- `kms:GetKeyPolicy`
- `kms:PutKeyPolicy`

Ces actions vous permettent de récupérer et de mettre à jour la politique clé AWS KMS key que vous souhaitez qu'Amazon Inspector utilise pour chiffrer votre rapport.

Pour utiliser la console Amazon Inspector pour exporter un rapport, vérifiez également que vous êtes autorisé à effectuer les AWS KMS actions suivantes :

- `kms:DescribeKey`
- `kms:ListAliases`

Ces actions vous permettent de récupérer et d'afficher les informations relatives AWS KMS keys à votre compte. Vous pouvez ensuite choisir l'une de ces clés pour chiffrer votre rapport.

Si vous envisagez de créer une nouvelle clé KMS pour le chiffrement de votre rapport, vous devez également être autorisé à effectuer cette `kms:CreateKey` action.

Amazon S3

Pour Amazon S3, vérifiez que vous êtes autorisé à effectuer les actions suivantes :

- `s3:CreateBucket`
- `s3:DeleteObject`

- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`
- `s3:PutObjectAcl`

Ces actions vous permettent de créer et de configurer le compartiment S3 dans lequel vous souhaitez qu'Amazon Inspector stocke votre rapport. Ils vous permettent également d'ajouter et de supprimer des objets dans le compartiment.

Si vous prévoyez d'utiliser la console Amazon Inspector pour exporter votre rapport, vérifiez également que vous êtes autorisé à effectuer les `s3:GetBucketLocation` actions `s3:ListAllMyBuckets` et. Ces actions vous permettent de récupérer et d'afficher des informations sur les compartiments S3 de votre compte. Vous pouvez ensuite choisir l'un de ces compartiments pour stocker le rapport.

Si vous n'êtes pas autorisé à effectuer une ou plusieurs des actions requises, demandez de l'aide à votre AWS administrateur avant de passer à l'étape suivante.

Étape 2 : Configuration d'un compartiment S3

Après avoir vérifié vos autorisations, vous êtes prêt à configurer le compartiment S3 dans lequel vous souhaitez stocker votre rapport de résultats. Il peut s'agir d'un compartiment existant pour votre propre compte ou d'un compartiment existant appartenant à un autre Compte AWS et auquel vous êtes autorisé à accéder. Si vous souhaitez stocker votre rapport dans un nouveau compartiment, créez-le avant de continuer.

Le compartiment S3 doit se trouver dans le même Région AWS emplacement que les données de résultats que vous souhaitez exporter. Par exemple, si vous utilisez Amazon Inspector dans la région USA Est (Virginie du Nord) et que vous souhaitez exporter les données de résultats pour cette région, le bucket doit également se trouver dans la région USA Est (Virginie du Nord).

En outre, la politique du compartiment doit autoriser Amazon Inspector à ajouter des objets au compartiment. Cette rubrique explique comment mettre à jour la politique du bucket et fournit un exemple de l'instruction à ajouter à la politique. Pour obtenir des informations détaillées sur l'ajout et la mise à jour des politiques de compartiment, consultez la section Utilisation des politiques de compartiment dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Si vous souhaitez stocker votre rapport dans un compartiment S3 appartenant à un autre compte, contactez le propriétaire du compartiment pour mettre à jour la politique du compartiment. Obtenez également l'URI du compartiment. Vous devrez saisir cette URI lorsque vous exporterez votre rapport.

Pour mettre à jour la politique relative aux compartiments

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le compartiment S3 dans lequel vous souhaitez stocker le rapport de résultats.
4. Choisissez l'onglet Permissions (Autorisations).
5. Dans la section Bucket policy (Politique de compartiment), sélectionnez Edit (Modifier).
6. Copiez l'exemple d'instruction suivant dans votre presse-papiers :

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "allow-inspector",
   "Effect": "Allow",
   "Principal": {
    "Service": "inspector2.amazonaws.com"
   },
   "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:AbortMultipartUpload"
   ],
   "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
   "Condition": {
    "StringEquals": {
     "aws:SourceAccount": "111122223333"
    },
    "ArnLike": {
     "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
    }
   }
  }
 ]
}
```

7. Dans l'éditeur de politique Bucket de la console Amazon S3, collez l'instruction précédente dans la politique pour l'ajouter à la politique.

   Lorsque vous ajoutez l'instruction, assurez-vous que la syntaxe est valide. Les politiques relatives aux compartiments utilisent le format JSON. Cela signifie que vous devez ajouter une virgule avant ou après la déclaration, selon l'endroit où vous l'ajoutez à la politique. Si vous ajoutez l'instruction en tant que dernière instruction, ajoutez une virgule après l'accolade de fermeture pour l'instruction précédente. Si vous l'ajoutez en tant que première instruction ou entre deux instructions existantes, ajoutez une virgule après l'accolade de fermeture de l'instruction.

8. Mettez à jour l'instruction avec les valeurs correctes pour votre environnement, où :

   - *DOC-EXAMPLE-BUCKET est le nom du bucket*.
   - *111122223333* est l'identifiant de votre compte. Compte AWS
   - La *région* est Région AWS celle dans laquelle vous utilisez Amazon Inspector et souhaitez autoriser Amazon Inspector à ajouter des rapports au compartiment. Par exemple, `us-east-1` pour la région de l'est des États-Unis (Virginie du Nord).

   > **Note**
   >
   > Si vous utilisez Amazon Inspector dans un environnement activé manuellementRégion AWS, ajoutez également le code de région approprié à la valeur du `Service` champ. Ce champ indique le principal du service Amazon Inspector.
   > Par exemple, si vous utilisez Amazon Inspector dans la région du Moyen-Orient (Bahreïn), dont le code de région est indiqué`me-south-1`, remplacez-le `inspector2.amazonaws.com` par `inspector2.me-south-1.amazonaws.com` dans le relevé.

   Notez que l'exemple d'instruction définit des conditions qui utilisent deux clés de condition globales IAM :

   - aws : SourceAccount — Cette condition permet à Amazon Inspector d'ajouter des rapports au bucket uniquement pour votre compte. Cela empêche Amazon Inspector d'ajouter des rapports au compartiment pour d'autres comptes. Plus précisément, la condition indique

quel compte peut utiliser le bucket pour les ressources et les actions spécifiées par la `aws:SourceArn` condition.

Pour stocker les rapports relatifs à des comptes supplémentaires dans le compartiment, ajoutez l'ID de compte de chaque compte supplémentaire à cette condition. Par exemple :

```
"aws:SourceAccount": [111122223333,444455556666,123456789012]
```

- aws : SourceArn — Cette condition restreint l'accès au compartiment en fonction de la source des objets ajoutés au compartiment. Cela empêche les autres Services AWS utilisateurs d'ajouter des objets au compartiment. Cela empêche également Amazon Inspector d'ajouter des objets au compartiment tout en effectuant d'autres actions pour votre compte. Plus précisément, cette condition permet à Amazon Inspector d'ajouter des objets au compartiment uniquement s'il s'agit de rapports de résultats, et uniquement si ces rapports sont créés par le compte et dans la région spécifiée dans la condition.

  Pour permettre à Amazon Inspector d'effectuer les actions spécifiées pour des comptes supplémentaires, ajoutez les Amazon Resource Names (ARN) pour chaque compte supplémentaire à cette condition. Par exemple :

```
"aws:SourceArn": [
    "arn:aws:inspector2:Region:111122223333:report/*",
    "arn:aws:inspector2:Region:444455556666:report/*",
    "arn:aws:inspector2:Region:123456789012:report/*"
]
```

  Les comptes spécifiés par les `aws:SourceArn` conditions `aws:SourceAccount` et doivent correspondre.

Ces deux conditions permettent d'éviter qu'Amazon Inspector ne soit utilisé comme un adjoint confus lors des transactions avec Amazon S3. Bien que cela ne soit pas recommandé, vous pouvez supprimer ces conditions de la politique relative aux compartiments.

9. Lorsque vous avez terminé de mettre à jour la politique de compartiment, choisissez Enregistrer les modifications.

Étape 3 : Configuration d'un AWS KMS key

Après avoir vérifié vos autorisations et configuré le compartiment S3, déterminez celui que AWS KMS key vous souhaitez qu'Amazon Inspector utilise pour chiffrer votre rapport de résultats. La clé doit être une clé KMS de chiffrement symétrique gérée par le client. En outre, la clé doit se trouver dans le même Région AWS compartiment S3 que vous avez configuré pour stocker le rapport.

La clé peut être une clé KMS existante de votre propre compte ou une clé KMS existante détenue par un autre compte. Si vous souhaitez utiliser une nouvelle clé KMS, créez-la avant de continuer. Si vous souhaitez utiliser une clé existante détenue par un autre compte, obtenez le nom de ressource Amazon (ARN) de la clé. Vous devrez saisir cet ARN lorsque vous exporterez votre rapport depuis Amazon Inspector. Pour plus d'informations sur la création et la révision des paramètres des clés KMS, consultez la section Gestion des clés dans le guide du AWS Key Management Service développeur.

Après avoir déterminé la clé KMS que vous souhaitez utiliser, autorisez Amazon Inspector à utiliser la clé. Dans le cas contraire, Amazon Inspector ne sera pas en mesure de chiffrer et d'exporter le rapport. Pour autoriser Amazon Inspector à utiliser la clé, mettez à jour la politique relative à la clé. Pour obtenir des informations détaillées sur les politiques clés et la gestion de l'accès aux clés KMS, consultez la section Politiques clés du guide du AWS Key Management Service développeur. AWS KMS

Pour mettre à jour la politique clé

> **Note**
>
> La procédure suivante permet de mettre à jour une clé existante afin de permettre à Amazon Inspector de l'utiliser. Si vous ne possédez pas encore de clé, consultez https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html les instructions pour en créer une.

1. Ouvrez la console AWS KMS à l'adresse https://console.aws.amazon.com/kms.
2. Pour changer de Région AWS, utilisez le sélecteur de région dans l'angle supérieur droit de la page.
3. Dans le volet de navigation, choisissez Clés gérées par le client.
4. Choisissez la clé KMS que vous souhaitez utiliser pour chiffrer le rapport. La clé doit être une clé de chiffrement symétrique (SYMMETRIC_DEFAULT).

5. Dans l'onglet Stratégie de clé choisissez Modifier. Si aucune politique clé n'est associée à un bouton Modifier, vous devez d'abord sélectionner Basculer vers l'affichage des politiques.
6. Copiez l'exemple d'instruction suivant dans votre presse-papiers :

```
{
    "Sid": "Allow Amazon Inspector to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
        }
    }
}
```

7. Dans l'éditeur de stratégie clé de la AWS KMS console, collez l'instruction précédente dans la politique clé pour l'ajouter à la stratégie.

   Lorsque vous ajoutez l'instruction, assurez-vous que la syntaxe est valide. Les politiques clés utilisent le format JSON. Cela signifie que vous devez ajouter une virgule avant ou après la déclaration, selon l'endroit où vous l'ajoutez à la politique. Si vous ajoutez l'instruction en tant que dernière instruction, ajoutez une virgule après l'accolade de fermeture pour l'instruction précédente. Si vous l'ajoutez en tant que première instruction ou entre deux instructions existantes, ajoutez une virgule après l'accolade de fermeture de l'instruction.
8. Mettez à jour l'instruction avec les valeurs correctes pour votre environnement, où :

   - *111122223333* est l'identifiant de votre compte. Compte AWS
   - La *région* est celle Région AWS dans laquelle vous souhaitez autoriser Amazon Inspector à chiffrer les rapports à l'aide de la clé. Par exemple, `us-east-1` pour la région de l'est des États-Unis (Virginie du Nord).

> **Note**
>
> Si vous utilisez Amazon Inspector dans un environnement activé manuellementRégion AWS, ajoutez également le code de région approprié à la valeur du `Service` champ. Par exemple, si vous utilisez Amazon Inspector dans la région du Moyen-Orient (Bahreïn), remplacez `inspector2.amazonaws.com` par`inspector2.me-south-1.amazonaws.com`.

À l'instar de l'exemple d'instruction pour la politique de compartiment présenté à l'étape précédente, les `Condition` champs de cet exemple utilisent deux clés de condition globales IAM :

- aws : SourceAccount — Cette condition permet à Amazon Inspector d'effectuer les actions spécifiées uniquement pour votre compte. Plus précisément, il détermine quel compte peut effectuer les actions spécifiées pour les ressources et les actions spécifiées par la `aws:SourceArn` condition.

  Pour permettre à Amazon Inspector d'effectuer les actions spécifiées pour des comptes supplémentaires, ajoutez l'ID de compte de chaque compte supplémentaire à cette condition. Par exemple :

  ```
  "aws:SourceAccount": [111122223333,444455556666,123456789012]
  ```

- aws : SourceArn — Cette condition empêche les autres d'Services AWSeffectuer les actions spécifiées. Cela empêche également Amazon Inspector d'utiliser la clé lorsqu'il effectue d'autres actions pour votre compte. En d'autres termes, cela permet à Amazon Inspector de chiffrer les objets S3 avec la clé uniquement s'ils sont des rapports de résultats, et uniquement si ces rapports sont créés par le compte et dans la région spécifiée dans la condition.

  Pour permettre à Amazon Inspector d'effectuer les actions spécifiées pour des comptes supplémentaires, ajoutez des ARN pour chaque compte supplémentaire à cette condition. Par exemple :

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:us-east-1:111122223333:report/*",
      "arn:aws:inspector2:us-east-1:444455556666:report/*",
  ```

```
    "arn:aws:inspector2:us-east-1:123456789012:report/*"
]
```

Les comptes spécifiés par les `aws:SourceArn` conditions `aws:SourceAccount` et doivent correspondre.

Ces conditions permettent d'éviter qu'Amazon Inspector ne soit utilisé comme un adjoint confus lors de transactions avecAWS KMS. Bien que cela ne soit pas recommandé, vous pouvez supprimer ces conditions de la déclaration.

9. Lorsque vous avez terminé de mettre à jour la politique clé, choisissez Enregistrer les modifications.

Étape 4 : Configuration et exportation d'un rapport de résultats

Après avoir vérifié vos autorisations et configuré les ressources pour chiffrer et stocker votre rapport de résultats, vous êtes prêt à configurer et à exporter le rapport.

Pour configurer et exporter un rapport de résultats

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sous Résultats, sélectionnez Tous les résultats.
3. (Facultatif) À l'aide de la barre de filtre située au-dessus du tableau des résultats, ajoutez des critères de filtre qui spécifient les résultats à inclure dans le rapport. Au fur et à mesure que vous ajoutez des critères, Amazon Inspector met à jour le tableau pour n'inclure que les résultats correspondant aux critères. Le tableau fournit un aperçu des données que votre rapport contiendra.

> **Note**
>
> Nous vous recommandons d'ajouter des critères de filtre. Si ce n'est pas le cas, le rapport inclura les données relatives à toutes vos découvertes actuelles Région AWS ayant le statut Actif. Si vous êtes l'administrateur Amazon Inspector d'une organisation, cela inclut les données de résultats pour tous les comptes membres de votre organisation.

> Si un rapport inclut des données pour l'ensemble ou plusieurs des résultats, la génération et l'exportation du rapport peuvent prendre du temps, et vous ne pouvez exporter qu'un seul rapport à la fois.

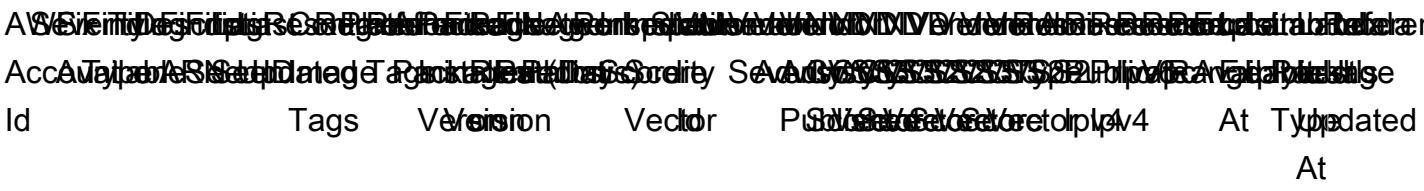
4. Choisissez Exporter les résultats.
5. Dans la section Paramètres d'exportation, pour Type de fichier d'exportation, spécifiez un format de fichier pour le rapport :

   - Pour créer un fichier de notation d' JavaScript objet (.json) contenant les données, choisissez JSON.

     Si vous choisissez l'option JSON, le rapport inclura tous les champs pour chaque résultat. Pour obtenir la liste des champs JSON possibles, consultez le type de données Finding dans la référence de l'API Amazon Inspector.

   - Pour créer un fichier de valeurs séparées par des virgules (.csv) contenant les données, choisissez CSV.

     Si vous choisissez l'option CSV, le rapport inclura uniquement un sous-ensemble de champs pour chaque résultat, soit environ 45 champs qui indiquent les principaux attributs d'un résultat. Les champs incluent : le type de recherche, le titre, la gravité, le statut, la description, le premier vu, le correctif disponible, l'identifiant du AWS compte, l'identifiant de la ressource, les balises de ressource et la correction. Ces champs s'ajoutent aux champs qui capturent les détails des scores et les URL de référence pour chaque résultat. Voici un exemple des en-têtes CSV d'un rapport de résultats :



6. Sous Emplacement d'exportation, pour l'URI S3, spécifiez le compartiment S3 dans lequel vous souhaitez stocker le rapport :

   - Pour stocker le rapport dans un compartiment appartenant à votre compte, choisissez Browse S3. Amazon Inspector affiche un tableau des compartiments S3 associés à votre compte. Sélectionnez la ligne correspondant au compartiment de votre choix, puis choisissez Choisir.

> **Tip**
>
> Pour également spécifier un préfixe de chemin Amazon S3 pour le rapport, ajoutez une barre oblique (/) et le préfixe à la valeur dans la zone URI S3. Amazon Inspector inclut ensuite le préfixe lorsqu'il ajoute le rapport au compartiment, et Amazon S3 génère le chemin spécifié par le préfixe.
> Par exemple, si vous souhaitez utiliser votre Compte AWS identifiant comme préfixe et que l'identifiant de votre compte est 111122223333, ajoutez-le **`/111122223333`** à la valeur dans la zone URI S3.
> Un préfixe est similaire à un chemin de répertoire dans un compartiment S3. Il vous permet de regrouper des objets similaires dans un compartiment, de la même manière que vous stockiez des fichiers similaires dans un dossier d'un système de fichiers.
> Pour plus d'informations, consultez la section Organisation des objets dans la console Amazon S3 à l'aide de dossiers dans le guide de l'utilisateur d'Amazon Simple Storage Service.

- Pour stocker le rapport dans un compartiment appartenant à un autre compte, entrez l'URI du compartiment, par exemple**`s3://DOC-EXAMPLE_BUCKET`**, où DOC-EXAMPLE_BUCKET est le nom du compartiment. Le propriétaire du bucket peut trouver ces informations pour vous dans les propriétés du bucket.

7. Pour la clé KMS, spécifiez AWS KMS key celle que vous souhaitez utiliser pour chiffrer le rapport :

   - Pour utiliser une clé de votre propre compte, choisissez-la dans la liste. La liste affiche les clés KMS de chiffrement symétriques gérées par le client pour votre compte.
   - Pour utiliser une clé détenue par un autre compte, entrez le nom de ressource Amazon (ARN) de la clé. Le propriétaire de la clé peut trouver ces informations pour vous dans les propriétés de la clé. Pour plus d'informations, consultez la section Recherche de l'ID et de l'ARN de la clé dans le Guide du AWS Key Management Service développeur.

8. Choisissez Export (Exporter).

Amazon Inspector génère le rapport de résultats, le chiffre avec la clé KMS que vous avez spécifiée et l'ajoute au compartiment S3 que vous avez spécifié. Selon le nombre de résultats que vous avez choisi d'inclure dans le rapport, ce processus peut prendre plusieurs minutes, voire plusieurs heures. Lorsque l'exportation est terminée, Amazon Inspector affiche un message indiquant que votre rapport

de résultats a été correctement exporté. Choisissez éventuellement Afficher le rapport dans le message pour accéder au rapport dans Amazon S3.

Notez que vous ne pouvez exporter qu'un seul rapport à la fois. Si une exportation est en cours, attendez qu'elle soit terminée avant d'essayer d'exporter un autre rapport.

Résoudre les erreurs d'exportation

Si une erreur se produit lorsque vous essayez d'exporter un rapport de résultats, Amazon Inspector affiche un message décrivant l'erreur. Vous pouvez utiliser les informations de cette rubrique comme guide pour identifier les causes possibles de l'erreur et les solutions.

Par exemple, vérifiez que le compartiment S3 se trouve dans le compartiment actuel Région AWS et que la politique du compartiment autorise Amazon Inspector à ajouter des objets au compartiment. Vérifiez également que le AWS KMS key est activé dans la région actuelle et assurez-vous que la politique en matière de clés autorise Amazon Inspector à utiliser la clé.

Après avoir corrigé l'erreur, réessayez d'exporter le rapport.

Impossible d'avoir plusieurs rapports d'erreur

Si vous tentez de créer un rapport mais qu'Amazon Inspector est déjà en train de générer un rapport, vous recevrez un message d'erreur indiquant Raison : Impossible d'avoir plusieurs rapports en cours d'élaboration. Cette erreur se produit car Amazon Inspector ne peut générer qu'un seul rapport à la fois pour un compte.

Pour résoudre l'erreur, vous pouvez attendre que l'autre rapport soit terminé ou l'annuler avant de demander un nouveau rapport.

Vous pouvez vérifier l'état d'un rapport à l'aide de l'GetFindingsReportStatusopération. Cette opération renvoie l'ID de rapport de tout rapport en cours de génération.

Si nécessaire, vous pouvez utiliser l'ID de rapport fourni par l'`GetFindingsReportStatus`opération pour annuler une exportation en cours à l'aide de l'CancelFindingsReportopération.

Création de réponses personnalisées aux résultats d'Amazon Inspector avec Amazon EventBridge

Amazon Inspector crée un événement EventBridge pour Amazon en cas de résultats récemment générés, de résultats récemment agrégés et de modifications de l'état des résultats. Tout ce qui n'est pas une modification `updatedAt` des `lastObservedAt` champs et publiera un nouvel événement. Cela signifie que de nouveaux événements relatifs à une recherche sont générés lorsque vous effectuez des actions telles que le redémarrage d'une ressource ou la modification des balises associées à une ressource. Toutefois, l'ID de recherche dans le `id` champ reste le même. Les événements sont générés sur la base du meilleur effort.

> **Note**
>
> Si votre compte est un administrateur délégué Amazon Inspector, EventBridge publie des événements sur votre compte en plus du compte membre dont ils proviennent.

Lorsque vous utilisez EventBridge des événements avec Amazon Inspector, vous pouvez automatiser des tâches pour vous aider à répondre aux problèmes de sécurité révélés par les résultats d'Amazon Inspector.

Amazon Inspector émet des événements vers le bus d'événements par défaut de la même région. Cela signifie que vous devez configurer des règles d'événements pour chaque région dans laquelle vous exécutez Amazon Inspector afin de voir les événements de cette région.

Pour recevoir des notifications concernant les résultats d'Amazon Inspector basés sur EventBridge des événements, vous devez créer une EventBridge règle et une cible pour Amazon Inspector. Cette règle permet d'EventBridgeenvoyer des notifications concernant les résultats générés par Amazon Inspector à la cible spécifiée dans la règle. Pour plus d'informations, consultez les EventBridgerègles Amazon dans le Guide de EventBridge l'utilisateur Amazon.

Schéma d'événement

Voici des exemples d'événement Amazon Inspector pour un événement pour une recherche EC2. Pour un exemple de schéma d'autres types de recherche et d'événements, voirEventBridge schéma.

```
{
    "version": "0",
```

```
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
```

```
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-image-
aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```

Création d'une EventBridge règle pour vous informer des résultats d'Amazon Inspector

Pour améliorer la visibilité des résultats d'Amazon Inspector, vous pouvez EventBridge configurer des alertes de recherche automatisées qui sont envoyées à un hub de messagerie. Cette rubrique explique comment envoyer des alertes `CRITICAL` et des résultats de `HIGH` gravité par e-mail, Slack ou Amazon Chime. Vous allez apprendre à configurer une rubrique Amazon Simple Notification Service, puis à associer cette rubrique à une règle d'EventBridgeévénement.

Étape 1. Configuration d'une rubrique et d'un point de terminaison Amazon SNS

Pour configurer des alertes automatiques, vous devez d'abord configurer une rubrique dans Amazon Simple Notification Service et ajouter un point de terminaison. Pour plus d'informations, consultez le guide SNS.

Cette procédure définit à l'endroit où vous voulez envoyer les données de résultats Amazon Inspector. La rubrique SNS peut être ajoutée à une règle d'EventBridgeévénement 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. Dans le volet de navigation, sélectionnez Rubriques, puis sélectionnez Créer une rubrique.
3. Dans la section Créer une rubrique, sélectionnez Standard. Saisissez ensuite un nom pour une rubrique, par exemple**`Inspector_to_Email`**. D'autres détails sont facultatifs.
4. Choisissez Créer la rubrique. Cela ouvre un nouveau panneau avec des détails pour votre nouveau sujet.
5. Dans la section Abonnements, sélectionnez Créer un abonnement.
6. a. Dans le menu Protocole sélectionnez E-mail.
   b. Dans le champ Endpoint, saisissez l'adresse e-mail à laquelle vous souhaitez recevoir des notifications.

> **Note**
>
> Il vous sera demandé de confirmer votre abonnement via votre client de messagerie après avoir créé l'abonnement.

c. Choisissez Create subscription (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. Dans le volet de navigation, sélectionnez Rubriques, puis sélectionnez Créer une rubrique.
3. Dans la section Créer une rubrique, sélectionnez Standard. Saisissez ensuite un nom pour une rubrique, par exemple**`Inspector_to_Slack`**. D'autres détails sont facultatifs. Choisissez Créer un sujet pour terminer la création du point de terminaison.

Configuration d'un AWS Chatbot client

1. Accédez à la console AWS Chatbot à l'adresse https://console.aws.amazon.com/chatbot/.
2. Dans le volet Clients configurés, sélectionnez Configurer un nouveau client.
3. Choisissez Slack, puis sélectionnez Configurer pour confirmer.

> **Note**
>
> Lorsque vous choisissez Slack, vous devez confirmer les autorisations d'accès AWS Chatbot à votre chaîne en sélectionnant Autoriser.

4. Sélectionnez Configurer un nouveau canal pour ouvrir le volet des détails de configuration.

   a. Saisissez un nom pour la chaîne.

   b. Pour un canal Slack, choisissez le canal que vous voulez utiliser.

c. Dans Slack, copiez l'identifiant de la chaîne privée en cliquant avec le bouton droit sur le nom de la chaîne et en sélectionnant Copier le lien.

d. Dans la AWS Chatbot fenêtreAWS Management Console, collez l'ID de la chaîne que vous avez copié depuis Slack dans le champ ID de la chaîne privée.

e. Dans Autorisations, choisissez de créer un rôle IAM à l'aide d'un modèle si vous ne possédez pas encore de rôle.

f. Pour les modèles de politiques, choisissez Autorisations de notification. Il s'agit du modèle de politique IAM pourAWS Chatbot. Cette politique 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. Pour les politiques de garde-corps de la chaîne, choisissez AmazonInspector 2. ReadOnlyAccess

h. 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).

Amazon 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 volet de navigation, puis sélectionnez Créer une rubrique.
3. Dans la section Créer une rubrique, sélectionnez Standard. Saisissez ensuite un nom pour une rubrique, par exemple**`Inspector_to_Chime`**. D'autres détails sont facultatifs. Choisissez Créer un sujet pour terminer.

Configuration d'un AWS Chatbot client

1. Accédez à la console AWS Chatbot à l'adresse https://console.aws.amazon.com/chatbot/.
2. Dans le panneau Clients configurés, sélectionnez Configurer un nouveau client.
3. Choisissez Chime, puis sélectionnez Configurer pour confirmer.
4. Dans le volet Détails de configuration, entrez le nom du canal.

5. Dans Amazon Chime, ouvrez la salle de conversation de votre choix.

   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. Dans la AWS Chatbot fenêtreAWS Management Console, collez l'URL que vous avez copiée dans le champ URL du Webhook.
7. Dans Autorisations, choisissez de créer un rôle IAM à l'aide d'un modèle si vous ne possédez pas encore de rôle.
8. Pour les modèles de politiques, choisissez Autorisations de notification. Il s'agit du modèle de politique IAM pourAWS 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 Amazon Chime.
10. Sélectionnez Configure (Configurer).

Étape 2. Création d'une EventBridge règle pour les résultats d'Amazon Inspector

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Sélectionnez Règles dans le volet de navigation, puis sélectionnez Créer une règle.
3. Saisissez un nom et une description facultative pour votre règle.
4. Sélectionnez Règle avec un modèle d'événements, puis Suivant.
5. Dans le volet Modèle d'événement, choisissez Modèles personnalisés (éditeur JSON).
6. Collez le JSON suivant dans l'éditeur.

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"],
  "detail": {
    "severity": ["HIGH", "CRITICAL"],
    "status": ["ACTIVE"]
  }
}
```

> **Note**
>
> Ce modèle envoie des notifications pour tout indice actif `CRITICAL` ou de `HIGH` gravité détecté par Amazon Inspector.

Sélectionnez Suivant lorsque vous avez fini de saisir le modèle d'événement.

7. Sur la page Sélectionner les cibles, choisissez Service AWS. Ensuite, pour Sélectionner le type de cible, choisissez la rubrique SNS.
8. Pour Rubrique, sélectionnez le nom de la rubrique SNS que vous avez créée à l'étape 1. Sélectionnez ensuite Next (Suivant).
9. Ajoutez des balises facultatives si nécessaire et choisissez Suivant.
10. Vérifiez votre règle, puis choisissez Créer une règle.

EventBridgepour les environnements multicomptes Amazon Inspector

Si vous êtes administrateur délégué d'Amazon Inspector, EventBridge les règles apparaissent sur votre compte en fonction des résultats applicables provenant de vos comptes de membre. Si vous configurez les notifications de résultats via EventBridge votre compte administrateur, comme indiqué dans la section précédente, vous recevrez des notifications concernant plusieurs comptes. En d'autres termes, vous serez informé des résultats et des événements générés par vos comptes de membre en plus de ceux générés par votre propre compte.

Vous pouvez utiliser les détails JSON `accountId` issus de la recherche pour identifier le compte membre à l'origine de la recherche Amazon Inspector.

Exporter des SBOM avec Amazon Inspector

Vous pouvez utiliser la console ou l'API Amazon Inspector pour générer une nomenclature logicielle (SBOM) pour vos ressources. Un SBOM est un inventaire imbriqué de tous les composants logiciels open source et tiers de votre base de code. Amazon Inspector fournit des SBOM pour les ressources individuelles de votre environnement. Les SBOM exportés depuis Amazon Inspector peuvent vous aider à obtenir une meilleure visibilité sur les informations relatives à votre offre logicielle, telles que les packages les plus utilisés et les vulnérabilités associées au sein de votre organisation.

Vous pouvez exporter des SBOM pour toutes les ressources prises en charge qui sont activement surveillées par Amazon Inspector. Vous pouvez consulter l'état de vos ressources enÉvaluation de la couverture de votre AWS environnement par Amazon Inspector.

> **Note**
>
> Amazon Inspector ne prend pas en charge l'exportation de SBOM pour les instances Windows EC2.

Formats Amazon Inspector

Amazon Inspector prend en charge l'exportation de SBOM aux formats compatibles avec CyclonedX 1.4 et SPDX 2.3. Amazon Inspector exporte les SBOM sous forme de `JSON` fichiers vers le compartiment Amazon S3 de votre choix.

> **Note**
>
> Les exportations au format SPDX depuis Amazon Inspector sont compatibles avec les systèmes utilisant SPDX 2.3, mais elles ne contiennent pas le champ Creative Commons Zero (CC0). En effet, l'inclusion de ce champ permettrait aux utilisateurs de redistribuer ou de modifier le matériel.

Exemple de format SBOM CycloneDX 1.4 d'Amazon Inspector

```
                    {
  "bomFormat": "CycloneDX",
```

```
  "specVersion": "1.4",
  "version": 1,
  "metadata": {
    "timestamp": "2023-06-02T01:17:46Z",
    "component": null,
    "properties": [
      {
        "name": "imageId",
        "value":
 "sha256:c8ee97f7052776ef223080741f61fcdf6a3a9107810ea9649f904aa4269fdac6"
      },
      {
        "name": "architecture",
        "value": "arm64"
      },
      {
        "name": "accountId",
        "value": "111122223333"
      },
      {
        "name": "resourceType",
        "value": "AWS_ECR_CONTAINER_IMAGE"
      }
    ]
  },
  "components": [
    {
      "type": "library",
      "name": "pip",
      "purl": "pkg:pypi/pip@22.0.4?path=usr/local/lib/python3.8/site-packages/
pip-22.0.4.dist-info/METADATA",
      "bom-ref": "98dc550d1e9a0b24161daaa0d535c699"
    },
    {
      "type": "application",
      "name": "libss2",
      "purl": "pkg:dpkg/libss2@1.44.5-1+deb10u3?
arch=ARM64&epoch=0&upstream=libss2-1.44.5-1+deb10u3.src.dpkg",
      "bom-ref": "2f4d199d4ef9e2ae639b4f8d04a813a2"
    },
    {
      "type": "application",
      "name": "liblz4-1",
```

```
      "purl": "pkg:dpkg/liblz4-1@1.8.3-1+deb10u1?
arch=ARM64&epoch=0&upstream=liblz4-1-1.8.3-1+deb10u1.src.dpkg",
      "bom-ref": "9a6be8907ead891b070e60f5a7b7aa9a"
    },
    {
      "type": "application",
      "name": "mawk",
      "purl": "pkg:dpkg/mawk@1.3.3-17+b3?
arch=ARM64&epoch=0&upstream=mawk-1.3.3-17+b3.src.dpkg",
      "bom-ref": "c2015852a729f97fde924e62a16f78a5"
    },
    {
      "type": "application",
      "name": "libgmp10",
      "purl": "pkg:dpkg/libgmp10@6.1.2+dfsg-4+deb10u1?
arch=ARM64&epoch=2&upstream=libgmp10-6.1.2+dfsg-4+deb10u1.src.dpkg",
      "bom-ref": "52907290f5beef00dff8da77901b1085"
    },
    {
      "type": "application",
      "name": "ncurses-bin",
      "purl": "pkg:dpkg/ncurses-bin@6.1+20181013-2+deb10u3?
arch=ARM64&epoch=0&upstream=ncurses-bin-6.1+20181013-2+deb10u3.src.dpkg",
      "bom-ref": "cd20cfb9ebeeadba3809764376f43bce"
    }
  ],
  "vulnerabilities": [
    {
      "id": "CVE-2022-40897",
      "affects": [
        {
          "ref": "a74a4862cc654a2520ec56da0c81cdb3"
        },
        {
          "ref": "0119eb286405d780dc437e7dbf2f9d9d"
        }
      ]
    }
  ]
}
```

Exemple de format SBOM SPDX 2.3 d'Amazon Inspector


```
{
 "name": "409870544328/EC2/i-022fba820db137c64/ami-074ea14c08effb2d8",
 "spdxVersion": "SPDX-2.3",
 "creationInfo": {
  "created": "2023-06-02T21:19:22Z",
  "creators": [
   "Organization: 409870544328",
   "Tool: Amazon Inspector SBOM Generator"
  ]
 },
 "documentNamespace": "EC2://i-022fba820db137c64/AMAZON_LINUX_2/null/x86_64",
 "comment": "",
 "packages": [{
   "name": "elfutils-libelf",
   "versionInfo": "0.176-2.amzn2",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/elfutils-libelf@0.176-2.amzn2?
arch=X86_64&epoch=0&upstream=elfutils-libelf-0.176-2.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-elfutils-libelf-ddf56a513c0e76ab2ae3246d9a91c463"
  },
  {
   "name": "libcurl",
   "versionInfo": "7.79.1-1.amzn2.0.1",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/libcurl@7.79.1-1.amzn2.0.1?
arch=X86_64&epoch=0&upstream=libcurl-7.79.1-1.amzn2.0.1.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
```

```
     "referenceType": "vulnerability",
     "referenceLocator": "CVE-2022-32205"
    }
   ],
   "SPDXID": "SPDXRef-Package-rpm-libcurl-710fb33829bc5106559bcd380cddb7d5"
  },
  {
   "name": "hunspell-en-US",
   "versionInfo": "0.20121024-6.amzn2.0.1",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/hunspell-en-US@0.20121024-6.amzn2.0.1?
arch=NOARCH&epoch=0&upstream=hunspell-en-US-0.20121024-6.amzn2.0.1.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-hunspell-en-US-de19ae0883973d6cea5e7e079d544fe5"
  },
  {
   "name": "grub2-tools-minimal",
   "versionInfo": "2.06-2.amzn2.0.6",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/grub2-tools-minimal@2.06-2.amzn2.0.6?
arch=X86_64&epoch=1&upstream=grub2-tools-minimal-2.06-2.amzn2.0.6.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
     "referenceType": "vulnerability",
     "referenceLocator": "CVE-2021-3981"
    }
   ],
   "SPDXID": "SPDXRef-Package-rpm-grub2-tools-minimal-c56b7ea76e5a28ab8f232ef6d7564636"
  },
  {
   "name": "unixODBC-devel",
   "versionInfo": "2.3.1-14.amzn2",
   "downloadLocation": "NOASSERTION",
```

```
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/unixODBC-devel@2.3.1-14.amzn2?
arch=X86_64&epoch=0&upstream=unixODBC-devel-2.3.1-14.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-unixODBC-devel-1bb35add92978df021a13fc9f81237d2"
  }
 ],
 "relationships": [{
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-elfutils-libelf-
ddf56a513c0e76ab2ae3246d9a91c463",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-yajl-8476ce2db98b28cfab2b4484f84f1903",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-unixODBC-
devel-1bb35add92978df021a13fc9f81237d2",
   "relationshipType": "DESCRIBES"
  }
 ],
 "SPDXID": "SPDXRef-DOCUMENT"
}
```


Filtres pour SBOM

Lorsque vous exportez des SBOM, vous pouvez inclure des filtres pour créer des rapports pour des sous-ensembles de ressources spécifiques. Si vous ne fournissez pas de filtre, les SBOM pour toutes les ressources actives prises en charge sont exportées. Et si vous êtes un administrateur délégué, cela inclut également des ressources pour tous les membres. Les filtres suivants sont disponibles :

- AccountID — Ce filtre peut être utilisé pour exporter les SBOM pour toutes les ressources associées à un ID de compte spécifique.

- Tag d'instance EC2 — Ce filtre peut être utilisé pour exporter des SBOM pour les instances EC2 avec des balises spécifiques.
- Nom de la fonction — Ce filtre peut être utilisé pour exporter des SBOM pour des fonctions Lambda spécifiques.
- Balise d'image — Ce filtre peut être utilisé pour exporter des SBOM pour des images de conteneur avec des balises spécifiques.
- Balise de fonction Lambda — Ce filtre peut être utilisé pour exporter des SBOM pour les fonctions Lambda avec des balises spécifiques.
- Type de ressource — Ce filtre peut être utilisé pour filtrer le type de ressource : EC2/ECR/Lambda.
- ID de ressource — Ce filtre peut être utilisé pour exporter une SBOM pour une ressource spécifique.
- Nom du référentiel : ce filtre peut être utilisé pour générer des SBOM pour les images de conteneur dans des référentiels spécifiques.

Configurer et exporter des SBOM

Pour exporter des SBOM, vous devez d'abord configurer un compartiment Amazon S3 et une AWS KMS clé qu'Amazon Inspector est autorisé à utiliser. Vous pouvez utiliser des filtres pour exporter des SBOM pour des sous-ensembles spécifiques de vos ressources. Pour exporter des SBOM pour plusieurs comptes au AWS sein d'une organisation, suivez ces étapes lorsque vous êtes connecté en tant qu'administrateur délégué Amazon Inspector.

Prérequis

- Ressources prises en charge qui sont surveillées activement par Amazon Inspector.
- Un compartiment Amazon S3 configuré avec une politique qui permet à Amazon Inspector d'y ajouter un objet. Pour plus d'informations sur la configuration de la politique, voir Configurer les autorisations d'exportation.
- Une AWS KMS clé configurée avec une politique qui permet à Amazon Inspector de l'utiliser pour chiffrer vos rapports. Pour plus d'informations sur la configuration de la politique, voir Configurer une AWS KMS clé pour l'exportation.

> **Note**
>
> Si vous avez déjà configuré un compartiment Amazon S3 et une AWS KMS clé pour l'exportation des résultats, vous pouvez utiliser le même compartiment et la même clé pour l'exportation SBOM.

Choisissez votre méthode d'accès préférée pour exporter un SBOM.

Console

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région contenant les ressources pour lesquelles vous souhaitez exporter le SBOM.
3. Dans le volet de navigation, choisissez Exporter les SBOM.
4. (Facultatif) Sur la page Exporter des SBOM, utilisez le menu Ajouter un filtre pour sélectionner un sous-ensemble de ressources pour lequel créer des rapports. Si aucun filtre n'est fourni, Amazon Inspector exportera des rapports pour toutes les ressources actives. Si vous êtes un administrateur délégué, cela inclura toutes les ressources actives de votre organisation.
5. Sous Réglage d'exportation, sélectionnez le format que vous souhaitez pour le SBOM.
6. Entrez un URI Amazon S3 ou choisissez Parcourir Amazon S3 pour sélectionner un emplacement Amazon S3 où stocker le SBOM.
7. Entrez une AWS KMSclé configurée pour qu'Amazon Inspector puisse utiliser pour chiffrer vos rapports.

API

- Pour exporter des SBOM pour vos ressources par programmation, utilisez le CreateSbomExportfonctionnement de l'API Amazon Inspector.

  Dans votre demande, utilisez le `reportFormat` paramètre pour spécifier le format de sortie SBOM, choisissez `CYCLONEDX_1_4` ou. `SPDX_2_3` Le `s3Destination` paramètre est obligatoire et vous devez spécifier un compartiment S3 configuré avec une politique permettant à Amazon Inspector d'y écrire. Utilisez éventuellement

`resourceFilterCriteria` des paramètres pour limiter la portée du rapport à des ressources spécifiques.

AWS CLI

- Pour exporter des SBOM pour vos ressources à l'aide AWS Command Line Interface de la commande suivante :

  ```
  aws inspector2 create-sbom-export --report-format
  FORMAT --s3-destination bucketName=DOC-EXAMPLE-
  BUCKET1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
  ```

  Dans votre demande, remplacez *FORMAT* par le format de votre choix, `CYCLONEDX_1_4` ou`SPDX_2_3`. Remplacez ensuite le nom *user input placeholders*de la destination s3 par le nom du compartiment S3 vers lequel exporter, le préfixe à utiliser pour la sortie dans S3 et l'ARN de la clé KMS que vous utilisez pour chiffrer les rapports.

Recherche dans la base de données de vulnérabilités Amazon Inspector

Vous pouvez rechercher des vulnérabilités et des expositions (CVE) dans la base de données des vulnérabilités d'Amazon Inspector. Amazon Inspector utilise les informations de la base de données de vulnérabilités pour produire des informations relatives à un identifiant CVE. Vous pouvez accéder à ces informations sur la page de détails du CVE.

Cette rubrique explique comment effectuer une recherche dans la base de données des vulnérabilités d'Amazon Inspector à l'aide d'un identifiant CVE et comment interpréter la page de détails du CVE. Pour plus d'informations sur les résultats, voirAmazon Inspector trouve des informations.

> **Note**
>
> Amazon Inspector suit les autres vulnérabilités logicielles présentes dans la base de données et produit des résultats pour les détecter. Toutefois, Amazon Inspector prend uniquement en charge les CVE dont les plateformes sont répertoriées dans la section Plateformes de détection de la page détaillée des CVE. Actuellement, la recherche CVE n'est pas prise en chargeMicrosoft Windows.

Recherche dans la base de données des vulnérabilités

Cette section explique comment effectuer une recherche dans la base de données des vulnérabilités dans la console et à l'aide de l'API Amazon Inspector.

> **Note**
>
> Vous devez activer Amazon Inspector dans votre compte actuel Région AWS avant de pouvoir effectuer une recherche dans la base de données des vulnérabilités.

Console

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/

2. Dans le volet de navigation, choisissez Vulnerability database search.
3. Dans la barre de recherche, entrez un identifiant CVE, puis choisissez Rechercher.

API

Exécutez l'SearchVulnerabilitiesAPI Amazon Inspector et fournissez un identifiant CVE unique `filterCriteria` au format suivant :`CVE-<year>-<ID>`.

Comprendre les détails de la CVE

Cette section explique comment interpréter la page de détails du CVE.

Détails du CVE

La section relative aux détails du CVE contient les informations suivantes :

- Description et identifiant du CVE
- Gravité du CVE
- Scores du système commun de notation des vulnérabilités (CVSS) et du système de notation prédictive des exploits (EPSS)
- Plateformes de détection

> **Note**
>
> Si ce champ est vide, Amazon Inspector ne prend pas en charge la détection de votre identifiant CVE.

- Énumération des faiblesses courantes (CWE)
- Dates de création et de mise à jour du fournisseur

Renseignements sur les vulnérabilités

La section des informations sur les vulnérabilités fournit des données de renseignement sur les menaces, telles que les cibles des exploits et la date du dernier exploit public connu.

Il fournit également des données de l'Agence de cybersécurité et de sécurité des infrastructures (CISA), notamment les mesures correctives, la date à laquelle le CVE a été ajouté au catalogue des

vulnérabilités connues exploitées et la date à laquelle la CISA attend des agences fédérales qu'elles corrigent le CVE.

Références

La section des références fournit des liens vers des ressources pour plus d'informations sur le CVE.

Schéma EventBridge d'événements Amazon pour les événements Amazon Inspector

Pour faciliter l'intégration avec d'autres applications, services et systèmes, tels que les systèmes de surveillance ou de gestion des événements, Amazon Inspector publie automatiquement les résultats sur Amazon EventBridge sous forme d'événements. EventBridgeest un service de bus d'événements sans serveur qui fournit un flux de données en temps réel provenant d'applications et d'autres sources Services AWS à des cibles telles que AWS Lambda les fonctions, les rubriques Amazon Simple Notification Service et les flux Amazon Kinesis Data Streams. Pour en savoir plus sur les EventBridge événements EventBridge et les événements, consultez le guide de EventBridge l'utilisateur Amazon.

Amazon Inspector publie des événements concernant les résultats, les modifications de la couverture des ressources et les analyses initiales des ressources individuelles. Chaque événement est un objet JSON conforme au EventBridge schéma des AWS événements. Les données étant structurées sous la forme d'un EventBridge événement, vous pouvez plus facilement surveiller, traiter et agir en fonction des résultats et des événements Amazon Inspector pris en charge en utilisant d'autres applications, services et outils.

Rubriques

Schéma EventBridge de base Amazon pour Amazon Inspector

Voici un exemple du schéma de base d'un EventBridge événement pour Amazon Inspector. Les détails de l'événement varient en fonction du type d'événement.

```
{
    "version": "0",
    "id": "Event ID",
    "detail-type": "Inspector2 *event type*",
    "source": "aws.inspector2",
    "account": "Compte AWS ID (string)",
```

```
    "time": "event timestamp (string)",
    "region": "Région AWS (string)",
    "resources": [
        *IDs or ARNs of the resources involved in the event*
    ],
    "detail": {
        *Details of an Amazon Inspector event type*
    }
}
```

Exemple de schéma d'événement de recherche par Amazon Inspector

Vous trouverez ci-dessous des exemples du schéma d'un EventBridge événement pour les résultats d'Amazon Inspector. Des événements de recherche sont créés lorsqu'Amazon Inspector identifie une vulnérabilité logicielle ou un problème réseau dans l'une de vos ressources. Pour un guide sur la création de notifications en réponse à ce type d'événement, consultezCréation de réponses personnalisées aux résultats d'Amazon Inspector avec Amazon EventBridge.

Les champs suivants identifient un événement de recherche :

- Le champ `detail-type` est défini sur `Inspector2 Finding`.
- L'`detail`objet décrit le résultat.

Sélectionnez l'une des options pour voir les schémas d'événements de recherche pour différentes ressources et différents types de recherche.

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
```

```
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
```

```
                "remediation": "apt update && apt install --only-upgrade linux-
image-aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```


Amazon EC2 network reachability finding


```
{
```

```
    "version": "0",
    "id": "d0384f63-1621-1b75-d014-a5e45628ef3e",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T09:17:57Z",
    "region": "us-east-1",
    "resources": ["i-0a96278c2206a8e4b"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "On the instance i-0a96278c2206a8e4b, the port range
 22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI
 eni-0976efe678170408f.",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "lastObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-72069c09",
                    "componentType": "AWS::EC2::InternetGateway"
                }, {
                    "componentId": "acl-91d74eec",
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0aaed0af450bd0165",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-0976efe678170408f",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-0a96278c2206a8e4b",
                    "componentType": "AWS::EC2::Instance"
                }]
            },
            "openPortRange": {
                "begin": 22,
                "end": 22
            },
            "protocol": "TCP"
        },
        "remediation": {
            "recommendation": {
```

```
                "text": "You can restrict access to your instance by modifying the
 Security Groups or ACLs in the network path."
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b5eea76982371e91",
                    "ipV4Addresses": ["3.89.90.19", "172.31.93.57"],
                    "ipV6Addresses": [],
                    "keyName": "example-inspector-test",
                    "launchedAt": "Jan 19, 2023, 7:25:02 PM",
                    "platform": "AMAZON_LINUX_2",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0a96278c2206a8e4b",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Jan 20, 2023, 9:17:57 AM"
    }
}
```

Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5b52952e-26df-3a51-6d14-4dbe737e58ec",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
```

```
    "time": "2023-01-19T21:59:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "libcurl would reuse a previously created connection even
 when a TLS or SSHrelated option had been changed that should have prohibited
 reuse.libcurl keeps previously used connections in a connection pool for
 subsequenttransfers to reuse if one of them matches the setup. However, several TLS
 andSSH settings were left out from the configuration match checks, making themmatch
 too easily.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 5,
                    "scoringVector": "AV:N/AC:L/Au:N/C:N/I:P/A:N",
                    "source": "NVD",
                    "version": "2.0"
                },
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                    "source": "NVD",
                    "version": "3.1"
```

```
                }
            ],
            "referenceUrls": [
                "https://hackerone.com/reports/1555796",
                "https://security.gentoo.org/glsa/202212-01",
                "https://lists.debian.org/debian-lts-announce/2022/08/
msg00017.html",
                "https://www.debian.org/security/2022/dsa-5197"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-27782",
            "vendorCreatedAt": "Jun 2, 2022, 2:15:00 PM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Jan 5, 2023, 5:51:00 PM",
            "vulnerabilityId": "CVE-2022-27782",
            "vulnerablePackages": [
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "libcurl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update libcurl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                },
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "curl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update curl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                }
            ]
        },
        "remediation": {
```

```
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "amd64",
                        "imageHash":
 "sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                        "imageTags": [
                            "o3"
                        ],
                        "platform": "ORACLE_LINUX_8",
                        "pushedAt": "Jan 19, 2023, 7:38:39 PM",
                        "registry": "111122223333",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                "partition": "aws",
                "region": "us-east-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-27782 - libcurl, curl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 9:59:00 PM"
    }
}
```

Lambda package vulnerability finding

```
{
    "version": "0",
    "id": "040bb590-3a12-353f-ecb1-05e54b0fbea7",
    "detail-type": "Inspector2 Finding",
```

```
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T19:20:25Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:lambda:us-east-1:111122223333:function:ExampleFunction:$LATEST"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "Those using Woodstox to parse XML data may be vulnerable to
 Denial of Service attacks (DOS) if DTD support is enabled. If the parser is running
 on user supplied input, an attacker may supply content that causes the parser to
 crash by stackoverflow. This effect may support a denial of service attack.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47434"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-40152",
```

```
            "vendorCreatedAt": "Sep 16, 2022, 10:15:00 AM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Nov 25, 2022, 11:15:00 AM",
            "vulnerabilityId": "CVE-2022-40152",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "lib/woodstox-core-6.2.7.jar",
                    "fixedInVersion": "6.4.0",
                    "name": "com.fasterxml.woodstox:woodstox-core",
                    "packageManager": "JAR",
                    "remediation": "Update woodstox-core to 6.4.0",
                    "version": "6.2.7"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "+EwrOrht2um4fdVCD73gj
+O7HJIAUvUxi8AD0eKHSkc=",
                        "executionRoleArn": "arn:aws:iam::111122223333:role/
ExampleFunction-ExecutionRole",
                        "functionName": "Example-function",
                        "lastModifiedAt": "Nov 7, 2022, 8:29:27 PM",
                        "packageType": "ZIP",
                        "runtime": "JAVA_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:us-
east-1:111122223333:function:ExampleFunction:$LATEST",
                "partition": "aws",
                "region": "us-east-1",
                "tags": {
```

```
                    "TargetAlias": "DeploymentStack",
                    "SoftwareType": "Infrastructure"
                },
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-40152 - com.fasterxml.woodstox:woodstox-core",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 7:20:25 PM"
    }
}
```

Lambda code vulnerability finding

```
{
   "version":"0",
   "id":"9df01cb1-df24-bc46-5650-085a4087e7aa",
   "detail-type":"Inspector2 Finding",
   "source":"aws.inspector2",
   "account":"111122223333",
   "time":"2023-12-07T22:14:45Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:lambda:us-east-1:111122223333:function:code-finding:$LATEST"
   ],
   "detail":{
      "awsAccountId":"111122223333",
      "codeVulnerabilityDetails":{
         "detectorId":"python/lambda-override-reserved@v1.0",
         "detectorName":"Override of reserved variable names in a Lambda function",
         "detectorTags":[
            "availability",
            "aws-python-sdk",
            "aws-lambda",
            "data-integrity",
            "maintainability",
            "security",
            "security-context",
            "python"
```

```
         ],
         "filePath":{
            "endLine":6,
            "fileName":"lambda_function.py",
            "filePath":"lambda_function.py",
            "startLine":6
         },
         "ruleId":"Rule-434311"
      },
      "description":"Overriding environment variables that are reserved by AWS
 Lambda might lead to unexpected behavior or failure of the Lambda function.",
      "findingArn":"arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
      "firstObservedAt":"Aug 8, 2023, 7:33:58 PM",
      "lastObservedAt":"Dec 7, 2023, 10:14:45 PM",
      "remediation":{
         "recommendation":{
            "text":"Your code attempts to override an environment variable that is
 reserved by the Lambda runtime environment. This can lead to unexpected behavior
 and might break the execution of your Lambda function.\n\n[Learn more](https://
docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-
envvars-runtime)"
         }
      },
      "resources":[
         {
            "details":{
               "awsLambdaFunction":{
                  "architectures":[
                     "X86_64"
                  ],
                  "codeSha256":"2mtfH+CgubesG6NYpb2zEqBja5WN6FfbH4AAYDuF8RE=",
                  "executionRoleArn":"arn:aws:iam::193043430472:role/service-role/
code-finding-role-7jgg3wan",
                  "functionName":"code-finding",
                  "lastModifiedAt":"Dec 7, 2023, 10:12:48 PM",
                  "packageType":"ZIP",
                  "runtime":"PYTHON_3_7",
                  "version":"$LATEST"
               }
            },
            "id":"arn:aws:lambda:us-east-1:193043430472:function:code-finding:
$LATEST",
            "partition":"aws",
            "region":"us-east-1",
```

```
            "type":"AWS_LAMBDA_FUNCTION"
         }
      ],
      "severity":"HIGH",
      "status":"ACTIVE",
      "title":"Overriding environment variables that are reserved by AWS Lambda
 might lead to unexpected behavior.",
      "type":"CODE_VULNERABILITY",
      "updatedAt":"Dec 7, 2023, 10:14:45 PM"
   }
}
```


> **Note**
>
> La valeur de détail renvoie les détails JSON d'une seule découverte sous forme d'objet. Il ne renvoie pas la syntaxe complète de la réponse aux résultats, qui prend en charge plusieurs résultats au sein d'un tableau.

Exemple de schéma d'événement complet du scan initial d'Amazon Inspector

Voici un exemple de schéma d' EventBridge événement pour un événement Amazon Inspector destiné à effectuer une analyse initiale. Cet événement est créé lorsque Amazon Inspector effectue une analyse initiale de l'une de vos ressources.

Les champs suivants identifient un événement de fin de numérisation initial :

- Le champ `detail-type` est défini sur `Inspector2 Scan`.
- L'`detail`objet contient un `finding-severity-counts` objet qui détaille le nombre de résultats dans les catégories de gravité applicables, telles que `CRITICAL`HIGH, et`MEDIUM`.

Sélectionnez l'une des options pour voir les différents schémas d'événements d'analyse initiale par type de ressource.

Amazon EC2 instance initial scan


```
{
    "version": "0",
    "id": "28a46762-6ac8-6cc4-4f55-bc9ab99af928",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:52:35Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "instance-id": "i-087d63509b8c97098",
        "version": "1.0"
    }
}
```


Amazon ECR image initial scan


```
{
    "version": "0",
    "id": "fdaa751a-984c-a709-44f9-9a9da9cd3606",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T23:15:18Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2"
    ],
    "detail": {
```

```
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "repository-name": "arn:aws:ecr:us-east-1:111122223333:repository/
inspector2",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "image-digest":
 "sha256:965fbcae990b0467ed5657caceaec165018ef44a4d2d46c7cdea80a9dff0d1ea",
        "image-tags": [
            "ubuntu22"
        ],
        "version": "1.0"
    }
}
```

Lambda function initial scan

```
{
  "version": "0",
  "id": "4f290a7c-361b-c442-03c8-a629f6f20d6c",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-02-23T18:06:03Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:lambda:us-west-2:111122223333:function:lambda-example:$LATEST"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "version": "1.0"
```

```
  }
}
```

Exemple de schéma d'événement de couverture Amazon Inspector

Voici un exemple de schéma d'événement pour un EventBridge événement Amazon Inspector à des fins de couverture. Cet événement est créé lorsque la couverture de numérisation d'une ressource par Amazon Inspector est modifiée. Les champs suivants identifient un événement de couverture :

- Le champ `detail-type` est défini sur `Inspector2 Coverage`.
- L'`detail`objet contient un `scanStatus` objet qui indique le nouvel état de numérisation de la ressource.

```
{
    "version": "0",
    "id": "000adda5-0fbf-913e-bc0e-10f0376412aa",
    "detail-type": "Inspector2 Coverage",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:51:39Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scanStatus": {
            "reason": "UNMANAGED_EC2_INSTANCE",
            "statusCodeValue": "INACTIVE"
        },
        "scanType": "PACKAGE",
        "eventTimestamp": "2023-01-20T22:51:35.665501Z",
        "version": "1.0"
    }
}
```

Intégration des scans Amazon Inspector dans votre pipeline CI/CD

Vous pouvez intégrer les scans d'images de conteneurs Amazon Inspector directement dans votre pipeline CI/CD pour détecter les vulnérabilités logicielles et fournir des rapports à la fin de votre build. Les rapports de vulnérabilité générés par Amazon Inspector vous permettent d'étudier et de corriger les risques avant le déploiement.

L'intégration Amazon Inspector CI/CD utilise une combinaison du générateur Amazon Inspector SBOM et de l'API Amazon Inspector Scan pour produire des rapports de vulnérabilité pour les images de vos conteneurs. Le générateur Amazon Inspector SBOM crée une nomenclature logicielle (SBOM) à partir d'une image de conteneur fournie, puis l'API Amazon Inspector Scan analyse cette nomenclature et crée un rapport contenant des informations détaillées sur les vulnérabilités détectées.

Vous pouvez réaliser une intégration CI/CD avec Amazon Inspector grâce aux plug-ins Amazon Inspector spécialement conçus pour les solutions CI/CD individuelles et disponibles sur leur marché, ou vous pouvez créer votre propre intégration de numérisation personnalisée.

Rubriques

Intégration du plugin

Amazon Inspector fournit des plug-ins pour les solutions CI/CD prises en charge. Vous pouvez installer ces plugins depuis leurs sites de vente respectifs, puis les utiliser pour ajouter Amazon Inspector Scans en tant qu'étape de création dans votre pipeline. L'étape de création du plugin

exécute le générateur Amazon Inspector SBOM sur l'image que vous fournissez, puis exécute l'API Amazon Inspector Scan sur le SBOM généré.

Voici un aperçu du fonctionnement d'une intégration Amazon Inspector CI/CD par le biais de plugins :

1. Vous configurez un Compte AWS pour autoriser l'accès à l'API Amazon Inspector Scan. Pour obtenir des instructions, veuillez consulter Configuration d'un AWS compte pour utiliser l'intégration Amazon Inspector CI/CD.
2. Vous installez le plugin Amazon Inspector depuis le Marketplace.
3. Vous installez et configurez le binaire Amazon Inspector SBOM Generator. Pour obtenir des instructions, veuillez consulter Générateur de SBOM Amazon Inspector.
4. Vous ajoutez Amazon Inspector Scans en tant qu'étape de création dans votre pipeline CI/CD et vous configurez le scan.
5. Lorsque vous exécutez une compilation, le plugin prend l'image de votre conteneur en entrée, puis exécute le générateur de SBOM Amazon Inspector sur l'image pour générer une SBOM CycloneDX compatible.
6. À partir de là, le plugin envoie le SBOM généré à un point de terminaison de l'API Amazon Inspector Scan qui évalue les vulnérabilités de chaque composant SBOM.
7. La réponse de l'API Amazon Inspector Scan est transformée en rapport de vulnérabilité aux formats CSV, SBOM, JSON et HTML. Le rapport contient des informations détaillées sur les vulnérabilités détectées par Amazon Inspector.

Solutions CI/CD prises en charge

Amazon Inspector prend actuellement en charge les solutions CI/CD suivantes. Pour obtenir des instructions complètes sur la configuration de l'intégration CI/CD à l'aide d'un plugin, sélectionnez le plugin correspondant à votre solution CI/CD :

- Plug-in Jenkins
- TeamCity plugin

Intégration personnalisée

Si Amazon Inspector ne fournit pas de plug-ins pour votre solution CI/CD, vous pouvez créer votre propre intégration CI/CD personnalisée en combinant le générateur Amazon Inspector SBOM et l'API

Amazon Inspector Scan. Vous pouvez également utiliser une intégration personnalisée pour affiner les scans à l'aide des options disponibles via Amazon Inspector SBOM Generator.

Voici un aperçu du fonctionnement d'une intégration personnalisée avec Amazon Inspector CI/CD :

1. Vous configurez un Compte AWS pour autoriser l'accès à l'API Amazon Inspector Scan. Pour obtenir des instructions, veuillez consulter Configuration d'un AWS compte pour utiliser l'intégration Amazon Inspector CI/CD.
2. Vous installez et configurez le binaire Amazon Inspector SBOM Generator. Pour obtenir des instructions, veuillez consulter Générateur de SBOM Amazon Inspector.
3. Vous utilisez le générateur SBOM d'Amazon Inspector pour générer un SBOM CycloneDX compatible pour votre image de conteneur.
4. Vous utilisez l'API Amazon Inspector Scan sur le SBOM généré pour générer un rapport de vulnérabilité.

Pour obtenir des instructions sur la configuration d'une intégration personnalisée, consultezCréation de votre propre intégration de pipeline CI/CD personnalisée avec Amazon Inspector Scan.

Configuration d'un AWS compte pour utiliser l'intégration Amazon Inspector CI/CD

Vous devez vous inscrire pour Compte AWS utiliser l'intégration Amazon Inspector CI/CD. Ils Compte AWS doivent avoir un rôle IAM qui accorde à votre pipeline l'accès à l'API Amazon Inspector Scan.

Effectuez les tâches décrites dans les rubriques suivantes pour vous inscrire à un Compte AWS, créer un utilisateur administrateur et configurer un rôle IAM pour l'intégration CI/CD.

> **Note**
>
> Si vous vous êtes déjà inscrit à un Compte AWS, vous pouvez passer àConfiguration d'un rôle IAM pour l'intégration CI/CD.

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur administratif

- Configuration d'un rôle IAM pour l'intégration CI/CD

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur root a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur administratif, et à uniquement utiliser l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur Mon compte.

Création d'un utilisateur administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur root, consultez Connexion en tant qu'utilisateur root dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur administratif.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Configuration d'un rôle IAM pour l'intégration CI/CD

Pour intégrer le scan Amazon Inspector dans votre pipeline CI/CD, vous devez créer une politique IAM qui autorise l'accès à l'API Amazon Inspector Scan qui scanne la nomenclature logicielle (SBOM). Vous pouvez ensuite associer cette politique à un rôle IAM que votre compte peut assumer pour exécuter l'API Amazon Inspector Scan.

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, sélectionnez Policies, puis Create Policy.
3. Dans l'éditeur de politiques, sélectionnez JSON et collez l'instruction suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "inspector-scan:ScanSbom",
            "Resource": "*"
        }
    ]
}
```

4. Choisissez Suivant.
5. Donnez un nom à la politique, par exemple`InspectorCICDscan-policy`, et ajoutez une description facultative, puis choisissez Create Policy. Cette politique sera attachée au rôle que vous allez créer au cours des prochaines étapes.
6. Dans le volet de navigation de la console IAM, sélectionnez Rôles, puis sélectionnez Créer un nouveau rôle.
7. Pour Type d'entité de confiance, choisissez Politique de confiance personnalisée et collez la politique suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{ACCOUNT_ID}:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

8. Choisissez Suivant.

9. Dans Ajouter des autorisations, recherchez et sélectionnez la politique que vous avez créée précédemment, puis choisissez Suivant.
10. Donnez un nom au rôle, par exemple`InspectorCICDscan-role`, et ajoutez une description facultative, puis choisissez`Create Role`.

Générateur de SBOM Amazon Inspector

Le générateur Amazon Inspector SBOM (Sbomgen) est un outil binaire qui produit une nomenclature logicielle (SBOM) pour une image de conteneur. Un SBOM est un inventaire collecté des logiciels installés sur un système.

Sbomgenfonctionne en recherchant les fichiers connus pour contenir des informations sur les packages installés. Si l'un de ces fichiers est trouvé, l'outil extrait les noms de package, les versions et les autres métadonnées. Les métadonnées de ce package sont ensuite transformées en CycloneDX SBOM.

Sbomgenpeut être utilisé comme outil autonome pour fournir du CycloneDX SBOM sous forme de fichier ou à STDOUT. Il est également utilisé dans le cadre de l'intégration Amazon Inspector CI/CD, qui analyse automatiquement les images des conteneurs dans le cadre de votre pipeline de déploiement. Pour plus d'informations, consultez Intégration des scans Amazon Inspector dans votre pipeline CI/CD.

Packages et formats d'image pris en charge

À l'heure actuelle, Sbomgen vous pouvez collecter des stocks pour les types de colis suivants :

- Alpine APK
- Debian / Ubuntu DPKG
- Red Hat RPM
- Gocolis via `go.mod` et `go mod cache`
- Javacolis via `pom.properties`
- Node.jspackages via des `package.json` fichiers à l'intérieur `node_modules`
- Packages C# via des fichiers Nuget (`.deps.json`,, `csprojPackages.config`, packages.lock.json)
- PHP via `installed.json` et `composer.lock`

- Pythonpackages via `requirements.txt`Pipfile.lock,`poetry.lock`, et `egg/wheel` fichiers
- Rubypackages via `Gemfile.lock` et gemmes installées dans le monde entier `.gemspec`
- Rustcolis via `Cargo.lock` et `Cargo.toml`

Sbomgenprend en charge les formats de manifeste d'image de conteneur suivants pour les images :

- Manifeste d'images OCI
- Dockermanifeste d'image version 2, schéma 2
- Dockermanifeste d'image version 2, schéma 1
- Dockermanifeste d'images version 1

> **Important**
>
> Sbomgenne peut pas numériser les images de conteneur si leur taille est supérieure à 5 Go, si elles comportent plus de 60 couches ou si plus de 2 000 packages sont installés.

Installation du générateur SBOM d'Amazon Inspector () Sbomgen

Sbomgenest uniquement disponible pour les systèmes d'exploitation Linux. Si vous l'utilisez pour analyser des images de conteneurs, un service de conteneur doit être installé, tel que Docker Podman, oucontainerd.

Pour de meilleures performances, nous recommandons d'exécuter le binaire à partir d'un système présentant les caractéristiques matérielles minimales suivantes :

- Processeur 4 cœurs
- 8 Go de RAM

Pour installer Sbomgen

1. Téléchargez le fichier Sbomgen zip à partir de l'URL correspondant à votre architecture :

   Linux AMD64 :

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip

Linux ARM64 :

https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip

2. Décompressez le téléchargement à l'aide de la commande suivante :

```
unzip inspector-sbomgen.zip
```

3. Vérifiez la présence des fichiers suivants dans l'archive :

- `inspector-sbomgen`— Il s'agit du binaire que vous allez exécuter pour générer des SBOM.
- `README.txt`— Voici la documentation d'utilisationSbomgen.
- `LICENSE.txt`— Ce fichier contient la licence logicielle pourSbomgen.
- `licenses`— Ce dossier contient les informations de licence pour les packages tiers utilisés parSbomgen.
- `checksums.txt`— Ce fichier fournit les hachages du Sbomgen binaire.
- `sbom.json`— Il s'agit d'un CycloneDX SBOM pour le Sbomgen binaire.

4. (Facultatif) Vérifiez l'authenticité et l'intégrité du binaire à l'aide de la commande suivante :

```
sha256sum < inspector-sbomgen
```

- Comparez les résultats avec le contenu du `checksums.txt` fichier.

5. Accordez des autorisations exécutables au binaire à l'aide de la commande suivante :

```
chmod +x inspector-sbomgen
```

6. Vérifiez qu'il Sbomgen est correctement installé à l'aide de la commande suivante :

```
./inspector-sbomgen --version
```

Vous devriez obtenir un résultat similaire à ce qui suit :

```
Version: 1.X.X
```

Utiliser Sbomgen

Vous pouvez l'utiliser Sbomgen pour générer un SBOM pour les images de conteneurs.

Vous pouvez également personnaliser les résultats de la génération de SBOM grâce à des options telles que l'exclusion de fichiers spécifiques ou la définition des packages recherchés par l'outil. Pour des exemples de ces cas d'utilisation, et bien d'autres encore, exécutez la commande suivante :

```
./inspector-sbomgen list-examples
```

Pour générer un SBOM pour une image de conteneur et afficher le résultat dans un fichier

Pour cet exemple, *image:tag*remplacez-le par l'ID de votre image et *output_path.json*par le chemin dans lequel enregistrer la sortie :

```
./inspector-sbomgen container --image image:tag -o output_path.json
```

Authentification auprès des registres privés avec Sbomgen

Vous pouvez générer un SBOM à partir de vos conteneurs hébergés dans des registres privés en fournissant vos informations d'authentification de registre privé. Vous pouvez fournir vos informations d'identification de plusieurs manières : via des informations d'identification mises en cache, via une méthode interactive ou via une méthode non interactive dans laquelle vos informations d'identification sont fournies sous forme de variables d'environnement avant l'exécution. Sbomgen

Authentification à l'aide des informations d'identification mises en cache (recommandé)

1. Sbomgenessaiera d'utiliser les informations d'identification mises en cache si elles sont disponibles sur votre agent. Pour cette méthode, authentifiez-vous d'abord auprès de votre registre de conteneurs. Par exemple, si vous utilisezDocker, vous pouvez vous authentifier auprès de votre registre à l'aide de la Docker `login` commande suivante :

   ```
   docker login
   ```

2. Ensuite, après avoir réussi à vous authentifier auprès de votre registre privé, vous pouvez utiliser Sbomgen une image de conteneur dans ce registre. Pour utiliser l'exemple suivant, remplacez-le *image:tag*par le nom de l'image à numériser :

   ```
   ./inspector-sbomgen container --image image:tag
   ```

Authentification à l'aide de la méthode interactive

- Pour cette méthode, vous devez fournir votre nom d'utilisateur en tant que paramètre et vous Sbomgen serez invité à saisir un mot de passe sécurisé en cas de besoin. Pour utiliser l'exemple

suivant, remplacez-le *image:tag*par le nom de l'image à numériser et *your_username*par un nom d'utilisateur ayant accès à cette image :

```
./inspector-sbomgen container --image image:tag --username
your_username
```

Authentification à l'aide d'une méthode non interactive

- Pour utiliser cette méthode, vous devez enregistrer votre mot de passe ou votre jeton de registre dans un fichier .txt lisible uniquement par l'utilisateur actuel. Le fichier texte ne doit contenir que votre mot de passe ou votre jeton sur une seule ligne. Pour utiliser l'exemple suivant, remplacez-le *your_username*par votre nom d'utilisateur, remplacez par *password.txt*le fichier contenant votre mot de passe ou jeton et remplacez *image:tag*par le nom de l'image à numériser :

```
INSPECTOR_SBOMGEN_USERNAME=your_username\
INSPECTOR_SBOMGEN_PASSWORD=`cat password.txt` \
./inspector-sbomgen container --image image:tag
```

Exemples de sorties de Sbomgen

Voici un exemple de SBOM pour une image de conteneur inventoriée à l'aide de. Sbomgen

Image du conteneur SBOM


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:828875ef-8c32-4777-b688-0af96f3cf619",
  "version": 1,
  "metadata": {
    "timestamp": "2023-11-17T21:36:38Z",
    "tools": [
      {
        "vendor": "Amazon Web Services, Inc. (AWS)",
        "name": "Amazon Inspector SBOM Generator",
        "version": "1.0.0",
        "hashes": [
          {
            "alg": "SHA-256",
```

```
            "content":
"10ab669cfc99774786301a745165b5957c92ed9562d19972fbf344d4393b5eb1"
          }
        ]
      }
    ],
    "component": {
      "bom-ref": "comp-1",
      "type": "container",
      "name": "fedora:latest",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:image_id",
          "value":
"sha256:c81c8ae4dda7dedc0711daefe4076d33a88a69a28c398688090c1141eff17e50"
        },
        {
          "name": "amazon:inspector:sbom_generator:layer_diff_id",
          "value":
"sha256:eddd0d48c295dc168d0710f70364581bd84b1dda6bb386c4a4de0b61de2f2119"
        }
      ]
    }
  },
  "components": [
    {
      "bom-ref": "comp-2",
      "type": "library",
      "name": "dnf",
      "version": "4.18.0",
      "purl": "pkg:pypi/dnf@4.18.0",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib/python3.12/site-packages/dnf-4.18.0.dist-info/METADATA"
        },
```

```
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-dnf@4.18.0-2.fc39?
arch=noarch&distro=39&epoch=0"
        }
      ]
    },
    {
      "bom-ref": "comp-3",
      "type": "library",
      "name": "libcomps",
      "version": "0.1.20",
      "purl": "pkg:pypi/libcomps@0.1.20",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib64/python3.12/site-packages/libcomps-0.1.20-py3.12.egg-
info/PKG-INFO"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-libcomps@0.1.20-1.fc39?
arch=x86_64&distro=39&epoch=0"
        }
      ]
    }
  ]
```

```
}
```

Création de votre propre intégration de pipeline CI/CD personnalisée avec Amazon Inspector Scan

Nous vous recommandons d'utiliser les plug-ins Amazon Inspector CI/CD s'ils sont disponibles sur votre site de vente de CI/CD. Pour une liste des plugins disponibles, voirSolutions CI/CD prises en charge.

Si Amazon Inspector ne fournit pas de plug-ins pour votre solution CI/CD, vous pouvez créer votre propre intégration CI/CD personnalisée en combinant le générateur Amazon Inspector SBOM et l'API Amazon Inspector Scan. Vous pouvez également utiliser une intégration personnalisée pour affiner les scans grâce aux options disponibles dans le générateur SBOM d'Amazon Inspector.

Pour configurer votre propre intégration personnalisée

1. Configurez un Compte AWS pour autoriser l'accès à l'API Amazon Inspector Scan. Pour obtenir des instructions, veuillez consulter Configuration d'un AWS compte pour utiliser l'intégration Amazon Inspector CI/CD.
2. Installez et configurez le binaire Amazon Inspector SBOM Generator. Pour obtenir des instructions, veuillez consulter Installation du générateur SBOM d'Amazon Inspector () Sbomgen.
3. Utilisez le générateur SBOM pour créer un fichier SBOM pour une image de conteneur que vous souhaitez numériser. Pour utiliser l'exemple suivant, remplacez-le *image:id*par le nom de l'image à numériser et *sbom_path.json*par l'emplacement où enregistrer la sortie SBOM :

   ```
   ./inspector-sbomgen container –image image:id -o sbom_path.json
   ```
4. Appelez l'`inspector-scan`API pour scanner le SBOM généré et fournir un rapport de vulnérabilité. Pour utiliser l'exemple suivant, remplacez *sbom_path.json* par le chemin d'accès à un fichier SBOM valide compatible avec CycloneDX. Remplacez ensuite *ENDPOINT* par le point de terminaison API pour lequel Région AWS vous êtes actuellement authentifié, et remplacez *REGION* par la région correspondante. Consultez Points de terminaison pour l'API Amazon Inspector Scan la liste complète des régions et des points de terminaison.

   ```
   aws inspector-scan scan-sbom --sbom file://sbom_path.json --endpoint
   "ENDPOINT" --region REGION
   ```

Formats de sortie de l'API

L'API Amazon Inspector Scan peut générer un rapport de vulnérabilité au format CycloneDX 1.5 ou Amazon Inspector trouve du JSON. La valeur par défaut peut être modifiée à l'aide du `--output-format` drapeau.

Exemple de sortie au format CycloneDX 1.5


```
{
  "status": "SBOM parsed successfully, 1 vulnerabilities found",
  "sbom": {
    "bomFormat": "CycloneDX",
    "specVersion": "1.5",
    "serialNumber": "urn:uuid:0077b45b-ff1e-4dbb-8950-ded11d8242b1",
    "metadata": {
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:critical_vulnerabilities",
          "value": "1"
        },
        {
          "name": "amazon:inspector:sbom_scanner:high_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:medium_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:low_vulnerabilities",
          "value": "0"
        }
      ],
      "tools": [
        {
          "name": "CycloneDX SBOM API",
          "vendor": "Amazon Inspector",
          "version": "empty:083c9b00:083c9b00:083c9b00"
        }
      ],
      "timestamp": "2023-06-28T14:15:53.760Z"
    },
    "components": [
```

```
      {
        "bom-ref": "comp-1",
        "type": "library",
        "name": "log4j-core",
        "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.12.1",
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:path",
            "value": "/home/dev/foo.jar"
          }
        ]
      }
    ],
    "vulnerabilities": [
      {
        "bom-ref": "vuln-1",
        "id": "CVE-2021-44228",
        "source": {
          "name": "NVD",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
        },
        "references": [
          {
            "id": "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            }
          },
          {
            "id": "GHSA-jfh8-c2jp-5v3q",
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            }
          }
        ],
        "ratings": [
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v3-1/"
            },
```

```
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          },
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v2/"
            },
            "score": 9.3,
            "severity": "critical",
            "method": "CVSSv2",
            "vector": "AC:M/Au:N/C:C/I:C/A:C"
          },
          {
            "source": {
              "name": "EPSS",
              "url": "https://www.first.org/epss/"
            },
            "score": 0.97565,
            "severity": "none",
            "method": "other",
            "vector": "model:v2023.03.01,date:2023-06-27T00:00:00+0000"
          },
          {
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
          },
          {
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
```

```
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          }
        ],
        "cwes": [
          400,
          20,
          502
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "advisories": [
          {
            "url": "https://www.intel.com/content/www/us/en/security-center/advisory/
intel-sa-00646.html"
          },
          {
            "url": "https://support.apple.com/kb/HT213189"
          },
          {
            "url": "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/"
          },
          {
            "url": "https://logging.apache.org/log4j/2.x/security.html"
          },
          {
            "url": "https://www.debian.org/security/2021/dsa-5020"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf"
          },
          {
            "url": "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpujan2022.html"
          },
```

```
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpuapr2022.html"
          },
          {
            "url": "https://twitter.com/kurtseifried/status/1469345530182455296"
          },
          {
            "url": "https://tools.cisco.com/security/center/content/
CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd"
          },
          {
            "url": "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html"
          },
          {
            "url": "https://www.kb.cert.org/vuls/id/930724"
          }
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "affects": [
          {
            "ref": "comp-1"
          }
        ],
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:exploit_available",
```

```
            "value": "true"
          },
          {
            "name": "amazon:inspector:sbom_scanner:exploit_last_seen_in_public",
            "value": "2023-03-06T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_added",
            "value": "2021-12-10T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_due",
            "value": "2021-12-24T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:fixed_version:comp-1",
            "value": "2.15.0"
          }
        ]
      }
    ]
  }
}
```

Exemple de sortie au format Inspector

```
                        {
  "status": "SBOM parsed successfully, 1 vulnerability found",
  "inspector": {
    "messages": [
      {
        "name": "foo",
        "purl": "pkg:maven/foo@1.0.0", // Will not exist in output if missing in sbom
        "info": "Component skipped: no rules found."
      }
    ],
    "vulnerability_count": {
      "critical": 1,
      "high": 0,
      "medium": 0,
      "low": 0
    },
```

```
    "vulnerabilities": [
      {
        "id": "CVE-2021-44228",
        "severity": "critical",
        "source": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228",
        "related": [
          "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
          "GHSA-jfh8-c2jp-5v3q"
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "references": [
          "https://www.intel.com/content/www/us/en/security-center/advisory/intel-
sa-00646.html",
          "https://support.apple.com/kb/HT213189",
          "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/",
          "https://logging.apache.org/log4j/2.x/security.html",
          "https://www.debian.org/security/2021/dsa-5020",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf",
          "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html",
          "https://www.oracle.com/security-alerts/cpujan2022.html",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/",
          "https://www.oracle.com/security-alerts/cpuapr2022.html",
          "https://twitter.com/kurtseifried/status/1469345530182455296",
          "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-
sa-apache-log4j-qRuKNEbd",
          "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html",
          "https://www.kb.cert.org/vuls/id/930724"
        ],
        "created": "2021-12-10T10:15:00Z",
```

```
        "updated": "2023-04-03T20:15:00Z",
        "properties": {
          "cisa_kev_date_added": "2021-12-10T00:00:00Z",
          "cisa_kev_date_due": "2021-12-24T00:00:00Z",
          "cwes": [
            400,
            20,
            502
          ],
          "cvss": [
            {
              "source": "NVD",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
              "cvss2_base_score": 9.3,
              "cvss2_base_vector": "AC:M/Au:N/C:C/I:C/A:C"
            },
            {
              "source": "SNYK",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
            },
            {
              "source": "GITHUB",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
            }
          ],
          "epss": 0.97565,
          "exploit_available": true,
          "exploit_last_seen_in_public": "2023-03-06T00:00:00Z"
        },
        "affects": [
          {
            "installed_version": "pkg:maven/org.apache.logging.log4j/log4j-
core@2.12.1",
            "fixed_version": "2.15.0",
            "path": "/home/dev/foo.jar"
          }
        ]
      }
```

```
    ]
  }
}
```

Utilisation du Jenkins plugin Amazon Inspector

Le Jenkins plugin utilise le binaire Amazon Inspector SBOM Generator et l'API Amazon Inspector Scan pour produire des rapports détaillés à la fin de votre build, afin que vous puissiez étudier et corriger les risques avant le déploiement.

Amazon Inspector est un service de gestion des vulnérabilités qui analyse les images de conteneurs pour détecter les vulnérabilités du système d'exploitation et des packages de langage de programmation sur la base des CVE.

À l'aide du Jenkins plug-in Amazon Inspector, vous pouvez ajouter des analyses de vulnérabilité Amazon Inspector à votre Jenkins pipeline.

> **Note**
>
> Les analyses de vulnérabilité d'Amazon Inspector peuvent être configurées pour réussir ou échouer les exécutions de pipeline en fonction du nombre et de la gravité des vulnérabilités détectées.

Vous pouvez consulter la dernière version du Jenkins plugin sur le Jenkins marché à l'adresse https://plugins.jenkins.io/amazon-inspector-image-scanner/.

Les étapes suivantes décrivent comment configurer le Jenkins plug-in Amazon Inspector.

> **Important**
>
> Avant d'effectuer les étapes suivantes, vous devez mettre à niveau Jenkins vers la version 2.387.3 ou supérieure pour que le plugin puisse s'exécuter.

Étape 1. Configurez un Compte AWS

Configurez un Compte AWS avec un rôle IAM qui autorise l'accès à l'API Amazon Inspector Scan. Pour obtenir des instructions, veuillez consulter Configuration d'un AWS compte pour utiliser l'intégration Amazon Inspector CI/CD.

Étape 2. Installez le plugin Jenkins d'Amazon Inspector

La procédure suivante décrit comment installer le plug-in Amazon Inspector Jenkins depuis le Jenkins tableau de bord.

1. Dans le tableau de bord Jenkins, choisissez Manage Jenkins, puis Manage Plugins.
2. Choisissez Disponible.
3. Dans l'onglet Available, recherchez Amazon Inspector Scans, puis installez le plugin.

(Facultatif) Étape 3. Ajoutez les informations d'identification du docker à Jenkins

> **Note**
>
> Ajoutez les informations d'identification du docker uniquement si l'image du docker se trouve dans un référentiel privé. Sinon, Ignorez cette étape.

La procédure suivante décrit comment ajouter des informations d'identification docker Jenkins depuis le Jenkins tableau de bord.

1. Dans le tableau de bord Jenkins, choisissez Manage Jenkins, Credentials, puis System.
2. Choisissez Informations d'identification globales, puis Ajouter des informations d'identification.
3. Pour Kind, sélectionnez Nom d'utilisateur avec mot de passe.
4. Pour Scope, sélectionnez Global (Jenkins, nœuds, éléments, tous les éléments enfants, etc.).
5. Entrez vos informations, puis cliquez sur OK.

(Facultatif) Étape 4. Ajouter des AWS informations d'identification

> **Note**
>
> Ajoutez des AWS informations d'identification uniquement si vous souhaitez vous authentifier en fonction d'un utilisateur IAM. Sinon, Ignorez cette étape.

La procédure suivante décrit comment ajouter des AWS informations d'identification depuis le Jenkins tableau de bord.

1. Dans le tableau de bord Jenkins, choisissez Manage Jenkins, Credentials, puis System.
2. Choisissez Informations d'identification globales, puis Ajouter des informations d'identification.
3. Pour Kind, sélectionnez AWS Credentials.
4. Entrez vos informations, y compris votre identifiant de clé d'accès et votre clé d'accès secrète, puis cliquez sur OK.

Étape 5. Ajouter le support CSS dans un Jenkins script

La procédure suivante décrit comment ajouter le support CSS dans un Jenkikns script.

1. Redémarrez Jenkins.
2. Dans le tableau de bord, choisissez Manage Jenkins, Nodes, Built-In Node, puis Script Console.
3. Dans la zone de texte, ajoutez la ligne`System.setProperty("hudson.model.DirectoryBrowserSupport.CSP", "")`, puis choisissez Exécuter.

Étape 6. Ajoutez Amazon Inspector Scan à votre build

Vous pouvez ajouter Amazon Inspector Scan à votre build en ajoutant une étape de compilation dans votre projet ou en utilisant le pipeline Jenkins déclaratif.

Amazon Inspector Scannez votre build en ajoutant une étape de compilation à votre projet

1. Sur la page de configuration, faites défiler la page vers le bas jusqu'à Build Steps, puis choisissez Add build step. Sélectionnez ensuite Amazon Inspector Scan.
2. Choisissez entre deux méthodes d'installation inspectors-sbomgen : automatique ou manuelle.

   a. (Option 1) Choisissez Automatique pour télécharger la dernière version d'inspectors-sbomgen. Si vous choisissez cette méthode, assurez-vous de sélectionner l'architecture du processeur qui correspond au système qui exécute le plugin.

   b. (Option 2) Choisissez Manuel si vous souhaitez configurer le binaire Amazon Inspector SBOM Generator pour la numérisation. Si vous choisissez cette méthode, assurez-vous de fournir le chemin complet vers une version précédemment téléchargée de inspectors-sbomgen.

   Pour plus d'informations, consultez Installation d'Amazon Inspector SBOM Generator (Sbomgen) dans Amazon Inspector SBOM Generator.
3. Pour terminer la configuration de l'étape de génération d'Amazon Inspector Scan, procédez comme suit :

   a. Entrez votre identifiant d'image. L'image peut être locale, distante ou archivée. Les noms des images doivent respecter la convention de Docker dénomination. Si vous analysez une image exportée, indiquez le chemin d'accès au fichier tar attendu. Consultez les exemples de chemins d'identification d'image suivants :

      i. Pour les conteneurs locaux ou distants : `NAME[:TAG|@DIGEST]`

      ii. Pour un fichier tar : `/path/to/image.tar`

   b. Sélectionnez et par lequel Région AWSenvoyer la demande de numérisation.

   c. (Facultatif) Pour les informations d'identification Docker, sélectionnez votre Docker nom d'utilisateur. Procédez ainsi uniquement si l'image de votre conteneur se trouve dans un dépôt privé.

   d. (Facultatif) Vous pouvez fournir les méthodes AWS d'authentification prises en charge suivantes :

      i. (Facultatif) Pour le rôle IAM, fournissez un ARN de rôle (arn:aws:iam : :role/). *AccountNumberRoleName*

ii. (Facultatif) Pour les informations d'identification AWS, sélectionnez l'identifiant à authentifier en fonction d'un utilisateur IAM.

iii. (Facultatif) Pour le nom du AWS profil, indiquez le nom du profil à authentifier à l'aide d'un nom de profil.

e. (Facultatif) Spécifiez les seuils de vulnérabilité par gravité. Si le nombre que vous spécifiez est dépassé lors d'une numérisation, la création de l'image échouera. Si les valeurs sont toutes`0`, la compilation réussira, que des vulnérabilités soient détectées ou non.

4. Choisissez Enregistrer.

Ajoutez Amazon Inspector Scan à votre build à l'aide du Jenkins pipeline déclaratif

Vous pouvez ajouter Amazon Inspector Scan à votre build à l'aide du pipeline déclaratif Jenkins automatiquement ou manuellement.

Pour télécharger automatiquement le pipeline déclaratif SBOMgen

- Pour ajouter Amazon Inspector Scan à une version, utilisez l'exemple de syntaxe suivant. Selon l'architecture de système d'exploitation que vous préférez pour le téléchargement d'Amazon Inspector SBOM Generator, remplacez *`SBOMGEN_SOURCE par LinuxAMD64 ou LinuxARM64`*. Remplacez *`IMAGE_PATH`* par le chemin d'accès à votre image (par exemple *`alpine:latest`*), IAM_ROLE *`par`* l'ARN du rôle IAM que vous avez configuré à l'étape 1 et *`ID`* par votre identifiant Docker d'identification si vous utilisez un référentiel privé. Vous pouvez éventuellement activer les seuils de vulnérabilité et spécifier des valeurs pour chaque gravité.

```
pipeline {
   agent any
   stages {
       stage('amazon-inspector-image-scanner') {
           steps {
               script {
               step([
               $class:
 'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
               sbomgenSource: 'SBOMGEN_SOURCE', // this can be linuxAmd64 or linuxArm64
               archivePath: 'IMAGE_PATH',
               awsRegion: 'REGION',
               iamRole: 'IAM ROLE',
```

```
                credentialId: 'Id', // provide empty string if image not in private
 repositories
                awsCredentialId: ''AWS ID;',
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
        }
    }
}
```

Pour télécharger manuellement le pipeline déclaratif SBOMgen

- Pour ajouter Amazon Inspector Scan à une version, utilisez l'exemple de syntaxe suivant. *Remplacez SBOMGEN_PATH par le chemin d'accès au générateur Amazon Inspector SBOM que vous avez installé à l'étape 3, IMAGE_PATH par le chemin d'accès à votre image (par exemple alpine:latest), IAM_ROLE par l'ARN du rôle IAM que vous avez configuré à l'étape 1, et ID par votre identifiant d'identification si vous utilisez un référentiel privé.* Docker Vous pouvez éventuellement activer les seuils de vulnérabilité et spécifier des valeurs pour chaque gravité.

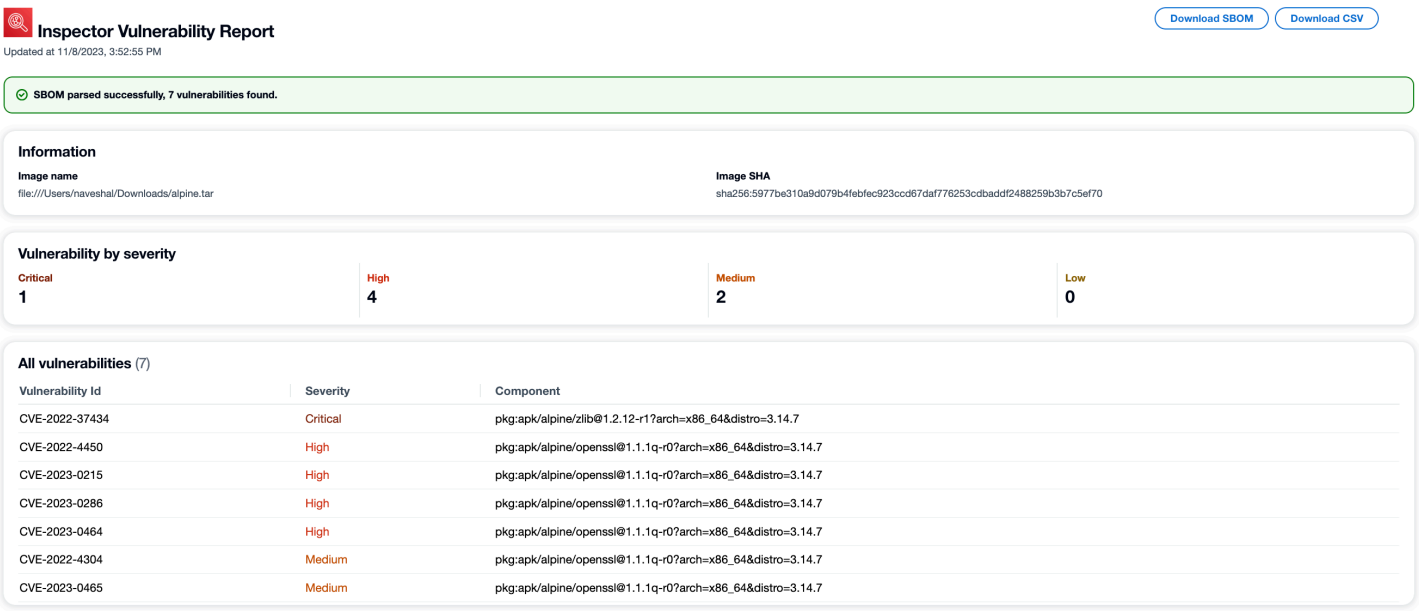
> **Note**
>
> SbomgenPlacez-le dans le répertoire Jenkins et fournissez le chemin d'accès au répertoire Jenkins dans le plugin (par exemple */opt/folder/arm64/inspector-sbomgen*).

```
pipeline {
    agent any
    stages {
        stage('amazon-inspector-image-scanner') {
            steps {
                script {
                step([
```

```
                $class:
'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenPath: 'SBOMGEN_PATH',
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                awsCredentialId: ''AWS ID;',
                credentialId: 'Id;', // provide empty string if image not in private
repositories
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
        }
      }
 }
```

Étape 7. Consultez votre rapport sur les vulnérabilités d'Amazon Inspector

1. Réalisez une nouvelle version de votre projet.
2. Une fois la génération terminée, sélectionnez un format de sortie parmi les résultats. Si vous sélectionnez HTML, vous avez la possibilité de télécharger une version JSON SBOM ou CSV du rapport. Voici un exemple de rapport HTML :



Résolution des problèmes

Les erreurs suivantes sont courantes que vous pouvez rencontrer lors de l'utilisation du plug-in Amazon Inspector Scan pourJenkins.

Impossible de charger les informations d'identification ou erreur d'exception STS

Erreur :

```
InstanceProfileCredentialsProvider(): Failed to load credentials or sts exception.
```

Résolution

Obtenez `aws_access_key_id` et `aws_secret_access_key` pour votre AWS compte. Configuration `aws_access_key_id` et mise `aws_secret_access_key` en place`~/.aws/credentials`.

Erreur de chemin Inspector-SBOMGen

Erreur :

```
Exception:com.amazon.inspector.jenkins.amazoninspectorbuildstep.exception.Sbomge
There was an issue running inspector-sbomgen, is /opt/inspector/inspector-sbomgen the correct path?
```

Résolution :

Suivez la procédure ci-dessous pour résoudre le problème.

1. Placez l'architecture du système d'exploitation correcte Inspector-SBOMGen dans le Jenkins répertoire Pour plus d'informations, consultez Amazon Inspector SBOM Generator.
2. Accordez des autorisations exécutables au binaire à l'aide de la commande suivante :`chmod +x inspector-sbomgen`.
3. Fournissez le chemin de Jenkins machine correct dans le plugin, par exemple`/opt/folder/arm64/inspector-sbomgen`.
4. Enregistrez la configuration et exécutez le Jenkins travail.

Utilisation du TeamCity plugin Amazon Inspector

Le TeamCity plugin Amazon Inspector vous permet d'ajouter des analyses de vulnérabilité Amazon Inspector à votre TeamCity pipeline. Le plugin utilise le binaire Amazon Inspector SBOM Generator et l'API Amazon Inspector Scan pour produire des rapports détaillés à la fin de votre build afin que vous puissiez étudier et corriger les risques avant le déploiement. Les analyses peuvent également être configurées pour réussir ou échouer les exécutions de pipeline en fonction du nombre et de la gravité des vulnérabilités détectées.

Amazon Inspector est un service de gestion des vulnérabilités proposé par AWS qui analyse les images de conteneurs pour détecter les vulnérabilités du système d'exploitation et des packages de langage de programmation sur la base des CVE. Pour plus d'informations sur l'intégration Amazon Inspector CI/CD, consultez. Intégration des scans Amazon Inspector dans votre pipeline CI/CD

Pour obtenir la liste des packages et des formats d'image de conteneur pris en charge par le plug-in Amazon Inspector, consultez,Packages et formats d'image pris en charge.

Vous pouvez consulter la dernière version du plugin sur le TeamCity marché à l'adresse https://plugins.jetbrains.com/plugin/23236 - amazon-inspector-scanner. Vous pouvez également suivre les étapes décrites dans chaque section de ce document pour configurer le TeamCity plug-in Amazon Inspector :

1. Configurez un Compte AWS.

- Configurez un Compte AWS avec un rôle IAM qui autorise l'accès à l'API Amazon Inspector Scan. Pour obtenir des instructions, veuillez consulter Configuration d'un AWS compte pour utiliser l'intégration Amazon Inspector CI/CD.

2. Installez le TeamCity plugin Amazon Inspector.

   a. Depuis votre tableau de bord, accédez à Administration > Plug-ins.

   b. Recherchez Amazon Inspector Scans.

   c. Installez le plug-in .

3. Installez le générateur Amazon Inspector SBOM.

   - Installez le binaire Amazon Inspector SBOM Generator dans le répertoire de votre serveur Teamcity. Pour obtenir des instructions, veuillez consulter Installation du générateur SBOM d'Amazon Inspector () Sbomgen.

4. Ajoutez une étape de génération d'Amazon Inspector Scan à votre projet.

   a. Sur la page de configuration, faites défiler la page vers le bas jusqu'à Build Steps, choisissez Add build step, puis sélectionnez Amazon Inspector Scan.

   b. Configurez l'étape de génération d'Amazon Inspector Scan en renseignant les informations suivantes :

      - Ajoutez un nom d'étape.
      - Choisissez entre deux méthodes d'installation du générateur Amazon Inspector SBOM : automatique ou manuelle.
        - Télécharge automatiquement la version la plus récente d'Amazon Inspector SBOM Generator en fonction de votre système et de l'architecture de votre processeur.
        - Le manuel exige que vous fournissiez un chemin complet vers une version précédemment téléchargée d'Amazon Inspector SBOM Generator.

        Pour plus d'informations, consultez Installation d'Amazon Inspector SBOM Generator (Sbomgen) dans Amazon Inspector SBOM Generator.
      - Entrez votre identifiant d'image. Votre image peut être locale, distante ou archivée. Les noms des images doivent respecter la convention de Docker dénomination. Si vous analysez une image exportée, indiquez le chemin d'accès au fichier tar attendu. Consultez les exemples de chemins d'identification d'image suivants :
        - Pour les conteneurs locaux ou distants : `NAME[:TAG|@DIGEST]`

- Pour un fichier tar : `/path/to/image.tar`

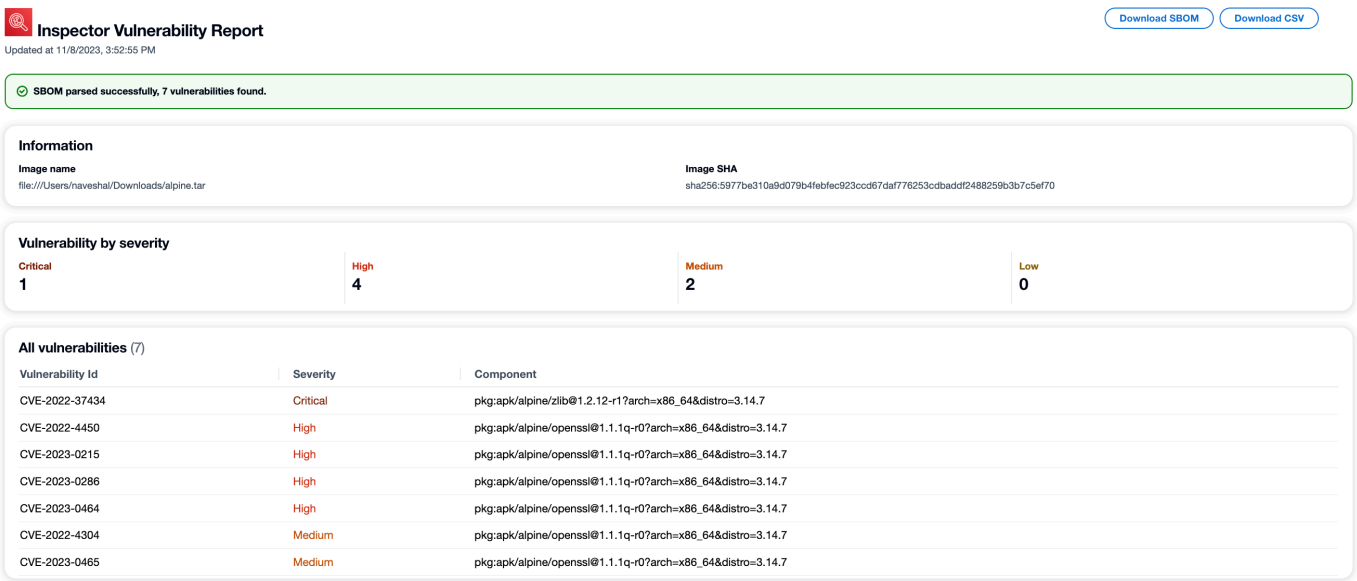
- Pour le rôle IAM, entrez l'ARN du rôle que vous avez configuré à l'étape 1.
- Sélectionnez et par lequel Région AWSenvoyer la demande de numérisation.
- (Facultatif) Pour l'authentification Docker, entrez votre nom d'utilisateur Docker et votre mot de passe Docker. Procédez ainsi uniquement si l'image de votre conteneur se trouve dans un dépôt privé.
- (Facultatif) Pour AWS l'authentification, entrez l'ID de votre clé d' AWS accès et votre clé AWS secrète. Ne le faites que si vous souhaitez vous authentifier en fonction des AWS informations d'identification.
- (Facultatif) Spécifiez les seuils de vulnérabilité par gravité. Si le nombre que vous spécifiez est dépassé lors d'une numérisation, la création de l'image échouera. Si les valeurs sont toutes, `0` le build réussira quel que soit le nombre de vulnérabilités détectées.

c. Sélectionnez Save.

5. Consultez votre rapport sur les vulnérabilités d'Amazon Inspector.

a. Réalisez une nouvelle version de votre projet.

b. Lorsque la construction est terminée, sélectionnez un format de sortie parmi les résultats. Lorsque vous sélectionnez HTML, vous avez la possibilité de télécharger une version JSON SBOM ou CSV du rapport. Voici un exemple de rapport HTML :



Espaces de CycloneDX noms Amazon Inspector

Amazon Inspector a réservé des CycloneDX espaces de noms et des noms de propriété à utiliser avec les SBOM produits par le générateur de SBOM Amazon Inspector et l'API Amazon Inspector Scan. Cette page décrit toutes les propriétés clé/valeur personnalisées qui peuvent être ajoutées aux composants des CycloneDX SBOM créés à l'aide des outils Amazon Inspector. Pour plus d'informations sur les taxonomies des CycloneDX propriétés, consultez la documentation officielle.

`amazon:inspector:sbom_scanner`taxonomie des espaces de noms

L'espace de `amazon:inspector:sbom_scanner` noms est utilisé par l'API Amazon Inspector Scan. Il comprend les propriétés suivantes :

Propriété	Description
`amazon:inspector:sbom_scanner:critical_vulnerabilities`	Nombre total de vulnérabilités critiques détectées dans le SBOM.
`amazon:inspector:sbom_scanner:high_vulnerabilities`	Nombre total de vulnérabilités très graves détectées dans le SBOM.
`amazon:inspector:sbom_scanner:medium_vulnerabilities`	Nombre total de vulnérabilités de gravité moyenne détectées dans le SBOM.
`amazon:inspector:sbom_scanner:low_vulnerabilities`	Nombre total de vulnérabilités de faible gravité détectées dans le SBOM.
`amazon:inspector:sbom_scanner:info`	Fournit un contexte d'analyse pour un composant donné, par exemple : « Composant scanné : aucune vulnérabilité détectée ».
`amazon:inspector:sbom_scanner:warning`	Fournit un contexte expliquant pourquoi un composant donné n'a pas été scanné, par exemple : « Composant ignoré : aucun purl fourni ».
`amazon:inspector:sbom_scanner:fixed_version: component_bom_ref`	Fournit la version corrigée du composant indiqué pour la vulnérabilité donnée.

Propriété	Description
`amazon:inspector:sbom_scanner:exploit_available`	Indique si un exploit est disponible pour la vulnérabilité donnée.
`amazon:inspector:sbom_scanner:exploit_last_seen_in_public`	Indique quand un exploit a été vu pour la dernière fois en public pour la vulnérabilité donnée.
`amazon:inspector:sbom_scanner:cisa_kev_date_added`	Indique à quel moment la vulnérabilité a été ajoutée au catalogue CISA Known Exploited Vulnerabilities.
`amazon:inspector:sbom_scanner:cisa_kev_date_due`	Indique la date à laquelle le correctif de vulnérabilité doit être corrigé conformément au catalogue CISA Known Exploited Vulnerabilities.
`amazon:inspector:sbom_scanner:path`	Le chemin d'accès au fichier qui a fourni les informations du package en question.

`amazon:inspector:sbom_generator`taxonomie des espaces de noms

L'espace de `amazon:inspector:sbom_generator` noms est utilisé par le générateur Amazon Inspector SBOM. Il comprend les propriétés suivantes :

Propriété	Description
`amazon:inspector:sbom_generator:os_hostname`	Le nom d'hôte du système en cours d'inventaire.
`amazon:inspector:sbom_generator:kernel_name`	Le nom du noyau du système en cours d'inventaire.
`amazon:inspector:sbom_generator:kernel_version`	Version du noyau du système inventoriée.

Propriété	Description
amazon:inspector:sbom_generator:cpu_architecture	Architecture du processeur du système inventorié, telle que x86_64.
amazon:inspector:sbom_generator:image_id	Le hachage du fichier de configuration de l'image du conteneur, également appelé ID d'image.
amazon:inspector:sbom_generator:layer_diff_id	Le hachage de la couche d'image du conteneur non compressée.
amazon:inspector:sbom_generator:source_file_scanner	Le scanner qui a trouvé le fichier contenant les informations du package, par exemple :/var/lib/dpkg/status .
amazon:inspector:sbom_generator:source_package_collector	Le collecteur qui a extrait le nom et la version du package à partir d'un fichier spécifique.
amazon:inspector:sbom_generator:source_path	Le chemin d'accès au fichier à partir duquel les informations du package en question ont été extraites.
amazon:inspector:sbom_generator:is_duplicate_package	Indique que le package en question a été trouvé par plusieurs analyseurs de fichiers.
amazon:inspector:sbom_generator:go_toolchain	Indique la version du Go compilateur ou de la chaîne d'outils utilisée pour produire un exécutable Go.
amazon:inspector:sbom_generator:expires_before	la date avant que le certificat SSL ne soit valide.
amazon:inspector:sbom_generator:expires_after	la date après laquelle le certificat SSL n'est plus valide.
amazon:inspector:sbom_generator:is_expired	une valeur booléenne qui indique si le certificat SSL a expiré.

Analyse automatisée des ressources avec Amazon Inspector

Le scan sans agent Amazon Inspector pour Amazon EC2 est disponible en version préliminaire. Votre utilisation de la fonctionnalité de numérisation sans agent Amazon EC2 est soumise à la section 2 des conditions de AWS service (« Bêtas et aperçus »).

Amazon Inspector utilise son propre moteur d'analyse spécialement conçu. Ce moteur surveille vos ressources pour détecter les vulnérabilités logicielles ou les chemins réseau ouverts susceptibles de compromettre les charges de travail, d'utiliser des ressources à des fins malveillantes ou d'accéder non autorisé à vos données. Lorsqu'Amazon Inspector détecte une vulnérabilité, il crée une constatation. Les résultats incluent des détails associés à la détection pour vous aider à remédier à la vulnérabilité. Vous pouvez consulter les résultats sur la console Amazon Inspector et en utilisant l'API Amazon Inspector. Pour de plus amples informations, veuillez consulter Gestion des résultats dans Amazon Inspector.

Lorsqu'il est activé, Amazon Inspector découvre automatiquement toutes les ressources éligibles et lance des analyses continues de ces ressources. Amazon Inspector analyse les vulnérabilités logicielles et les risques d'exposition involontaire au réseau. Amazon Inspector exécute également des scans en réponse à des événements tels que l'installation d'une nouvelle application ou d'un nouveau correctif.

Lorsque vous activez Amazon Inspector pour la première fois, votre compte est automatiquement inscrit à tous les types de scan. Les rubriques suivantes présentent des informations spécifiques sur les types de scan proposés par Amazon Inspector. Amazon Inspector classe les types de scan en fonction du type de ressource concerné par une vulnérabilité. Les rubriques suivantes décrivent les ressources qu'Amazon Inspector analyse, les éléments qui déclenchent de nouvelles analyses pour ces ressources et la manière de configurer les analyses pour chaque type de ressource.

Rubriques

- AWS Lambda Fonctions de numérisation avec Amazon Inspector
- Désactivation d'un type de scan

Lorsque vous activez Amazon Inspector pour la première fois, votre compte est automatiquement inscrit aux types de scan suivants : scan Amazon EC2, scan Amazon ECR, scan standard Lambda. Le scan de code Lambda est une couche optionnelle de numérisation des fonctions Lambda que vous pouvez activer à tout moment.

Présentation des types de scan Amazon Inspector

Amazon Inspector propose différents types de scan axés sur des types de ressources spécifiques de votre AWS environnement.

Numérisation Amazon EC2

Lorsque vous activez le scan Amazon EC2, Amazon Inspector analyse vos instances Amazon EC2 pour détecter les vulnérabilités des packages de système d'exploitation et de langage de programmation, ainsi que l'accessibilité au réseau. Amazon Inspector analyse votre instance EC2 pour détecter les vulnérabilités et expositions courantes (CVE) et les problèmes d'exposition au réseau. Amazon Inspector effectue des scans à l'aide de l'agent SSM installé sur votre instance ou via des instantanés Amazon EBS des instances. Pour plus d'informations sur les scans pour Amazon EC2, consultez. Numérisation d'instances Amazon EC2 avec Amazon Inspector

Numérisation Amazon ECR

Lorsque vous activez le scan Amazon ECR, Amazon Inspector convertit tous les référentiels de conteneurs de numérisation de base de votre registre privé en un scan amélioré avec analyse continue. Vous pouvez également éventuellement configurer ce paramètre pour analyser uniquement en mode push ou pour analyser certains référentiels via des règles d'inclusion. Toutes les images envoyées au cours des 30 derniers jours ou extraites au cours des 90 derniers jours sont initialement numérisées. Amazon Inspector continue de surveiller les images pendant 90 jours par défaut. Ce paramètre peut être modifié à tout moment. Pour plus d'informations sur les scans pour Amazon ECR, consultezNumérisation d'images de conteneurs Amazon ECR avec Amazon Inspector.

Numérisation standard Lambda

Lorsque vous activez le scan standard Lambda, Amazon Inspector découvre les fonctions Lambda de votre compte et commence immédiatement à les analyser pour détecter les

vulnérabilités. Amazon Inspector analyse les nouvelles fonctions et couches Lambda lorsqu'elles sont déployées, et les réanalyse lorsqu'elles sont mises à jour ou lorsque de nouvelles vulnérabilités et expositions communes (CVE) sont publiées. Pour plus d'informations sur le scan des fonctions Lambda, consultez. AWS Lambda Fonctions de numérisation avec Amazon Inspector

Numérisation standard Lambda + Numérisation de code Lambda

Cette option combine le scan standard Lambda avec le scan du code Lambda. Lorsque le scan du code Lambda est activé, Amazon Inspector découvre les fonctions et les couches Lambda de votre compte et analyse les dépendances de votre package d'application pour détecter les vulnérabilités du code. Le scan du code Lambda analyse le code d'application personnalisé dans vos fonctions Lambda pour détecter les vulnérabilités du code. Ces deux types de scan doivent être activés ensemble. Pour plus d'informations, consultez Numérisation du code Lambda d'Amazon Inspector.

Activation d'un type de scan

Vous pouvez activer un nouveau type de scan Amazon Inspector à tout moment. Une fois que vous avez activé un type de scan, Amazon Inspector commence immédiatement à scanner les ressources éligibles pour ce type de scan. Pour un aperçu des types de scan disponibles, voirPrésentation des types de scan Amazon Inspector. Ce qui suit décrit ce qui se passe lorsque vous activez pour la première fois chaque type de scan :

- Scan Amazon EC2 — Lorsque vous activez le scan Amazon EC2 pour un compte, Amazon Inspector analyse toutes les instances éligibles de votre compte pour détecter les vulnérabilités des packages et les problèmes d'accessibilité au réseau. Le plug-in Amazon Inspector SSM est installé sur tous vos hôtes gérés par SSMWindows. Pour de plus amples informations, veuillez consulter WindowsInstances de numérisation. En outre, Amazon Inspector crée les associations SSM suivantes dans votre compte :
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`.

- Numérisation Amazon ECR — Lorsque vous activez la numérisation d'images de conteneurs Amazon ECR pour un compte, le type de numérisation Amazon ECR pour les référentiels privés de ce compte passe de la numérisation de base avec Amazon ECR à la numérisation améliorée avec Amazon Inspector. Toutes les images de conteneurs Amazon ECR éligibles envoyées au cours des 30 derniers jours, ou extraites au cours des 90 derniers jours, sont ensuite analysées pour détecter les vulnérabilités des packages. En outre, la durée de votre nouvelle analyse Amazon ECR est fixée à 90 jours pour la date d'envoi et d'extraction des images.
- Analyse standard Lambda : lorsque vous activez l'analyse standard Lambda dans un compte, toutes les fonctions Lambda de votre compte qui ont été invoquées ou mises à jour au cours des 90 derniers jours sont analysées pour détecter les vulnérabilités des packages. De plus, une chaîne liée à un CloudTrail service est créée dans votre compte.
- Numérisation standard Lambda + numérisation par code Lambda — Ces types de numérisation par fonction Lambda sont activés ensemble. Lorsque vous activez le scan de code Lambda dans un compte, toutes les fonctions Lambda de votre compte qui ont été invoquées ou mises à jour au cours des 90 derniers jours sont analysées pour détecter les vulnérabilités du code.

Activation des scans

Si vous êtes l'administrateur délégué d'Amazon Inspector au AWS sein d'une organisation, vous pouvez activer automatiquement différents types de scan Amazon Inspector pour plusieurs comptes dans plusieurs régions à l'aide d'un script shell développé par Amazon Inspector inspector2-enablement-with-cli on. GitHub Sinon, pour effectuer cette procédure dans un environnement multi-comptes via la console, effectuez les étapes suivantes lorsque vous êtes connecté en tant qu'administrateur délégué Amazon Inspector.

Console

Pour activer les scans

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
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 un nouveau type de numérisation.
3. Dans le volet de navigation, sélectionnez Gestion des comptes.
4. Sur la page Gestion des comptes, sélectionnez les comptes pour lesquels vous souhaitez activer un type de scan.

5. Choisissez Activer et sélectionnez le type de numérisation que vous souhaitez activer.
6. (Recommandé) Répétez ces étapes Région AWS pour chacune des étapes pour lesquelles vous souhaitez activer ce type de scan.

API

Exécutez l'opération Enable API. Dans la demande, indiquez les identifiants de compte pour lesquels vous activez les scans, le jeton d'idempotentie, et un ou plusieurs des`EC2`, `ECR`, `LAMBDA`, ou `LAMBDA_CODE` `resourceTypes` pour activer les scans de ce type.

Numérisation d'instances Amazon EC2 avec Amazon Inspector

Le scan sans agent Amazon Inspector pour Amazon EC2 est disponible en version préliminaire. Votre utilisation de la fonctionnalité de numérisation sans agent Amazon EC2 est soumise à la section 2 des conditions de AWS service (« Bêtas et aperçus »).

L'analyse Amazon Inspector EC2 extrait les métadonnées de votre instance EC2, puis compare ces métadonnées aux règles collectées à partir des avis de sécurité afin de produire des résultats. Amazon Inspector analyse les instances pour détecter les vulnérabilités des packages et les problèmes d'accessibilité au réseau. Pour plus d'informations sur les types de résultats produits pour ces problèmes, voirRecherche de types dans Amazon Inspector.

Amazon Inspector effectue des analyses d'accessibilité au réseau toutes les 24 heures, tandis que les analyses de vulnérabilité des packages sont effectuées à une cadence variable en fonction de la méthode d'analyse associée à l'instance.

Méthodes de numérisation

Les analyses de vulnérabilité des packages peuvent être effectuées à l'aide d'une méthode d'analyse basée sur un agent ou sans agent. Ces méthodes d'analyse déterminent comment et quand Amazon Inspector collecte l'inventaire des logiciels à partir d'une instance EC2 pour les analyses de vulnérabilité des packages. La méthode basée sur un agent repose sur l'agent SSM pour collecter l'inventaire des logiciels, tandis que la méthode sans agent utilise des instantanés Amazon EBS au lieu d'un agent.

Les méthodes de scan utilisées par Amazon Inspector dépendent du paramètre du mode de scan de votre compte. Pour plus d'informations, consultez,Gestion du mode de numérisation.

Pour activer les scans Amazon EC2, consultez. Activation d'un type de scan

Numérisation basée sur un agent

Les scans basés sur des agents sont effectués en continu à l'aide de l'agent SSM sur toutes les instances éligibles. Pour les scans basés sur des agents, Amazon Inspector utilise des associations SSM et des plug-ins installés par le biais de ces associations pour collecter l'inventaire des logiciels à partir de vos instances. Outre les analyses de vulnérabilité des packages pour les packages de système d'exploitation, l'analyse basée sur l'agent Amazon Inspector peut également détecter les vulnérabilités des packages de langage de programmation d'applications dans les instances basées sur Linux via. Inspection approfondie d'Amazon Inspector pour les instances Linux Amazon EC2

Le processus suivant explique comment Amazon Inspector utilise SSM pour collecter l'inventaire et effectuer des scans basés sur des agents :

1. Amazon Inspector crée des associations SSM dans votre compte pour collecter le stock de vos instances. Pour certains types d'instances (Windows et Linux), ces associations installent des plug-ins sur des instances individuelles afin de collecter un inventaire.
2. À l'aide de SSM, Amazon Inspector extrait l'inventaire des packages d'une instance.
3. Amazon Inspector évalue l'inventaire extrait et génère des résultats pour détecter toute vulnérabilité détectée.

Instances éligibles

Amazon Inspector utilisera la méthode basée sur un agent pour scanner une instance si elle répond aux conditions suivantes :

- L'instance possède un système d'exploitation compatible. Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez la colonne Support du scan basé sur un agent de. the section called “Systèmes d'exploitation pris en charge pour le scan Amazon EC2”
- L'instance n'est pas exclue des scans par les balises d'exclusion Amazon Inspector EC2.
- L'instance est gérée par SSM. Pour obtenir des instructions sur la vérification et la configuration de l'agent, consultezConfiguration de l'agent SSM.

Comportements de scan basés sur les agents

Lorsque vous utilisez la méthode d'analyse basée sur un agent, Amazon Inspector lance de nouvelles analyses de vulnérabilité sur les instances EC2 dans les situations suivantes :

- Lorsque vous lancez une nouvelle instance EC2.
- Lorsque vous installez un nouveau logiciel sur une instance EC2 existante (Linux et Mac).
- Lorsqu'Amazon Inspector ajoute un nouvel élément Common Vulnerabilities and Exposures (CVE) à sa base de données, et que ce CVE est pertinent pour votre instance EC2 (Linux et Mac).

Amazon Inspector met à jour le champ Dernière analyse pour une instance EC2 lorsqu'une analyse initiale est terminée. Ensuite, le champ Dernière analyse est mis à jour lorsqu'Amazon Inspector évalue l'inventaire SSM (toutes les 30 minutes par défaut) ou lorsqu'une instance est scannée à nouveau parce qu'un nouveau CVE ayant un impact sur cette instance a été ajouté à la base de données Amazon Inspector.

Vous pouvez vérifier la date à laquelle une instance EC2 a été analysée pour la dernière fois pour détecter des vulnérabilités dans l'onglet Instances de la page de gestion du compte ou en utilisant la ListCoveragecommande.

Configuration de l'agent SSM

Pour qu'Amazon Inspector puisse détecter les vulnérabilités logicielles d'une instance Amazon EC2 à l'aide de la méthode de scan basée sur les agents, l'instance doit être une instance gérée dans Amazon EC2 Systems Manager (SSM). L'agent SSM est installé et exécuté sur une instance gérée par SSM, et SSM est autorisé à gérer l'instance. Si vous utilisez déjà SSM pour gérer vos instances, aucune autre étape n'est nécessaire pour les scans basés sur des agents.

L'agent SSM est installé par défaut sur les instances EC2 créées à partir de certaines Amazon Machine Images (AMI). Pour plus d'informations, consultez la section À propos de l'agent SSM dans le guide de AWS Systems Manager l'utilisateur. Toutefois, même s'il est installé, vous devrez peut-être activer l'agent SSM manuellement et accorder à SSM l'autorisation de gérer votre instance.

La procédure suivante décrit comment configurer une instance Amazon EC2 en tant qu'instance gérée à l'aide d'un profil d'instance IAM. La procédure fournit également des liens vers des informations plus détaillées dans le guide de AWS Systems Manager l'utilisateur.

AmazonSSMManagedInstanceCoreest la politique recommandée à utiliser lorsque vous attachez un profil d'instance. Cette politique dispose de toutes les autorisations nécessaires à l'analyse par Amazon Inspector EC2.

> **Note**
>
> Vous pouvez également automatiser la gestion SSM de toutes vos instances EC2, sans utiliser de profils d'instance IAM à l'aide de la configuration de gestion d'hôte par défaut SSM. Pour de plus amples informations, consultez Gestion de l'enregistreur de configuration.

Pour configurer SSM pour une instance Amazon EC2

1. S'il n'est pas déjà installé par le fournisseur de votre système d'exploitation, installez l'agent SSM. Pour plus d'informations, consultez la section Utilisation de l'agent SSM.
2. Utilisez le AWS CLI pour vérifier que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez Vérification du statut de l'SSM Agent et démarrage de l'agent.
3. Autorisez SSM à gérer votre instance. Vous pouvez accorder une autorisation en créant un profil d'instance IAM et en l'attachant à votre instance. Nous vous recommandons d'utiliser cette AmazonSSMManagedInstanceCorepolitique, car elle dispose des autorisations nécessaires pour le distributeur SSM, l'inventaire SSM et le gestionnaire d'état SSM, dont Amazon Inspector a besoin pour les scans. Pour obtenir des instructions sur la création d'un profil d'instance avec ces autorisations et sur le rattachement à une instance, consultez la section Configurer les autorisations d'instance pour Systems Manager Systems Manager.
4. (Facultatif) Activez les mises à jour automatiques pour l'agent SSM. Pour plus d'informations, consultez Automatisation des mises à jour de l'agent SSM.
5. (Facultatif) Configurez Systems Manager pour utiliser un point de terminaison Amazon Virtual Private Cloud (Amazon VPC). Pour plus d'informations, consultez Créer des points de terminaison Amazon VPC.

> **Important**
>
> Amazon Inspector nécessite une association Systems Manager State Manager dans votre compte pour collecter l'inventaire des applications logicielles. Amazon Inspector crée automatiquement une association appelée `InspectorInventoryCollection-do-not-delete` s'il n'en existe pas déjà une.

Amazon Inspector nécessite également une synchronisation des données des ressources et en crée automatiquement une appelée `InspectorResourceDataSync-do-not-delete` s'il n'en existe pas déjà une. Pour plus d'informations, consultez la section Configuration de la synchronisation des données des ressources pour l'inventaire dans le guide de AWS Systems Manager l'utilisateur. Chaque compte peut disposer d'un nombre défini de synchronisations de données de ressources par région. Pour plus d'informations, voir Nombre maximal de synchronisations de données de ressources (Compte AWS par région) dans les points de terminaison et quotas SSM. Si vous avez atteint ce maximum, vous devrez supprimer une synchronisation des données des ressources, voir Gestion des synchronisations des données des ressources.

Ressources SSM créées pour la numérisation

Amazon Inspector a besoin d'un certain nombre de ressources SSM dans votre compte pour exécuter les scans Amazon EC2. Les ressources suivantes sont créées lorsque vous activez pour la première fois le scan Amazon Inspector EC2 :

Note

Si l'une de ces ressources SSM est supprimée alors que le scan Amazon EC2 par Amazon Inspector est activé pour votre compte, Amazon Inspector tentera de les recréer lors du prochain intervalle d'analyse.

`InspectorInventoryCollection-do-not-delete`

Il s'agit d'une association Systems Manager State Manager (SSM) qu'Amazon Inspector utilise pour collecter l'inventaire des applications logicielles à partir de vos instances Amazon EC2. Si votre compte possède déjà une association SSM pour collecter le stock`InstanceIds*`, Amazon Inspector l'utilisera au lieu de créer la sienne.

`InspectorResourceDataSync-do-not-delete`

Il s'agit d'une synchronisation des données de ressources qu'Amazon Inspector utilise pour envoyer les données d'inventaire collectées depuis vos instances Amazon EC2 vers un compartiment Amazon S3 appartenant à Amazon Inspector. Pour plus d'informations, consultez la section Configuration de la synchronisation des données des ressources pour l'inventaire dans le guide de AWS Systems Manager l'utilisateur.

`InspectorDistributor-do-not-delete`

Il s'agit d'une association SSM utilisée par Amazon Inspector pour scanner les instances Windows. Cette association installe le plug-in Amazon Inspector SSM sur vos instances Windows. Si le fichier du plugin est supprimé par inadvertance, cette association le réinstallera au prochain intervalle d'association.

`InvokeInspectorSsmPlugin-do-not-delete`

Il s'agit d'une association SSM utilisée par Amazon Inspector pour scanner les instances Windows. Cette association permet à Amazon Inspector de lancer des scans à l'aide du plugin. Vous pouvez également l'utiliser pour définir des intervalles personnalisés pour les scans des instances Windows. Pour de plus amples informations, veuillez consulter Définition de plannings personnalisés pour les scans Windows par exemple.

`InspectorLinuxDistributor-do-not-delete`

Il s'agit d'une association SSM qu'Amazon Inspector utilise pour l'inspection approfondie d'Amazon EC2 Linux. Cette association installe le plugin Amazon Inspector SSM sur vos instances Linux.

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

Il s'agit d'une association SSM utilisée par Amazon Inspector pour l'inspection approfondie d'Amazon EC2 Linux. Cette association permet à Amazon Inspector de lancer des scans à l'aide du plugin.

> **Note**
>
> Lorsque vous désactivez l'analyse ou l'inspection approfondie Amazon EC2 par Amazon Inspector, toutes les ressources SSM sont automatiquement désinstallées des hôtes Linux correspondants.

Numérisation sans agent

Amazon Inspector utilise une méthode d'analyse sans agent sur les instances éligibles lorsque votre compte est en mode de numérisation hybride (qui inclut à la fois les scans avec et sans agent). Pour les scans sans agent, Amazon Inspector utilise des instantanés EBS pour collecter un inventaire logiciel à partir de vos instances. Les instances scannées à l'aide de la méthode sans agent sont

analysées à la fois pour détecter les vulnérabilités des packages du système d'exploitation et des packages de langage de programmation d'applications.

> **Note**
>
> Lorsque vous analysez des instances Linux pour détecter les vulnérabilités des packages de langage de programmation d'applications, la méthode sans agent analyse tous les chemins disponibles, tandis que l'analyse basée sur un agent analyse uniquement les chemins par défaut et les chemins supplémentaires que vous spécifiez dans le cadre desquels vous les spécifiez. Inspection approfondie d'Amazon Inspector pour les instances Linux Amazon EC2 Cela peut entraîner des résultats différents pour la même instance selon qu'elle est scannée à l'aide de la méthode à base d'agent ou de la méthode sans agent.

Le processus suivant explique comment Amazon Inspector utilise les instantanés EBS pour collecter des stocks et effectuer des scans sans agent :

1. Amazon Inspector crée un instantané EBS de tous les volumes attachés à l'instance. Pendant qu'Amazon Inspector l'utilise, l'instantané est stocké dans votre compte et étiqueté `InspectorScan` comme clé de balise, et un identifiant de scan unique comme valeur de balise.
2. Amazon Inspector extrait les données des instantanés à l'aide des API directes d'EBS et les évalue pour détecter les vulnérabilités. Des résultats sont générés pour toutes les vulnérabilités détectées.
3. Amazon Inspector supprime les instantanés EBS qu'il a créés dans votre compte.

Instances éligibles

Amazon Inspector utilisera la méthode sans agent pour scanner une instance si elle répond aux conditions suivantes :

- L'instance possède un système d'exploitation compatible. Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez la colonne Support du scan basé sur un agent de. the section called “Systèmes d'exploitation pris en charge pour le scan Amazon EC2”
- L'instance n'est pas exclue des scans par les balises d'exclusion Amazon Inspector EC2.
- Le statut de l'instance est `Unmanaged EC2 instance`Stale `inventory`, ou`No inventory`.
- L'instance est basée sur EBS et possède l'un des formats de système de fichiers suivants :

- `ext3`
- `ext4`
- `xfs`

Comportements de scan sans agent

Lorsque votre compte est configuré pour le scan hybride, Amazon Inspector effectue des scans sans agent sur les instances éligibles toutes les 24 heures. Amazon Inspector détecte et analyse les nouvelles instances éligibles toutes les heures, y compris les nouvelles instances sans agents SSM ou les instances préexistantes dont le statut est passé à. `SSM_UNMANAGED`

Amazon Inspector met à jour le champ Dernière analyse pour une instance Amazon EC2 chaque fois qu'il analyse des instantanés extraits d'une instance après un scan sans agent.

Vous pouvez vérifier la date à laquelle une instance EC2 a été analysée pour la dernière fois pour détecter des vulnérabilités dans l'onglet Instances de la page de gestion du compte ou en utilisant la ListCoveragecommande.

Gestion du mode de numérisation

Votre mode de scan EC2 détermine les méthodes de scan qu'Amazon Inspector utilisera pour effectuer des scans EC2 sur votre compte. Vous pouvez consulter le mode de numérisation de votre compte sur la page des paramètres de numérisation EC2 sous Paramètres généraux. Les comptes autonomes ou les administrateurs délégués d'Amazon Inspector peuvent modifier le mode de numérisation. Lorsque vous définissez le mode de numérisation en tant qu'administrateur délégué d'Amazon Inspector, ce mode de numérisation est défini pour tous les comptes membres de votre organisation. Amazon Inspector propose les modes de numérisation suivants :

Analyse basée sur un agent : dans ce mode de numérisation, Amazon Inspector utilisera exclusivement la méthode de numérisation basée sur un agent pour détecter les vulnérabilités des packages. Ce mode d'analyse analyse uniquement les instances gérées par SSM dans votre compte, mais présente l'avantage de fournir des analyses continues en réponse aux nouveaux CVE ou aux modifications apportées aux instances. Le scan basé sur un agent fournit également une inspection approfondie par Amazon Inspector pour les instances éligibles. Il s'agit du mode de scan par défaut pour les comptes nouvellement activés.

Analyse hybride : dans ce mode de numérisation, Amazon Inspector utilise une combinaison de méthodes basées sur un agent et de méthodes sans agent pour détecter les vulnérabilités des

packages. Pour les instances EC2 éligibles sur lesquelles l'agent SSM est installé et configuré, Amazon Inspector utilise la méthode basée sur l'agent. Pour les instances éligibles qui ne sont pas gérées par SSM, Amazon Inspector utilisera la méthode sans agent pour les instances éligibles soutenues par EBS.

Pour modifier le mode de numérisation

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez modifier le mode de numérisation EC2.
3. Dans le panneau de navigation latéral, sous Paramètres généraux, sélectionnez Paramètres de numérisation EC2.
4. Sous Mode de numérisation, sélectionnez Modifier.
5. Choisissez un mode de numérisation, puis sélectionnez Enregistrer les modifications.

Exclure les instances des scans Amazon Inspector

Vous pouvez étiqueter certaines instances pour les exclure des scans Amazon Inspector. L'exclusion des instances des scans permet d'éviter les alertes inexploitables. Les instances exclues ne vous sont pas facturées.

Pour exclure une instance EC2 des scans, balisez cette instance avec la clé suivante :

- `InspectorEc2Exclusion`

La valeur est facultative.

Pour plus d'informations sur l'ajout de balises, consultez Marquer vos ressources Amazon EC2.

En outre, vous pouvez exclure un volume EBS chiffré des analyses sans agent en étiquetant la AWS KMS clé utilisée pour chiffrer ce volume avec cette balise. `InspectorEc2Exclusion` Pour plus d'informations, consultez la section Balisage des clés

Systèmes d'exploitation pris en charge

Amazon Inspector analyse les instances EC2 Mac, Windows et Linux prises en charge à la recherche de vulnérabilités dans les packages du système d'exploitation. Pour les instances Linux, Amazon

Inspector peut produire des résultats pour les packages de langage de programmation d'applications à l'aide deInspection approfondie d'Amazon Inspector pour les instances Linux Amazon EC2. Pour les instances Mac et Windows, seuls les packages du système d'exploitation sont analysés.

Pour plus d'informations sur les systèmes d'exploitation pris en charge, notamment sur les systèmes d'exploitation pouvant être analysés sans agent SSM, consultezSystèmes d'exploitation pris en charge pour le scan Amazon EC2.

Inspection approfondie d'Amazon Inspector pour les instances Linux Amazon EC2

Amazon Inspector étend sa couverture de numérisation Amazon EC2 pour inclure une inspection approfondie. Grâce à une inspection approfondie, Amazon Inspector détecte les vulnérabilités des packages de langage de programmation d'applications dans vos instances Amazon EC2 basées sur Linux.

Amazon Inspector analyse les chemins par défaut pour les bibliothèques de packages de langage de programmation. Vous pouvez également configurer des chemins personnalisés en plus des chemins par défaut. Pour de plus amples informations, veuillez consulter Chemins personnalisés pour l'inspection approfondie d'Amazon Inspector.

Amazon Inspector effectue des analyses d'inspection approfondies à l'aide des données collectées à l'aide du plug-in Amazon Inspector SSM. Pour gérer le plugin et effectuer une inspection approfondie pour Linux, Amazon Inspector crée automatiquement l'association SSM suivante `InvokeInspectorLinuxSsmPlugin-do-not-delete` dans votre compte. Cela se produit lorsqu'Amazon Inspector active une inspection approfondie.

Amazon Inspector collecte l'inventaire des applications mis à jour à partir des instances pour une inspection approfondie toutes les 6 heures.

Pour obtenir la liste des langages de programmation pris en charge par Amazon Inspector pour une inspection approfondie, consultezLangages de programmation pris en charge : Amazon EC2 Deep Inspection.

> **Note**
>
> L'inspection approfondie n'est pas prise en charge pour les instances Windows ou Mac.

Activation ou désactivation de l'inspection approfondie

> **Note**
>
> L'inspection approfondie est automatiquement activée dans le cadre de l'analyse Amazon EC2 pour les comptes qui activent Amazon Inspector après le 17 avril 2023.

Vous pouvez vérifier si l'inspection approfondie est active pour un compte dans la console Amazon Inspector à partir de la colonne de numérisation Amazon EC2 sur la page de gestion du compte. Si l'inspection approfondie n'est pas active, cette colonne indiquera Activé (inspection approfondie désactivée). Pour vérifier l'état d'activation par programmation, utilisez l'GetEc2DeepInspectionConfigurationAPI. Ou, pour plusieurs comptes, utilisez l'BatchGetMemberEc2DeepInspectionStatusAPI.

Si vous avez activé Amazon Inspector avant le 17 avril 2023, vous pouvez activer l'inspection approfondie via la bannière de la console ou l'UpdateEc2DeepInspectionConfigurationAPI. Si vous êtes l'administrateur délégué d'une organisation dans Amazon Inspector, vous pouvez utiliser l'BatchUpdateMemberEc2DeepInspectionStatusAPI pour l'activer pour vous-même et pour vos comptes membres.

Vous pouvez désactiver l'inspection approfondie via l'UpdateEc2DeepInspectionConfigurationAPI. Les comptes membres d'une organisation ne peuvent pas désactiver l'inspection approfondie. Le compte du membre doit plutôt être désactivé par son administrateur délégué à l'aide de l'BatchUpdateMemberEc2DeepInspectionStatusAPI.

À propos du plug-in Amazon Inspector SSM pour Linux

Amazon Inspector utilise le plug-in Amazon Inspector SSM pour effectuer une inspection approfondie de vos instances Linux. Le plugin Amazon Inspector SSM est automatiquement installé sur vos instances Linux dans le répertoire suivant :`/opt/aws/inspector/bin`. Le nom de l'exécutable est`inspectorssmplugin`.

> **Note**
>
> Amazon Inspector utilise Systems Manager Distributor pour déployer le plugin dans votre instance Amazon EC2. Systems Manager Distributor prend en charge les systèmes d'exploitation répertoriés dans la catégorie Plateformes et architectures de packages pris en charge dans le guide Systems Manager. Le système d'exploitation de votre instance Amazon

EC2 doit être pris en charge par Systems Manager Distributor et Amazon Inspector pour qu'Amazon Inspector puisse effectuer des analyses d'inspection approfondies.

Amazon Inspector crée les répertoires de fichiers suivants pour gérer les données collectées à des fins d'inspection approfondie par le plugin Amazon Inspector SSM :

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - Ce répertoire contient les chemins complets vers les packages découverts lors d'une inspection approfondie. `packages.txt` Si Amazon Inspector a détecté le même package plusieurs fois sur votre instance, ce fichier répertorie chaque emplacement où le package a été trouvé.

Amazon Inspector stocke les journaux du plugin dans le `/var/log/amazon/inspector` répertoire.

Désinstaller le plug-in Amazon Inspector SSM

Si le `inspectorssmplugin` fichier est supprimé par inadvertance, l'association `InspectorLinuxDistributor-do-not-delete` SSM essaiera de réinstaller le plug-in au prochain intervalle d'analyse.

Si vous désactivez le scan Amazon EC2, le plugin sera automatiquement désinstallé de tous les hôtes Linux.

Chemins personnalisés pour l'inspection approfondie d'Amazon Inspector

Vous pouvez configurer des chemins personnalisés pour qu'Amazon Inspector effectue une inspection approfondie de vos instances Linux Amazon EC2. Lorsque vous ajoutez un chemin personnalisé, Amazon Inspector recherche les packages dans ce répertoire et dans tous les sous-répertoires qu'il contient.

Tous les comptes peuvent définir jusqu'à 5 chemins personnalisés pour leur compte individuel. Si vous êtes l'administrateur délégué de votre organisation, vous pouvez définir 5 chemins supplémentaires qui s'appliqueront à l'ensemble de votre organisation. Cela représente un total de 10 chemins personnalisés scannés par compte au sein de l'organisation.

Amazon Inspector analyse tous les chemins personnalisés en plus des chemins par défaut suivants, qui sont analysés pour tous les comptes :

- `/usr/lib`
- `/usr/lib64`
- `/usr/local/lib`
- `/usr/local/lib64`

> **Note**
>
> Les chemins personnalisés doivent être des chemins locaux. Amazon Inspector n'analyse pas les chemins réseau mappés tels que les montages NFS (Network File System) ou les montages du système de fichiers Amazon S3.

Formatage pour les tracés personnalisés

Voici un exemple de format pour un chemin personnalisé : `/home/usr1/project01`

Vos chemins personnalisés ne peuvent pas comporter plus de 256 caractères.

Il existe une limite de 5 000 packages par instance et une durée maximale de collecte de l'inventaire des packages de 15 minutes. Nous vous recommandons d'essayer de choisir des chemins personnalisés pour éviter ces limites.

Définissez un chemin personnalisé dans la console

Console

Connectez-vous en tant qu'administrateur délégué d'Amazon Inspector et suivez les étapes ci-dessous pour ajouter des chemins personnalisés pour votre organisation.

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
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 le scan standard Lambda.
3. Dans le panneau de navigation latéral, sous Paramètres généraux, sélectionnez Paramètres de numérisation EC2.
4. Sous Chemins personnalisés pour votre propre compte, sélectionnez Modifier pour ajouter des chemins pour votre compte individuel. Si vous êtes l'administrateur délégué, vous pouvez

choisir Modifier dans le volet Chemins personnalisés pour votre organisation afin d'ajouter des chemins personnalisés pour tous les comptes de l'organisation.

5. Entrez vos chemins personnalisés dans les zones de texte.
6. Choisissez Enregistrer pour enregistrer vos chemins personnalisés. Amazon Inspector inclura ces chemins lors de sa prochaine inspection approfondie.

API

Exécutez la commande UpdateEc2DeepInspectionConfiguration. Pour `packagePaths` spécifier un tableau de chemins à scanner.

Langages de programmation pris en charge

Pour les instances Linux, l'inspection approfondie d'Amazon Inspector peut produire des résultats concernant les packages de langages de programmation d'applications, ainsi que des vulnérabilités dans les packages du système d'exploitation. Pour les instances Mac et Windows, seuls les packages du système d'exploitation sont analysés.

Pour plus d'informations sur les langages de programmation pris en charge, consultezLangages de programmation pris en charge pour l'inspection approfondie d'Amazon Inspector.

Numérisation Windows d'instances EC2 avec Amazon Inspector

> **Note**
>
> Le 31 août 2022, Amazon Inspector a étendu sa couverture de numérisation Amazon EC2 pour inclure les instances EC2 en cours d'exécution. Windows

Amazon Inspector découvre automatiquement toutes les Windows instances prises en charge et les inclut dans le scan continu sans aucune action supplémentaire. Pour plus d'informations sur les instances prises en charge, consultezSystèmes d'exploitation pris en charge pour le scan Amazon EC2.

Contrairement aux scans pour les instances basées sur Linux, Amazon Inspector exécute des Windows scans à intervalles réguliers. Windowsles instances sont initialement scannées lors de la découverte, puis scannées toutes les 6 heures. Toutefois, l'intervalle de numérisation par défaut de

6 heures est réglable. Pour de plus amples informations, veuillez consulter Définition de plannings personnalisés pour les scans Windows par exemple. Voici un aperçu de la façon dont Amazon Inspector analyse Windows les instances :

1. Lorsque le scan Amazon EC2 est activé, Amazon Inspector crée de nouvelles associations SSM pour vos Windows ressources :`InspectorDistributor-do-not-delete`, et`InspectorInventoryCollection-do-not-delete`. `InvokeInspectorSsmPlugin-do-not-delete`
2. L'association `InspectorDistributor-do-not-delete` SSM utilise le document `AWS-ConfigureAWSPackage` SSM et le package `AmazonInspector2-InspectorSsmPlugin` SSM Distributor pour installer le plug-in Amazon Inspector SSM sur vos instances. Windows Pour plus d'informations, consultez À propos du plug-in Amazon Inspector SSM pour Windows.
3. L'association `InvokeInspectorSsmPlugin-do-not-delete` SSM exécute le plug-in Amazon Inspector SSM à intervalles réguliers pour collecter les données d'instance et générer les résultats d'Amazon Inspector. Par défaut, l'intervalle est toutes les 6 heures. Toutefois, vous pouvez le personnaliser en définissant une expression cron ou une expression de taux pour l'association à l'aide de SSM. Pour plus d'informations, reportez-vous à la section Reference : Cron and rate expressions for Systems Manager dans le guide de l'AWS Systems Manager utilisateur.

> **Note**
>
> Amazon Inspector place les fichiers de définition OVAL (Open Vulnerability and Assessment Language) mis à jour dans le compartiment S3`inspector2-oval-prod-`*`REGION`*. Ce compartiment S3 contient les définitions OVAL utilisées dans les scans et ne doit pas être modifié. La modification de ce paramètre empêchera Amazon Inspector de rechercher de nouveaux CV au fur et à mesure de leur publication.

Exigences relatives au scan d'Amazon Inspector pour les Windows instances

Pour scanner une Windows instance, Amazon Inspector exige que celle-ci réponde aux critères suivants :

- L'instance est une instance gérée par SSM. Pour obtenir des instructions sur la configuration de votre instance pour la numérisation, consultezConfiguration de l'agent SSM.

- Le système d'exploitation de l'instance est l'un des systèmes Windows d'exploitation pris en charge. Pour obtenir la liste complète des systèmes d'exploitation pris en charge, consultezSystèmes d'exploitation pris en charge pour le scan Amazon EC2.
- Le plug-in Amazon Inspector SSM est installé sur l'instance. Amazon Inspector installe automatiquement le plug-in Amazon Inspector SSM pour les instances gérées lors de la découverte. Consultez la rubrique suivante pour plus de détails sur le plugin.

> **Note**
>
> Si votre hôte fonctionne dans un Amazon VPC sans accès Internet sortant, le Windows scan nécessite que votre hôte soit en mesure d'accéder aux points de terminaison Amazon S3 régionaux. Pour savoir comment configurer un point de terminaison Amazon S3 Amazon VPC, consultez la section Créer un point de terminaison de passerelle dans le guide de l'utilisateur Amazon Virtual Private Cloud. Si votre politique de point de terminaison Amazon VPC restreint l'accès aux compartiments S3 externes, vous devez spécifiquement autoriser l'accès au compartiment géré par Amazon Inspector dans votre compartiment Région AWS qui stocke les définitions OVAL utilisées pour évaluer votre instance. Ce compartiment a le format suivant :`inspector2-oval-prod-`*`REGION`*.

À propos du plug-in Amazon Inspector SSM pour Windows

Le plug-in Amazon Inspector SSM est nécessaire pour qu'Amazon Inspector puisse scanner vos Windows instances. Le plug-in Amazon Inspector SSM est automatiquement installé sur vos Windows instances dans`C:\Program Files\Amazon\Inspector`, et le fichier binaire exécutable est nommé`InspectorSsmPlugin.exe`.

Les emplacements de fichiers suivants sont créés pour stocker les données collectées par le plug-in Amazon Inspector SSM :

- `C:\ProgramData\Amazon\Inspector\Input`
- `C:\ProgramData\Amazon\Inspector\Output`
- `C:\ProgramData\Amazon\Inspector\Logs`

> **Note**
>
> Par défaut, le plug-in Amazon Inspector SSM s'exécute avec une priorité inférieure à la normale.

Désinstaller le plug-in Amazon Inspector SSM

Si le `InspectorSsmPlugin.exe` fichier est supprimé par inadvertance, l'association `InspectorDistributor-do-not-delete` SSM réinstallera le plug-in au prochain Windows intervalle d'analyse. Si vous souhaitez désinstaller le plug-in Amazon Inspector SSM, vous pouvez utiliser l'action Désinstaller du `AmazonInspector2-ConfigureInspectorSsmPlugin` document.

En outre, le plug-in Amazon Inspector SSM sera automatiquement désinstallé de tous les Windows hôtes si vous désactivez le scan Amazon EC2.

> **Note**
>
> Si vous désinstallez l'agent SSM avant de désactiver Amazon Inspector, le plug-in Amazon Inspector SSM restera sur l'Windowshôte mais n'enverra plus de données au plug-in Amazon Inspector SSM. Pour de plus amples informations, veuillez consulter Désactivation d'Amazon Inspector.

Définition de plannings personnalisés pour les scans Windows par exemple

Vous pouvez personnaliser le délai entre les scans de votre instance Windows Amazon EC2 en définissant une expression cron ou une expression de débit pour l'`InvokeInspectorSsmPlugin-do-not-delete`association à l'aide de SSM. Pour plus d'informations, reportez-vous à la section Reference : Cron and rate expressions for Systems Manager dans le guide de AWS Systems Manager l'utilisateur ou suivez les instructions suivantes.

Sélectionnez l'un des exemples de code suivants pour modifier la cadence de numérisation des Windows instances de 6 heures par défaut à 12 heures à l'aide d'une expression de débit ou d'une expression cron.

Dans les exemples suivants, vous devez utiliser le AssociationIdpour l'association nomméeInvokeInspectorSsmPlugin-do-not-delete. Vous pouvez récupérer votre AssociationIden exécutant la AWS CLI commande suivante :

```
$ aws ssm list-associations --association-filter-list
 "key=AssociationName,value=InvokeInspectorSsmPlugin-do-not-delete" --region us-east-1
```

> **Note**
>
> AssociationIdC'est régional, vous devez donc d'abord récupérer un identifiant unique pour chacun Région AWS. Vous pouvez ensuite exécuter la commande pour modifier la cadence de numérisation dans chaque région où vous souhaitez définir un calendrier de scan personnalisé pour les Windows instances.

Example rate expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "rate(12 hours)"
```

Example cron expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "cron(0 0/12 * * ? *)"
```

Numérisation d'images de conteneurs Amazon ECR avec Amazon Inspector

Amazon Inspector analyse les images des conteneurs stockées dans Amazon ECR à la recherche de vulnérabilités logicielles afin de générer des informations sur les vulnérabilités liées aux Packages. Pour plus d'informations sur les types de résultats produits pour ces problèmes, voirRecherche de types dans Amazon Inspector.

Lorsque vous activez les scans Amazon Inspector pour Amazon ECR, vous définissez Amazon Inspector comme service de numérisation préféré pour votre registre privé. Cela remplace le scan de base par défaut, qui est fourni gratuitement par Amazon ECR, par le scan amélioré, qui est fourni et facturé via Amazon Inspector.

L'analyse améliorée fournie par Amazon Inspector vous permet de bénéficier de l'analyse des vulnérabilités pour les packages de système d'exploitation et de langage de programmation au niveau du registre. Vous pouvez consulter les résultats découverts grâce à la numérisation améliorée au niveau de l'image, pour chaque couche de l'image, sur la console Amazon ECR. En outre, vous pouvez consulter et utiliser ces résultats dans d'autres services qui ne sont pas disponibles pour les résultats de numérisation de base, notamment AWS Security Hub Amazon EventBridge. Vous pouvez consulter les résultats découverts lors des scans sur la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home. Pour plus d'informations sur l'utilisation des résultats, voirGestion des résultats dans Amazon Inspector.

Pour obtenir des instructions sur l'activation des scans Amazon ECR, consultezActivation d'un type de scan.

Comportements de scan pour le scan Amazon ECR

Lorsque vous activez la numérisation ECR pour la première fois et que votre référentiel est configuré pour une numérisation continue, Amazon Inspector détecte toutes les images éligibles que vous avez envoyées dans les 30 jours ou que vous avez extraites au cours des 90 derniers jours. Amazon Inspector analyse ensuite les images détectées et définit leur statut de numérisation sur`active`. Amazon Inspector continue de surveiller les images tant qu'elles ont été envoyées ou extraites au cours des 90 derniers jours (par défaut), ou pendant la durée de nouvelle analyse ECR que vous avez configurée. Pour de plus amples informations, veuillez consulter Configuration de la durée de la nouvelle analyse ECR.

Pour une analyse continue, Amazon Inspector lance de nouvelles analyses de vulnérabilité des images de conteneurs dans les situations suivantes :

- Chaque fois qu'une nouvelle image de conteneur est envoyée.
- Chaque fois qu'Amazon Inspector ajoute un nouvel élément Common Vulnerabilities and Exposures (CVE) à sa base de données, et que ce CVE est pertinent pour cette image de conteneur (numérisation continue uniquement).

Si vous configurez votre dépôt pour la numérisation instantanée, les images ne sont numérisées que lorsque vous les envoyez.

Vous pouvez vérifier la date à laquelle une image de conteneur a été vérifiée pour la dernière fois pour détecter des vulnérabilités dans l'onglet Images du conteneur sur la page de gestion du compte,

ou en utilisant l'ListCoverageAPI. Amazon Inspector met à jour le champ Dernière numérisation d'une image Amazon ECR en réponse aux événements suivants :

- Lorsqu'Amazon Inspector effectue la numérisation initiale d'une image de conteneur.
- Lorsqu'Amazon Inspector analyse à nouveau une image de conteneur parce qu'un nouvel élément CVE (Common Vulnerabilities and Exposures) ayant un impact sur cette image de conteneur a été ajouté à la base de données Amazon Inspector.

Systèmes d'exploitation et types de supports pris en charge

Pour plus d'informations sur les systèmes d'exploitation pris en charge, consultezSystèmes d'exploitation pris en charge pour le scan Amazon ECR.

Les scans des référentiels Amazon ECR effectués par Amazon Inspector couvrent les types de supports pris en charge suivants :

- `"application/vnd.docker.distribution.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v1+prettyjws"`
- `"application/vnd.oci.image.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v2+json"`

> **Note**
>
> Les images à gratter et `DockerV2ListMediaType` les images ne sont pas prises en charge.

Configuration de l'analyse améliorée pour les référentiels Amazon ECR

Lorsque vous activez les scans Amazon Inspector pour les images de conteneurs Amazon ECR, vous modifiez le paramètre de configuration de numérisation pour votre registre privé. Le type de scan de votre registre passe du scan de base au scan amélioré fourni par Amazon Inspector. Pour plus d'informations, consultez la section Numérisation d'images dans le guide de l'utilisateur Amazon ECR.

Vous pouvez gérer les paramètres pour une analyse améliorée au niveau du référentiel dans ECR. Vous pouvez choisir une analyse continue ou une analyse instantanée pour vos référentiels. Le scan

continu inclut des scans instantanés et des rescans automatisés. La numérisation en mode push ne numérise que lorsque vous envoyez une image pour la première fois. Pour les deux options, vous pouvez affiner l'étendue de numérisation à l'aide de filtres d'inclusion. Par défaut, lorsque vous activez l'analyse améliorée pour la première fois, vos paramètres sont définis pour Analyser en continu tous les référentiels.

Pour configurer vos paramètres de numérisation améliorés

1. Ouvrez la console Amazon ECR à l'adresse https://console.aws.amazon.com/ecr/.
2. Dans le Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région contenant les référentiels que vous analysez.
3. Dans le volet de navigation, choisissez Registre privé, puis Scanning.
4. Sous Type de numérisation, assurez-vous que l'option Numérisation améliorée est sélectionnée. Si ce n'est pas le cas, sélectionnez Numérisation améliorée.

   Par défaut, l'option Analyser en continu tous les référentiels est sélectionnée, ce qui active la couverture complète du scan par Amazon Inspector pour tous les référentiels.
5. Désélectionnez Analyser en continu tous les référentiels pour filtrer ceux qui sont analysés en continu ou en mode push.

Pour plus d'informations sur la configuration des scans améliorés, consultez la section Utilisation du scan amélioré dans le guide de l'utilisateur Amazon ECR.

Configuration de la durée de la nouvelle analyse ECR

Le paramètre de durée de nouvelle analyse ECR détermine la durée pendant laquelle Amazon Inspector surveille en permanence les images des conteneurs dans les référentiels. Vous pouvez configurer la durée de nouvelle numérisation pour la date de diffusion de l'image et la date d'extraction de l'image. La durée d'analyse par défaut pour les nouveaux comptes, y compris les nouveaux comptes ajoutés à une organisation, est de 90 jours.

Durée de la date de diffusion de l'image

La durée de la date de diffusion des images détermine la durée pendant laquelle Amazon Inspector surveille en permanence les images après leur transfert vers des référentiels après la dernière date d'extraction. Les options suivantes sont disponibles sous forme de durées de nouvelle numérisation :

- 14 jours

- 30 jours
- 60 jours
- 90 jours (par défaut)
- 180 jours
- Durée de vie

Durée de la date d'extraction de l'image

La durée de la date d'extraction des images détermine la durée pendant laquelle Amazon Inspector surveille en permanence les images après la dernière date d'extraction. Les options suivantes sont disponibles sous forme de durées de nouvelle numérisation :

- 14 jours
- 30 jours
- 60 jours
- 90 jours (par défaut)
- 180 jours

Amazon Inspector continuera de surveiller et de scanner à nouveau une image tant qu'elle a été poussée ou extraite dans les délais de diffusion et d'extraction configurés. Si l'image n'a pas été envoyée ou extraite dans les délais d'envoi et d'extraction configurés, Amazon Inspector arrête de la surveiller.

> **Note**
>
> Lorsqu'Amazon Inspector arrête de surveiller une image, il définit le code d'état de numérisation de l'image sur `inactive` et le code de motif sur`expired`. Il planifie ensuite la fermeture de tous les résultats d'image associés.

Définissez la durée de la nouvelle analyse en fonction de votre environnement. Par exemple, si vous créez souvent des images, choisissez une durée de numérisation plus courte. De même, si vous utilisez des images pendant de longues périodes, choisissez une durée de numérisation plus longue.

Lorsque vous configurez la durée de la nouvelle analyse à partir d'un compte d'administrateur délégué, Amazon Inspector applique le paramètre à tous les comptes membres de l'organisation.

Pour configurer la durée de la nouvelle analyse ECR

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, choisissez Paramètres généraux, puis sélectionnez Paramètres de numérisation ECR.
3. Dans les paramètres de numérisation ECR, sous Durée de nouvelle numérisation ECR, choisissez la durée de la date de diffusion de l'image et la durée de la date d'extraction de l'image que vous souhaitez définir.
4. Choisissez Enregistrer. Vos nouveaux paramètres sont appliqués immédiatement.

> **Note**
>
> Si vous augmentez la durée de la date de diffusion, Amazon Inspector applique la modification à toutes les images activement numérisées dans des référentiels configurés pour une numérisation continue. Cependant, les images inactives restent inactives, même si vous les avez transférées pendant la nouvelle durée.

AWS Lambda Fonctions de numérisation avec Amazon Inspector

Le support des AWS Lambda fonctions d'Amazon Inspector fournit des évaluations continues et automatisées des vulnérabilités de sécurité pour les fonctions et les couches Lambda. Amazon Inspector propose deux types de numérisation pour Lambda. Ces types de scan recherchent différents types de vulnérabilités.

Numérisation standard Amazon Inspector Lambda

Il s'agit du type de scan Lambda par défaut. L'analyse standard Lambda analyse les dépendances des applications au sein d'une fonction Lambda et de ses couches pour détecter les vulnérabilités des packages. Pour de plus amples informations, veuillez consulter Numérisation standard Lambda.

Numérisation du code Lambda d'Amazon Inspector

Ce type de scan analyse le code d'application personnalisé dans vos fonctions et couches pour détecter les vulnérabilités du code. Vous pouvez activer l'analyse standard Lambda ou activer

l'analyse standard Lambda conjointement avec l'analyse du code Lambda. Pour de plus amples informations, veuillez consulter Numérisation du code Lambda d'Amazon Inspector.

Lorsque vous activez le scan Lambda, Amazon Inspector crée les canaux AWS CloudTrail liés aux services suivants dans votre compte :

- `cloudtrail:CreateServiceLinkedChannel`
- `cloudtrail:DeleteServiceLinkedChannel`

Amazon Inspector gère ces canaux et les utilise pour surveiller vos CloudTrail événements à des fins d'analyse. Pour plus d'informations sur les canaux liés à un service, voir Affichage des canaux liés à un service à CloudTrail l'aide de la CLI. AWS

> **Note**
>
> Les canaux liés aux services créés par Amazon Inspector vous permettent de voir les CloudTrail événements de votre compte comme si vous en aviez une CloudTrail trace. Toutefois, nous vous recommandons de créer les vôtres CloudTrail pour gérer les événements de votre compte.

Pour obtenir des instructions sur l'activation des scans fonctionnels Lambda, voir. Activation d'un type de scan

Comportements de scan pour l'analyse des fonctions Lambda

Lors de l'activation, Amazon Inspector analyse toutes les fonctions Lambda invoquées ou mises à jour dans votre compte au cours des 90 derniers jours. Amazon Inspector lance des analyses de vulnérabilité des fonctions Lambda dans les situations suivantes :

- Dès qu'Amazon Inspector découvre une fonction Lambda existante.
- Lorsque vous déployez une nouvelle fonction Lambda sur le service Lambda.
- Lorsque vous déployez une mise à jour du code d'application ou des dépendances d'une fonction Lambda existante ou de ses couches.
- Chaque fois qu'Amazon Inspector ajoute un nouvel élément Common Vulnerabilities and Exposures (CVE) à sa base de données, et que ce CVE est pertinent pour votre fonction.

Amazon Inspector surveille chaque fonction Lambda pendant toute sa durée de vie jusqu'à ce qu'elle soit supprimée ou exclue de l'analyse.

Vous pouvez vérifier la date à laquelle une fonction Lambda a été vérifiée pour la dernière fois pour détecter des vulnérabilités dans l'onglet Fonctions Lambda de la page de gestion du compte, ou en utilisant l'API. ListCoverage Amazon Inspector met à jour le champ Dernière analyse effectuée pour une fonction Lambda en réponse aux événements suivants :

- Lorsqu'Amazon Inspector effectue une analyse initiale d'une fonction Lambda.
- Lorsqu'une fonction Lambda est mise à jour.
- Lorsqu'Amazon Inspector réanalyse une fonction Lambda parce qu'un nouvel élément CVE impactant cette fonction a été ajouté à la base de données Amazon Inspector.

Runtimes pris en charge et fonctions éligibles

Amazon Inspector prend en charge différents environnements d'exécution pour le scan standard Lambda et le scan du code Lambda. Pour obtenir la liste des environnements d'exécution pris en charge pour chaque type de scan, reportez-vous aux sections Runtimes pris en charge : analyse standard Amazon Inspector Lambda etRuntimes pris en charge : analyse du code Lambda par Amazon Inspector.

En plus de disposer d'un environnement d'exécution compatible, une fonction Lambda doit répondre aux critères suivants pour être éligible aux scans Amazon Inspector :

- La fonction a été invoquée ou mise à jour au cours des 90 derniers jours.
- La fonction est marquée`$LATEST`.
- La fonction n'est pas exclue des scans par balises.

> **Note**
>
> Les fonctions Lambda qui n'ont pas été invoquées ou modifiées au cours des 90 derniers jours sont automatiquement exclues des scans. Amazon Inspector reprendra l'analyse d'une fonction automatiquement exclue si elle est à nouveau invoquée ou si des modifications sont apportées au code de fonction Lambda.

Numérisation standard Amazon Inspector Lambda

Le scan standard Amazon Inspector Lambda identifie les vulnérabilités logicielles dans les dépendances des packages d'applications que vous ajoutez à votre code de fonction Lambda et à vos couches. Par exemple, si votre fonction Lambda utilise une version du `python-jwt` package présentant une vulnérabilité connue, l'analyse standard Lambda générera un résultat pour cette fonction.

Si Amazon Inspector détecte une vulnérabilité dans les dépendances des packages d'applications de votre fonction Lambda, Amazon Inspector produit une recherche détaillée du type de vulnérabilité du package.

Pour obtenir des instructions sur l'activation d'un type de scan, voirActivation d'un type de scan.

> **Note**
>
> Le scan standard Lambda n'analyse pas la dépendance du AWS SDK installée par défaut dans l'environnement d'exécution Lambda. Amazon Inspector analyse uniquement les dépendances chargées avec le code de fonction ou héritées d'une couche.

> **Note**
>
> La désactivation du scan standard Amazon Inspector Lambda désactivera également le scan du code Lambda d'Amazon Inspector.

Exclusion de fonctions du scan standard Lambda

Vous pouvez étiqueter certaines fonctions pour les exclure des scans standard Amazon Inspector Lambda. L'exclusion de fonctions des scans peut aider à éviter les alertes inexploitables.

Pour exclure une fonction Lambda du scan standard Lambda, balisez la fonction avec la paire clé-valeur suivante :

- Clé : `InspectorExclusion`
- Valeur : `LambdaStandardScanning`

Pour exclure une fonction du scan standard Lambda

1. Ouvrez la console Lambda à l'adresse https://console.aws.amazon.com/lambda/.
2. Sélectionnez Fonctions.
3. Dans le tableau des fonctions, sélectionnez le nom de la fonction que vous souhaitez exclure du scan standard Amazon Inspector Lambda.
4. Sélectionnez Configuration, puis choisissez Tags dans le menu.
5. Sélectionnez Gérer les balises, puis Ajouter une nouvelle balise.
6. Dans le champ Clé`InspectorExclusion`, entrez, puis dans le champ Valeur, entrez`LambdaStandardScanning`.
7. Sélectionnez Enregistrer pour ajouter le tag et exclure votre fonction du scan standard Amazon Inspector Lambda.

Pour plus d'informations sur l'ajout de balises dans Lambda, consultez la section Utilisation de balises dans les fonctions Lambda.

Numérisation du code Lambda d'Amazon Inspector

> **Important**
>
> L'analyse de code capture des extraits de code issus des fonctions Lambda afin de mettre en évidence les vulnérabilités détectées. Ces extraits peuvent afficher des informations d'identification codées en dur ou d'autres informations sensibles en texte clair.

Le scan du code Lambda par Amazon Inspector analyse le code d'application personnalisé au sein d'une fonction Lambda pour détecter les vulnérabilités du code, conformément aux meilleures pratiques de sécurité. AWS L'analyse du code Lambda permet de détecter des défauts d'injection, des fuites de données, une cryptographie faible ou un chiffrement manquant dans votre code. Pour plus d'informations sur les régions disponibles, consultezDisponibilité des fonctionnalités propres à la région.

L'analyse standard Lambda est une fonctionnalité qui évalue les dépendances des packages d'applications utilisés dans une fonction pour détecter les vulnérabilités et les expositions courantes (CVE). Vous pouvez activer le scan de code Lambda en même temps que le scan standard Lambda.

Amazon Inspector évalue le code de votre application de fonction Lambda à l'aide d'un raisonnement automatique et d'un apprentissage automatique qui analyse le code de votre application pour vérifier sa conformité globale en matière de sécurité. Il identifie les violations des politiques et les vulnérabilités sur la base de détecteurs internes développés en collaboration avec Amazon CodeGuru. Pour obtenir la liste des détections possibles, consultez la bibliothèque de CodeGuru détecteurs.

Si Amazon Inspector détecte une vulnérabilité dans le code d'application de votre fonction Lambda, Amazon Inspector produit une recherche détaillée du type de vulnérabilité dans le code. Ce type de recherche inclut l'emplacement exact du problème dans le code, un extrait de code illustrant le problème et les solutions suggérées. La correction suggérée inclut des blocs de plug-and-play code que vous pouvez utiliser pour remplacer vos lignes de code vulnérables. Ces corrections de code suggérées sont fournies en plus des conseils généraux de correction du code pour cette constatation.

> **Important**
>
> Les suggestions de correction du code sont basées sur un raisonnement automatisé et des services d'intelligence artificielle générative, et peuvent donc ne pas fonctionner comme prévu. Vous êtes responsable des suggestions de correction du code que vous adoptez. Passez toujours en revue les suggestions de correction du code avant de les adopter. Vous devrez peut-être apporter des modifications aux suggestions de correction du code pour vous assurer que celui-ci fonctionne comme prévu. Veuillez consulter la politique en matière d'IA responsable.

Chiffrer votre code lors de la découverte d'une vulnérabilité

Les extraits de code détectés dans le cadre d'une détection de vulnérabilité au code à l'aide de l'analyse de code Lambda sont stockés par le service. CodeGuru Par défaut, une cléAWS détenue contrôlée par CodeGuru est utilisée pour chiffrer votre code, mais vous pouvez utiliser votre propre clé gérée par le client pour le chiffrement via l'API Amazon Inspector. Pour plus d'informations, consultez Chiffrement inexistant pour le code contenu dans vos résultats.

Le scan de code Lambda peut être activé conjointement avec le scan standard Lambda. Pour obtenir des instructions sur l'activation d'un type de scan, voirActivation d'un type de scan.

Exclusion de fonctions du scan de code Lambda

Vous pouvez baliser certaines fonctions pour les exclure des scans de code Lambda d'Amazon Inspector. L'exclusion de fonctions des scans peut aider à éviter les alertes inexploitables.

Pour exclure une fonction Lambda d'Amazon Inspector, les scans de code Lambda balisent la fonction avec la paire clé-valeur suivante :

- Clé : `InspectorCodeExclusion`
- Valeur : `LambdaCodeScanning`

Pour exclure une fonction de l'analyse du code Lambda

1. Connectez-vous à la console Lambda à l'adresse https://console.aws.amazon.com/lambda/.
2. Sélectionnez Fonctions.
3. Dans le tableau des fonctions, sélectionnez le nom de la fonction que vous souhaitez exclure du scan du code Lambda par Amazon Inspector.
4. Sélectionnez Configuration, puis choisissez Tags dans le menu.
5. Sélectionnez Gérer les balises, puis Ajouter une nouvelle balise.
6. Dans le champ Clé`InspectorCodeExclusion`, entrez, puis dans le champ Valeur, entrez`LambdaCodeScanning`.
7. Sélectionnez Enregistrer pour ajouter le tag et exclure votre fonction du scan du code Lambda par Amazon Inspector.

Pour plus d'informations sur l'ajout de balises dans Lambda, consultez la section Utilisation de balises dans les fonctions Lambda.

Désactivation d'un type de scan

Vous pouvez désactiver un nouveau type de scan Amazon Inspector à tout moment. Lorsque vous désactivez un type de scan, vous perdez l'accès à tous les résultats existants qui ont été produits par ce type de scan. Si vous réactivez le type de scan, vos ressources éligibles sont scannées et Amazon Inspector produira de nouvelles découvertes. Pour conserver une trace des données de vos résultats, vous pouvez exporter vos résultats avant de les désactiver. Pour de plus amples informations, veuillez consulter Exportation de rapports de résultats depuis Amazon Inspector.

Lorsque vous désactivez un type de scan, certaines modifications peuvent être apportées à ce AWS compte en fonction du type de scan désactivé. Les modifications qui se produiront lorsque vous désactiverez ces types de scan sont les suivantes :

- Scan Amazon EC2 — Lorsque vous désactivez le scan Amazon EC2 par Amazon Inspector pour un compte, les associations SSM suivantes utilisées par Amazon Inspector sont supprimées :
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`. En outre, le plug-in Amazon Inspector SSM installé via cette association est supprimé de tous vos Windows hôtes. Pour de plus amples informations, veuillez consulter WindowsInstances de numérisation.
- Numérisation Amazon ECR — Lorsque vous désactivez la numérisation d'images de conteneurs Amazon ECR pour un compte, le type de numérisation Amazon ECR pour ce compte passe de la numérisation améliorée avec Amazon Inspector à la numérisation de base avec Amazon ECR.
- Numérisation standard Lambda : lorsque vous désactivez la numérisation standard Lambda dans un compte, la numérisation de code Lambda est désactivée si la numérisation de code était également active. En outre, le canal lié au CloudTrail service créé lors de l'activation de la numérisation est supprimé.

Désactivation des scans

La désactivation de tous les types de scan pour un compte désactive Amazon Inspector pour ce compte. Région AWS Pour de plus amples informations, veuillez consulter Désactivation d'Amazon Inspector.

Pour effectuer cette procédure dans un environnement multi-comptes, suivez ces étapes lorsque vous êtes connecté en tant qu'administrateur délégué Amazon Inspector.

Console

Pour désactiver les scans

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désactiver les scans.
3. Dans le volet de navigation, sélectionnez Gestion des comptes.
4. Choisissez l'onglet Comptes pour afficher l'état de numérisation d'un compte.
5. Cochez la case de chaque compte pour lequel vous souhaitez désactiver les scans.
6. Choisissez Actions, puis, parmi les options de désactivation, sélectionnez le type de scan que vous souhaitez désactiver.
7. (Recommandé) Répétez ces étapes Région AWS pour chacune des étapes pour lesquelles vous souhaitez désactiver ce type de scan.

API

Exécutez l'opération Disable API. Dans la demande, indiquez les identifiants de compte pour lesquels vous désactivez les scans, et pour `resourceTypes` fournir un ou plusieurs des`EC2`, `ECR`LAMBDA, ou `LAMBDA_CODE` pour désactiver les scans.

Le Center for Internet Security (CIS) analyse les instances EC2

Lorsque vous activez le scan Amazon Inspector EC2 pour un compte, vous permettez à Amazon Inspector d'effectuer ou de planifier des scans CIS. Amazon Inspector CIS analyse les systèmes d'exploitation de vos instances Amazon EC2 pour vérifier s'ils sont configurés conformément aux meilleures pratiques établies par le Center for Internet Security. Le programme CIS Security Benchmarks fournit des bases de configuration conformes aux normes du secteur et les meilleures pratiques pour configurer un système en toute sécurité. Pour plus d'informations, voir Que sont les benchmarks CIS ?

Amazon Inspector effectue des analyses CIS sur les instances Amazon EC2 cibles en fonction des balises d'instance et du calendrier d'analyse que vous définissez dans une configuration de scan. Pour chaque instance ciblée, Amazon Inspector effectue une série de contrôles sur l'instance. Chaque contrôle permet d'évaluer si la configuration de votre système répond à une recommandation spécifique du CIS Benchmark. Chaque chèque possède un identifiant et un titre de contrôle CIS, qui correspondent directement à une recommandation du CIS Benchmark pour cette plate-forme. Une fois l'analyse terminée, vous pouvez consulter les résultats et voir quels contrôles votre instance a réussi, échoué ou ignorés pour ce système.

Exigences relatives aux instances EC2 pour les scans Amazon Inspector CIS

Pour exécuter un scan CIS sur votre instance, Amazon Inspector exige que l'instance réponde aux critères suivants :

- Le système d'exploitation de l'instance est l'un des systèmes d'exploitation pris en charge pour les scans CIS. Pour obtenir la liste complète des systèmes d'exploitation pris en charge, consultezSystèmes d'exploitation pris en charge : scan CIS.
- L'instance est une instance gérée par Amazon EC2 Systems Manager (SSM). Pour plus d'informations, consultez la section Utilisation de l'agent SSM.
- Le plug-in Amazon Inspector SSM est installé sur l'instance. Amazon Inspector installe automatiquement ce plugin pour les instances gérées par SSM.
- L'instance possède un profil d'instance qui autorise SSM à gérer l'instance et à Amazon Inspector pour exécuter des scans CIS pour cette instance. Pour accorder ces autorisations, associez les

ManagedCispolicy politiques AmazonInspector2FullAccess, AmazonSSM ManagedInstanceCore et AmazonInspector2 à un rôle IAM et associez ce rôle à votre instance en tant que profil d'instance. Pour obtenir des instructions sur la création et l'attachement d'un profil d'instance, consultez la section Travailler avec des rôles IAM dans le guide de l'utilisateur Amazon EC2.

> **Note**
>
> L'activation de l'inspection approfondie d'Amazon Inspector n'est plus obligatoire lors de l'exécution d'un scan CIS sur une instance. Si vous désactivez l'inspection approfondie, Amazon Inspector continue d'installer l'agent SSM, mais le plug-in ne sera plus invoqué pour exécuter une inspection approfondie. Cela signifie que l'association suivante sera présente sur votre compte :`InspectorLinuxDistributor-do-not-delete`.

Exécution de scans CIS

Vous pouvez exécuter une analyse CIS une seule fois à la demande ou sous la forme d'une analyse récurrente planifiée. Pour exécuter une analyse, vous devez d'abord créer une configuration de numérisation.

Lorsque vous créez une configuration de scan, vous spécifiez les paires clé-valeur de balise à utiliser pour cibler les instances. Si vous êtes l'administrateur délégué d'Amazon Inspector pour une organisation, vous pouvez spécifier plusieurs comptes dans la configuration de scan, et Amazon Inspector recherchera les instances avec les balises spécifiées dans chacun de ces comptes. Vous choisissez le niveau de référence CIS pour le scan. Pour chaque référence, CIS prend en charge un profil de niveau 1 et de niveau 2 conçu pour fournir des bases de référence pour les différents niveaux de sécurité requis par différents environnements.

- Niveau 1 : recommande les paramètres de sécurité de base essentiels qui peuvent être configurés sur n'importe quel système. La mise en œuvre de ces paramètres ne devrait entraîner que peu ou pas d'interruption du service. L'objectif de ces recommandations est de réduire le nombre de points d'entrée dans vos systèmes, réduisant ainsi les risques globaux de cybersécurité.
- Niveau 2 : recommande des paramètres de sécurité plus avancés pour les environnements de haute sécurité. La mise en œuvre de ces paramètres nécessite une planification et une coordination afin de minimiser le risque d'impact sur l'entreprise. L'objectif de ces recommandations est de vous aider à vous conformer à la réglementation.

Le niveau 2 étend le niveau 1. Lorsque vous choisissez le niveau 2, Amazon Inspector vérifie toutes les configurations recommandées pour les niveaux 1 et 2.

Après avoir défini les paramètres de votre analyse, vous pouvez choisir de l'exécuter sous la forme d'une analyse ponctuelle, qui s'exécute une fois la configuration terminée, ou d'une analyse récurrente. Les analyses récurrentes peuvent être effectuées tous les jours, toutes les semaines ou tous les mois, à l'heure de votre choix.

> **Tip**
>
> Nous vous recommandons de choisir le jour et l'heure les moins susceptibles d'avoir un impact sur votre système pendant l'exécution de l'analyse.

Pour créer une configuration de scan CIS

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez l' Région AWS endroit où vous souhaitez exécuter un scan CIS.
3. Dans le panneau de navigation, sous Analyses à la demande, sélectionnez Analyses CIS.
4. Choisissez Créer un nouveau scan.
    a. Entrez un nom de configuration de scan.
    b. Pour Ressource cible, entrez la clé et la valeur correspondante d'une balise sur les instances que vous souhaitez scanner. Vous pouvez spécifier un total de 25 balises à inclure dans le scan, et pour chaque clé, vous pouvez spécifier jusqu'à cinq valeurs différentes.
    c. Choisissez un niveau de référence CIS. Vous pouvez sélectionner le niveau 1 pour les configurations de sécurité de base ou le niveau 2 pour les configurations de sécurité avancées.
5. Pour les comptes Target, spécifiez les comptes à inclure dans l'analyse. Un compte autonome ou un membre d'une organisation peut sélectionner Self pour créer une configuration de numérisation pour son compte. Un administrateur délégué d'Amazon Inspector peut sélectionner Tous les comptes pour cibler tous les comptes de l'organisation, ou sélectionner Spécifier les comptes et spécifier un sous-ensemble de comptes membres à cibler. L'administrateur délégué peut saisir, à la `SELF` place d'un identifiant de compte, une configuration de scan pour son

propre compte. Pour plus d'informations, consultez Considérations relatives à la gestion des scans Amazon Inspector CIS dans une AWS organisation.

6. Choisissez un calendrier pour les scans. Choisissez entre un scan unique, qui sera exécuté dès que vous aurez fini de créer la configuration du scan, ou un scan récurrent, qui sera exécuté à l'heure planifiée que vous avez choisie jusqu'à ce qu'il soit supprimé.
7. Choisissez Créer pour terminer la création de la configuration de numérisation.

Affichage et modification des configurations de numérisation CIS

Vous pouvez consulter ou modifier vos scans précédemment planifiés à tout moment.

Pour afficher ou modifier une configuration de scan CIS

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez l' Région AWS endroit où vous avez créé votre configuration de scan CIS.
3. Dans le panneau de navigation, sous Analyses à la demande, sélectionnez Analyses CIS.
4. Choisissez Planifié pour afficher les configurations de scan programmé.
5. Sélectionnez un élément dans la colonne Nom de la configuration de numérisation pour ouvrir les détails de cette configuration de numérisation.
6. (Facultatif) Choisissez Modifier pour modifier les paramètres de cette analyse.

Afficher les résultats de vos scans CIS

Amazon Inspector crée une tâche de scan à chaque fois qu'une configuration de scan est exécutée et collecte les résultats du scan sous un identifiant de scan unique.

Les résultats du scan sont disponibles pendant 90 jours après la fin du scan. Vous pouvez afficher les résultats de l'analyse agrégés par chèque ou par ressource cible.

Résultats du scan agrégés par chèques

Les résultats de l'analyse sont regroupés en fonction de chaque contrôle individuel effectué au cours de l'analyse. Pour chaque vérification, vous obtenez un rapport indiquant le nombre de ressources transmises, échouées ou ignorées.

Résultats du scan agrégés par ressource

Les résultats de l'analyse sont regroupés en fonction de chaque ressource ciblée par la configuration de l'analyse. Pour chaque ressource, vous obtenez un rapport indiquant les vérifications qu'une ressource a été validée, a échoué ou a été ignorée pour cette ressource.

Pour afficher les résultats du scan

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez l' Région AWS endroit où vous souhaitez afficher les résultats de numérisation.
3. Dans le panneau de navigation, sous Analyses à la demande, sélectionnez Analyses CIS.
4. Sélectionnez l'ID du scan dont vous souhaitez afficher les résultats dans la colonne Scan ID.
5. Choisissez le mode d'affichage des résultats de votre scan :
    - Sélectionnez l'onglet Contrôles pour afficher les résultats de l'analyse agrégés par contrôles.
        - Pour une vérification répertoriée, sélectionnez un chiffre parmi réussi, ignoré ou échoué dans la colonne État des ressources pour ouvrir une vue des ressources filtrées en fonction de ce statut et de cette vérification.
    - Sélectionnez l'onglet Ressources numérisées pour afficher les résultats de l'analyse agrégés par ressource.
        - Sélectionnez une ressource pour ouvrir un panneau de détails répertoriant les vérifications que la ressource a réussi, échoué ou ignorées.
6. (Facultatif) Utilisez la barre de filtre dans l'une ou l'autre des vues pour affiner vos résultats.

Vous pouvez télécharger les résultats d'un scan CIS à l'aide de la console ou de l'API.

Pour télécharger les résultats du scan

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez l' Région AWS endroit où vous souhaitez afficher les résultats de numérisation.
3. Dans le panneau de navigation, sous Analyses à la demande, sélectionnez Analyses CIS.
4. Sélectionnez l'ID du scan dont vous souhaitez afficher les résultats dans la colonne Scan ID.

5. Choisissez Téléchargement. Si vous êtes l'administrateur délégué, vous pouvez choisir de télécharger les résultats pour des comptes de membres spécifiques.

Considérations relatives à la gestion des scans Amazon Inspector CIS dans une AWS organisation

Lors de l'exécution de scans CIS au sein d'une organisation, les comptes membres et les administrateurs délégués d'Amazon Inspector interagissent avec les configurations de scan CIS et analysent les résultats de différentes manières.

Lorsqu'un administrateur délégué crée une configuration de scan CIS pour tous les comptes ou une liste d'identifiants de comptes membres, l'organisation est propriétaire de cette configuration de scan. Quel que soit le compte, l'administrateur délégué actuel peut gérer les configurations de scan appartenant à l'organisation, même si elles ont été créées par un autre compte. Les configurations de scan CIS détenues par l'organisation auront un ARN qui répertorie l'ID de l'organisation en tant que propriétaire, selon le modèle :`arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId`*. L'identifiant du compte sera l'identifiant du compte de gestion des Organizations.

> **Important**
>
> Vous ne pouvez pas ajouter de balises aux configurations de scan CIS détenues par l'organisation.

Lorsqu'un administrateur délégué crée une configuration de scan et indique `SELF` qu'il s'agit du compte cible, son compte possède cette configuration de scan. Même s'ils quittent leur organisation, ils peuvent toujours gérer cette configuration de numérisation.

> **Note**
>
> Un administrateur délégué ne peut pas modifier les cibles d'une configuration de scan qui cible`SELF`.

Les configurations de scan créées par des comptes membres, des comptes autonomes ou des administrateurs délégués SELF ayant pour cible sont détenues par le compte qui les a créées. Ces configurations de scan CIS ont un ARN qui répertorie ce compte comme propriétaire selon le modèle :`arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`111122223333`*`/cis-configuration/`*`scanId`*. L'identifiant du compte sera celui qui a créé le scan.

Un compte membre d'une organisation peut créer des configurations de numérisation pour son propre compte. L'administrateur délégué peut consulter les configurations de scan créées par les membres, mais ne peut ni les modifier ni les supprimer. Si le compte d'un membre quitte l'organisation, l'administrateur délégué ne pourra plus voir les configurations de scan créées par ce compte.

L'administrateur délégué peut consulter les résultats du scan de n'importe quel compte de l'organisation, y compris ceux planifiés par les membres. Un compte membre peut consulter les résultats de toutes les analyses CIS des ressources de son compte, y compris celles planifiées par l'administrateur délégué.

Compartiments Amazon S3 appartenant à Amazon Inspector et utilisés pour les scans CIS par Amazon Inspector

Amazon Inspector prépare les fichiers de définition OVAL (Open Vulnerability and Assessment Language) mis à jour requis pour les scans CIS. Le tableau suivant répertorie tous les compartiments Amazon S3 détenus par Amazon Inspector avec des définitions OVAL prises en charge par CIS Scan. Région AWS Les compartiments doivent être autorisés dans les VPC si nécessaire.

> **Note**
>
> Les détails de chacun des compartiments Amazon S3 suivants appartenant à Amazon Inspector ne sont pas sujets à modification. Cependant, la liste peut être mise à jour pour refléter les nouveaux supports Régions AWS. Vous ne pouvez pas utiliser ces compartiments pour d'autres opérations Amazon S3 ou dans vos propres compartiments Amazon S3.

seau CIS	Région AWS
`cis-datasets-prod-arn-5908f6f`	Europe (Stockholm)

seau CIS	Région AWS
cis-datasets-prod-bah-8f88801	Moyen-Orient (Bahreïn)
cis-datasets-prod-bjs-0f40506	Chine (Beijing)
cis-datasets-prod-bom-435a167	Asie-Pacifique (Mumbai)
cis-datasets-prod-cdg-f3a9c58	Europe (Paris)
cis-datasets-prod-cgk-09eb12f	Asie-Pacifique (Jakarta)
cis-datasets-prod-cmh-63030b9	USA Est (Ohio)
cis-datasets-prod-cpt-02c5c6f	Afrique (Le Cap)
cis-datasets-prod-dub-984936f	Europe (Irlande)
cis-datasets-prod-fra-6eb96eb	Europe (Francfort)
cis-datasets-prod-gru-de69f99	Amérique du Sud (São Paulo)
cis-datasets-prod-hkg-8e30800	Asie-Pacifique (Hong Kong)
cis-datasets-prod-iad-8438411	USA Est (Virginie du Nord)
cis-datasets-prod-icn-f4eff1c	Asie-Pacifique (Séoul)
cis-datasets-prod-kix-5743b21	Asie-Pacifique (Osaka)
cis-datasets-prod-lhr-8b1fbd0	Europe (Londres)
cis-datasets-prod-mxp-7b1bbce	Europe (Milan)
cis-datasets-prod-nrt-464f684	Asie-Pacifique (Tokyo)
cis-datasets-prod-osu-5bead6f	AWS GovCloud (USA Est)
cis-datasets-prod-pdt-adadf9c	AWS GovCloud (US-Ouest)
cis-datasets-prod-pdx-acfb052	USA Ouest (Oregon)

seau CIS	Région AWS
`cis-datasets-prod-sfo-1515ba8`	USA Ouest (Californie du Nord)
`cis-datasets-prod-sin-309725b`	Asie-Pacifique (Singapour)
`cis-datasets-prod-syd-f349107`	Asie-Pacifique (Sydney)
`cis-datasets-prod-yul-5e0c95e`	Canada (Centre)
`cis-datasets-prod-zhy-5a8eacb`	Chine (Ningxia)
`cis-datasets-prod-zrh-67e0e3d`	Europe (Zurich)

Évaluation de la couverture de votre AWS environnement par Amazon Inspector

Pour vous aider à évaluer et à interpréter la couverture de votre AWS environnement par Amazon Inspector, la page de gestion des comptes de la console Amazon Inspector fournit des statistiques et des détails sur le statut de l'analyse de vos comptes et ressources par Amazon Inspector. Cette page vous permet de consulter les statistiques agrégées et d'autres données relatives à vos ressources. Vous pouvez également effectuer une analyse approfondie de la couverture d'Amazon Inspector pour des ressources individuelles et passer en revue les résultats relatifs à des ressources spécifiques. Si vous êtes l'administrateur délégué d'Amazon Inspector pour une organisation, les données incluent les statistiques et les détails de tous les comptes de votre organisation.

Pour évaluer la couverture de votre AWS environnement par Amazon Inspector

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Gestion des comptes.
3. Sur la page de gestion du compte, choisissez l'onglet correspondant à l'une des cinq vues de couverture différentes :

    - Comptes, pour une couverture au niveau du compte.
    - Instances, pour la couverture des instances Amazon Elastic Compute Cloud (Amazon EC2).
    - Référentiels, pour la couverture des référentiels Amazon Elastic Container Registry (Amazon ECR).
    - Images, pour la couverture des images de conteneurs Amazon ECR.
    - Lambda, pour la couverture des fonctions Lambda.

Les rubriques de cette section décrivent les informations fournies par chaque onglet, y compris le statut d'analyse que peut avoir une ressource individuelle.

Rubriques

- Évaluation de la couverture des images de conteneurs Amazon ECR
- Évaluation de la couverture des AWS Lambda fonctions

Évaluation de la couverture au niveau du compte

Si votre compte ne fait pas partie d'une organisation ou n'est pas le compte administrateur Amazon Inspector délégué d'une organisation, l'onglet Comptes fournit des informations sur votre compte et le statut de l'analyse des ressources de votre compte. Dans cet onglet, vous pouvez activer ou désactiver l'analyse de tous les types de ressources de votre compte ou uniquement de certains types spécifiques. Pour plus d'informations, consultez Analyse automatisée des ressources avec Amazon Inspector.

Si votre compte est le compte administrateur Amazon Inspector délégué d'une organisation, l'onglet Comptes fournit des paramètres d'activation automatique pour les comptes de votre organisation et répertorie tous les comptes de votre organisation. Pour chaque compte, la liste indique si Amazon Inspector est activé pour le compte et, dans l'affirmative, les types d'analyse des ressources activés pour le compte. En tant qu'administrateur délégué, vous pouvez utiliser cet onglet pour modifier les paramètres d'activation automatique de votre organisation. Vous pouvez également activer ou désactiver des types spécifiques d'analyse des ressources pour les comptes de membres individuels. Pour plus d'informations, consultez Activation des scans Amazon Inspector pour les comptes membres.

Évaluation de la couverture des instances Amazon EC2

L'onglet Instances affiche les instances Amazon EC2 présentes dans votre AWS environnement. Les listes sont organisées en groupes dans les onglets suivants :

- Tout : affiche toutes les instances de votre environnement. La colonne Status indique l'état d'analyse actuel d'une instance.
- Numérisation : affiche toutes les instances qu'Amazon Inspector surveille et analyse activement dans votre environnement.
- Pas de numérisation : affiche toutes les instances qu'Amazon Inspector ne surveille ni ne scanne dans votre environnement. La colonne Reason indique pourquoi Amazon Inspector ne surveille ni n'analyse une instance.

  Une instance EC2 peut apparaître dans l'onglet Non numérisée pour plusieurs raisons. Amazon Inspector utilise AWS Systems Manager (SSM) et l'agent SSM pour surveiller et analyser

automatiquement vos instances EC2 afin de détecter les vulnérabilités. Si l'agent SSM n'est pas en cours d'exécution sur une instance, si elle ne possède pas de rôle AWS Identity and Access Management (IAM) compatible avec Systems Manager ou si elle n'exécute pas de système d'exploitation ou d'architecture compatible, Amazon Inspector ne peut pas surveiller ni scanner l'instance. Pour plus d'informations, consultez Numérisation d'instances Amazon EC2.

Dans chaque onglet, la colonne Compte Compte AWS indique le propriétaire d'une instance.

Balises d'instance EC2 : cette colonne indique les balises associées à l'instance et peut être utilisée pour déterminer si votre instance a été exclue des analyses par balises.

Système d'exploitation : cette colonne indique le type de système d'exploitation, qui peut être `WINDOWS` `MACLINUX`, ou`UNKNOWN`.

Surveillé à l'aide : cette colonne indique si Amazon Inspector utilise la méthode de scan avec ou sans agent sur cette instance.

Dernière analyse : cette colonne indique la date à laquelle Amazon Inspector a vérifié pour la dernière fois la présence de vulnérabilités dans cette ressource. La fréquence à laquelle Amazon Inspector effectue des scans dépend de la méthode de scan utilisée pour scanner l'instance.

Pour consulter des informations supplémentaires sur une instance EC2, cliquez sur le lien dans la colonne instance EC2. Amazon Inspector affiche ensuite les détails de l'instance et les résultats actuels relatifs à l'instance. Pour consulter les détails d'une découverte, cliquez sur le lien dans la colonne Titre. Pour plus d'informations sur ces détails, consultezAmazon Inspector trouve des informations.

Numérisation des valeurs d'état pour les instances Amazon EC2

Pour une instance Amazon Elastic Compute Cloud (Amazon EC2), les valeurs de statut possibles sont les suivantes :

- Surveillance active : Amazon Inspector surveille et scanne en permanence l'instance.
- Instance EC2 arrêtée : Amazon Inspector a suspendu le scan de l'instance car celle-ci est dans un état arrêté. Toutes les découvertes existantes seront conservées jusqu'à la fermeture de l'instance. Si l'instance est redémarrée, Amazon Inspector reprendra automatiquement le scan de l'instance.
- Erreur interne — Une erreur interne s'est produite lorsqu'Amazon Inspector a tenté de scanner l'instance. Amazon Inspector corrigera automatiquement l'erreur et reprendra l'analyse dès que possible.

- Aucun inventaire : Amazon Inspector n'a pas trouvé l'inventaire des applications logicielles à scanner pour l'instance. Les associations Amazon Inspector associées à l'instance ont peut-être été supprimées ou elles n'ont peut-être pas pu être exécutées.

  Pour résoudre ce problème, utilisez AWS Systems Manager pour vous assurer que l'`InspectorInventoryCollection-do-not-delete`association existe et que son statut d'association est satisfaisant. Utilisez également AWS Systems Manager Fleet Manager pour vérifier l'inventaire des applications logicielles de l'instance.
- Désactivation en attente : Amazon Inspector a arrêté de scanner l'instance. L'instance est en cours de désactivation, en attendant la fin des tâches de nettoyage.
- En attente de l'analyse initiale : Amazon Inspector a mis l'instance en file d'attente pour une analyse initiale.
- Ressource interrompue : l'instance a été interrompue. Amazon Inspector nettoie actuellement les résultats et les données de couverture existants pour l'instance.
- Inventaire périmé : Amazon Inspector n'a pas été en mesure de collecter un inventaire d'applications logicielles mis à jour qui a été capturé au cours des 7 derniers jours pour l'instance.

  Pour résoudre ce problème, assurez-vous que AWS Systems Manager les associations Amazon Inspector requises existent et sont exécutées pour l'instance. Utilisez également AWS Systems Manager Fleet Manager pour vérifier l'inventaire des applications logicielles de l'instance.
- Instance EC2 non gérée : Amazon Inspector ne surveille ni ne scanne l'instance. L'instance n'est pas gérée parAWS Systems Manager.

  Pour résoudre ce problème, vous pouvez utiliser le logiciel AWSSupport-TroubleshootManagedInstance runbookfourni par AWS Systems Manager Automation. Une fois que vous avez configuré AWS Systems Manager la gestion de l'instance, Amazon Inspector commence automatiquement à surveiller et à scanner l'instance en continu.
- Système d'exploitation non pris en charge : Amazon Inspector ne surveille ni ne scanne l'instance. L'instance utilise un système d'exploitation ou une architecture non pris en charge par Amazon Inspector. Pour obtenir la liste des systèmes d'exploitation pris en charge par Amazon Inspector, consultezSystèmes d'exploitation pris en charge pour le scan Amazon EC2.
- Surveillance active avec erreurs partielles : cet état indique que le scan EC2 est actif, mais que des erreurs y sont associéesInspection approfondie d'Amazon Inspector pour les instances Linux Amazon EC2. Les erreurs d'inspection approfondies possibles sont les suivantes :
  - Limite de collecte de packages d'inspection approfondie dépassée : l'instance a dépassé la limite de 5 000 packages pour l'inspection approfondie d'Amazon Inspector. Pour reprendre

une inspection approfondie de cette instance, vous pouvez essayer d'ajuster les chemins personnalisés associés au compte.

- Dépassement de la limite d'inventaire SSM quotidienne pour une inspection approfondie : l'agent SSM n'a pas pu envoyer de stock à Amazon Inspector car le quota SSM pour les données d'inventaire collectées par instance et par jour a déjà été atteint pour cette instance. Pour plus d'informations, consultez la section Points de terminaison et quotas Amazon EC2 Systems Manager.
- Dépassement du délai de collecte pour inspection approfondie : Amazon Inspector n'a pas réussi à extraire l'inventaire des colis car le temps de collecte des colis a dépassé le seuil maximum de 15 minutes.
- L'inspection approfondie n'a aucun inventaire — Le plugin Amazon Inspector SSM n'a pas encore été en mesure de collecter un inventaire des packages pour cette instance. Cela est généralement dû à une analyse en attente. Toutefois, si cet état persiste après 6 heures, utilisez Amazon EC2 Systems Manager pour vous assurer que les associations Amazon Inspector requises existent et sont exécutées pour l'instance.

Pour plus de détails sur la configuration des paramètres de numérisation pour une instance EC2, consultezNumérisation d'instances Amazon EC2.

Évaluation de la couverture des référentiels Amazon ECR

L'onglet Référentiels affiche les référentiels Amazon ECR de votre environnement. AWS Les listes sont organisées en groupes dans les onglets suivants :

- Tout : affiche tous les référentiels de votre environnement. La colonne État indique l'état d'analyse actuel d'un référentiel.
- Activé : affiche tous les référentiels qu'Amazon Inspector est configuré pour surveiller et analyser dans votre environnement. La colonne État indique l'état d'analyse actuel d'un référentiel.
- Non activé : affiche tous les référentiels qu'Amazon Inspector ne surveille ni n'analyse dans votre environnement. La colonne Reason indique pourquoi Amazon Inspector ne surveille ni n'analyse un référentiel.

Dans chaque onglet, la colonne Compte Compte AWS indique le propriétaire d'un référentiel.

Pour consulter des informations supplémentaires sur un dépôt, choisissez le nom du dépôt. Amazon Inspector affiche ensuite une liste des images du conteneur dans le référentiel ainsi que les détails de

chaque image. Les détails incluent la balise d'image, le résumé de l'image et l'état de numérisation. Ils incluent également des statistiques de recherche clés, telles que le nombre de résultats critiques pour l'image. Pour effectuer une recherche détaillée et consulter les données nécessaires à la recherche de statistiques, choisissez la balise d'image associée à l'image.

Numérisation des valeurs d'état pour les référentiels Amazon ECR

Pour un référentiel Amazon Elastic Container Registry (Amazon ECR), les valeurs de statut possibles sont les suivantes :

- Activé (continu) — Pour un référentiel, Amazon Inspector surveille en permanence les images de ce référentiel. Le paramètre de numérisation amélioré pour le référentiel est défini sur une analyse continue. Amazon Inspector scanne initialement les nouvelles images lorsqu'elles sont envoyées et les analyse à nouveau si un nouveau CVE correspondant à cette image est publié. Amazon Inspector continuera de surveiller les images de ce référentiel pendant la durée de scan ECR que vous avez configurée.
- Activé (en mode push) : Amazon Inspector scanne automatiquement chaque image de conteneur dans le référentiel lorsqu'une nouvelle image est envoyée. L'analyse améliorée est activée pour le référentiel et configurée pour numériser en mode push.
- Accès refusé : Amazon Inspector n'est pas autorisé à accéder au référentiel ni à aucune image de conteneur du référentiel.

  Pour résoudre ce problème, assurez-vous que les politiques AWS Identity and Access Management (IAM) du référentiel autorisent Amazon Inspector à accéder au référentiel.
- Désactivé (manuel) — Amazon Inspector ne surveille ni ne scanne aucune image de conteneur dans le référentiel. Le paramètre d'analyse Amazon ECR pour le référentiel est défini sur une analyse manuelle de base.

  Pour commencer à numériser des images du référentiel avec Amazon Inspector, modifiez le paramètre de numérisation du référentiel en mode de numérisation améliorée, puis choisissez de numériser les images en continu ou uniquement lorsqu'une nouvelle image est envoyée.
- Activé (en mode push) : Amazon Inspector scanne automatiquement chaque image de conteneur dans le référentiel lorsqu'une nouvelle image est envoyée. Le paramètre de numérisation amélioré pour le référentiel est configuré pour scanner en mode push.
- Erreur interne — Une erreur interne s'est produite lorsqu'Amazon Inspector a tenté de scanner le référentiel. Amazon Inspector corrigera automatiquement l'erreur et reprendra l'analyse dès que possible.

Pour plus de détails sur la configuration des paramètres de numérisation pour les référentiels. Numérisation d'images de conteneurs Amazon ECR

Évaluation de la couverture des images de conteneurs Amazon ECR

L'onglet Images affiche les images des conteneurs Amazon ECR de votre AWS environnement. Les listes sont organisées en groupes dans les onglets suivants :

- Tout : affiche toutes les images de conteneurs de votre environnement. La colonne État indique l'état actuel de numérisation d'une image.
- Numérisation : affiche toutes les images de conteneurs qu'Amazon Inspector est configuré pour surveiller et scanner dans votre environnement. La colonne État indique l'état actuel de numérisation d'une image.
- Pas de numérisation : affiche toutes les images de conteneurs qu'Amazon Inspector ne surveille pas et ne scanne pas dans votre environnement. La colonne Reason indique pourquoi Amazon Inspector ne surveille ni ne scanne une image.

  Une image de conteneur peut apparaître dans l'onglet Non activé pour plusieurs raisons. L'image peut être stockée dans un référentiel pour lequel les scans d'Amazon Inspector ne sont pas activés, ou les règles de filtrage Amazon ECR empêchent la numérisation de ce référentiel. Ou bien l'image n'a pas été poussée ou extraite pendant le nombre de jours que vous avez configuré pour la durée de la nouvelle numérisation ECR. Pour plus d'informations, consultez Configuration de la durée de la nouvelle analyse ECR.

Dans chaque onglet, la colonne Nom du référentiel indique le nom du référentiel qui stocke une image de conteneur. La colonne Compte Compte AWS indique le propriétaire du référentiel. La colonne Dernière analyse indique la date à laquelle Amazon Inspector a vérifié pour la dernière fois la présence de vulnérabilités dans cette ressource. Cela peut inclure des vérifications en cas de mise à jour de la recherche de métadonnées, de mise à jour de l'inventaire des applications de la ressource ou d'une nouvelle analyse en réponse à un nouveau CVE. Pour plus d'informations, consultez Comportements de scan pour le scan Amazon ECR.

Pour consulter des informations supplémentaires sur une image de conteneur, cliquez sur le lien dans la colonne d'image de conteneur ECR. Amazon Inspector affiche ensuite les détails de l'image et les résultats actuels relatifs à l'image. Pour consulter les détails d'une découverte, cliquez sur le

lien dans la colonne Titre. Pour plus d'informations sur ces détails, consultezAmazon Inspector trouve des informations.

Valeurs d'état de numérisation pour les images de conteneurs Amazon ECR

Pour une image de conteneur Amazon Elastic Container Registry, les valeurs de statut possibles sont les suivantes :

- Surveillance active (continue) : Amazon Inspector effectue une surveillance continue et l'image ainsi que les nouvelles numérisations y sont effectuées chaque fois qu'un nouveau CVE pertinent est publié. La durée de réanalyse Amazon ECR pour l'image est actualisée chaque fois que l'image est poussée ou extraite. La numérisation améliorée est activée pour le référentiel qui stocke l'image, et le paramètre de numérisation amélioré pour le référentiel est défini sur une numérisation continue.
- Activé (en mode push) : Amazon Inspector scanne automatiquement l'image chaque fois qu'une nouvelle image est envoyée. La numérisation améliorée est activée pour le référentiel qui stocke l'image, et le paramètre de numérisation amélioré pour le référentiel est défini pour numériser en mode push.
- Erreur interne — Une erreur interne s'est produite lorsqu'Amazon Inspector a tenté de scanner l'image du conteneur. Amazon Inspector corrigera automatiquement l'erreur et reprendra l'analyse dès que possible.
- En attente de la numérisation initiale : Amazon Inspector a mis l'image en file d'attente pour une première numérisation.
- L'éligibilité à la numérisation a expiré (en continu) — Amazon Inspector a suspendu la numérisation de l'image. L'image n'a pas été mise à jour pendant la durée que vous avez spécifiée pour les nouvelles numérisations automatiques des images dans le référentiel. Vous pouvez appuyer ou tirer l'image pour reprendre la numérisation.
- L'éligibilité à la numérisation a expiré (On push) — Amazon Inspector a suspendu la numérisation de l'image. L'image n'a pas été mise à jour pendant la durée que vous avez spécifiée pour les nouvelles numérisations automatiques des images dans le référentiel. Vous pouvez appuyer sur l'image pour reprendre la numérisation.
- Manuel de fréquence de numérisation (manuel) — Amazon Inspector ne scanne pas l'image du conteneur Amazon ECR. Le paramètre de numérisation Amazon ECR pour le référentiel qui stocke l'image est défini sur une numérisation manuelle de base. Pour commencer à numériser l'image automatiquement avec Amazon Inspector, modifiez le paramètre du référentiel pour une

numérisation améliorée, puis choisissez de numériser les images en continu ou uniquement lorsqu'une nouvelle image est envoyée.

- Système d'exploitation non pris en charge : Amazon Inspector ne surveille ni ne scanne l'image. L'image est basée sur un système d'exploitation non pris en charge par Amazon Inspector ou utilise un type de support non pris en charge par Amazon Inspector.

  Pour obtenir la liste des systèmes d'exploitation pris en charge par Amazon Inspector, consultezSystèmes d'exploitation pris en charge pour le scan Amazon ECR. Pour obtenir la liste des types de médias pris en charge par Amazon Inspector, consultez la section Types de médias pris en charge.

Pour plus de détails sur la configuration des paramètres de numérisation pour les référentiels et les images, consultezNumérisation d'images de conteneurs Amazon ECR.

Évaluation de la couverture des AWS Lambda fonctions

L'onglet Lambda affiche les fonctions Lambda de votre environnement. AWS Cette page contient deux tableaux, l'un présentant les détails de la couverture des fonctions pour le scan standard Lambda et l'autre pour le scan du code Lambda. Vous pouvez regrouper les fonctions en fonction des onglets suivants :

- Tout — Affiche toutes les fonctions Lambda de votre environnement. La colonne Status indique l'état actuel du scan pour une fonction Lambda.
- Numérisation : affiche les fonctions Lambda pour lesquelles Amazon Inspector est configuré pour scanner. La colonne Status indique l'état actuel du scan pour chaque fonction Lambda.
- Pas de numérisation : affiche les fonctions Lambda pour lesquelles Amazon Inspector n'est pas configuré pour analyser. La colonne Reason indique pourquoi Amazon Inspector ne surveille ni n'analyse une fonction.

  Une fonction Lambda peut apparaître dans l'onglet Ne pas scanner pour plusieurs raisons. La fonction Lambda peut appartenir à un compte qui n'a pas été ajouté à Amazon Inspector ou les règles de filtrage empêchent l'analyse de cette fonction. Pour plus d'informations, consultez AWS Lambda Fonctions de numérisation.

Dans chaque onglet, la colonne Nom de la fonction indique le nom de la fonction Lambda. La colonne Compte Compte AWS indique le propriétaire de la fonction. Runtime spécifie le temps d'exécution

de la fonction. La colonne Status indique l'état actuel du scan pour chaque fonction Lambda. Les balises de ressources indiquent les balises qui ont été appliquées à la fonction. La colonne Dernière analyse indique la date à laquelle Amazon Inspector a vérifié pour la dernière fois la présence de vulnérabilités dans cette ressource. Cela peut inclure des vérifications en cas de mise à jour de la recherche de métadonnées, de mise à jour de l'inventaire des applications de la ressource ou d'une nouvelle analyse en réponse à un nouveau CVE. Pour plus d'informations, consultez Comportements de scan pour l'analyse des fonctions Lambda.

Numérisation des valeurs d'état des AWS Lambda fonctions

Pour une fonction Lambda, les valeurs d'état possibles sont les suivantes :

- Surveillance active : Amazon Inspector surveille et analyse en permanence les fonctions Lambda. L'analyse continue inclut une analyse initiale des nouvelles fonctions lorsqu'elles sont transférées vers le référentiel et une nouvelle analyse automatique des fonctions lorsqu'elles sont mises à jour ou lorsque de nouvelles vulnérabilités et expositions communes (CVE) sont publiées.
- Exclu par balise : Amazon Inspector n'analyse pas cette fonction car elle a été exclue des analyses par balises.
- L'éligibilité au scan a expiré — Amazon Inspector ne surveille pas cette fonction car 90 jours ou plus se sont écoulés depuis sa dernière utilisation ou mise à jour.
- Erreur interne : une erreur interne s'est produite lorsqu'Amazon Inspector a tenté de scanner la fonction. Amazon Inspector corrigera automatiquement l'erreur et reprendra l'analyse dès que possible.
- En attente de l'analyse initiale : Amazon Inspector a mis en file d'attente la fonction pour une analyse initiale.
- Non pris en charge : le runtime de la fonction Lambda n'est pas pris en charge.

Gestion de plusieurs comptes dans Amazon Inspector with Organizations

Vous pouvez utiliser Amazon Inspector pour gérer plusieurs comptes associés via AWSOrganizations. Pour gérer plusieurs comptes Amazon Inspector, le compte de gestion Organizations désigne un compte au sein de l'organisation en tant que compte d'administrateur délégué pour Amazon Inspector. L'administrateur délégué gère Amazon Inspector pour l'organisation et dispose d'autorisations spéciales lui permettant d'effectuer des tâches au nom de votre organisation. Ces tâches incluent l'activation ou la désactivation des scans des comptes des membres, l'affichage des données de recherche agrégées provenant de l'ensemble de l'organisation, ainsi que la création et la gestion de règles de suppression.

> **Note**
>
> Pour activer Amazon Inspector par programmation pour plusieurs comptesRégions AWS, vous pouvez utiliser un script shell développé par Amazon Inspector. Pour plus d'informations sur l'utilisation de ce script, consultez inspector2- enablement-with-cli sur le GitHub site Web.

Rubriques

- Comprendre la relation entre les comptes d'administrateur et de membre dans Amazon Inspector
- Désignation d'un administrateur délégué pour Amazon Inspector

Comprendre la relation entre les comptes d'administrateur et de membre dans Amazon Inspector

Lorsque vous utilisez Amazon Inspector dans un environnement à comptes multiples, le compte d'administrateur délégué Amazon Inspector a accès à certaines métadonnées. Ces métadonnées incluent les données de configuration Amazon EC2 et Amazon ECR ainsi que les résultats des constatations de sécurité pour les comptes des membres. Le compte administrateur peut également créer des règles de suppression des recherches appliquées aux comptes des membres. Pour plus d'informations, consultez Suppression des résultats d'Amazon Inspector à l'aide de règles de suppression.

Actions d'administrateur déléguées

Généralement, lorsque l'administrateur délégué applique des paramètres à son compte, ces paramètres sont appliqués à tous les autres comptes de l'organisation. L'administrateur délégué peut également consulter et récupérer des informations pour son propre compte et pour tout membre associé. Un compte d'administrateur délégué Amazon Inspector peut effectuer les actions suivantes :

- Consultez et gérez le statut d'Amazon Inspector pour les comptes associés, notamment en activant et en désactivant Amazon Inspector.
- Activez ou désactivez les types de numérisation pour tous les comptes membres de l'organisation.
- Consultez les données de recherche agrégées au sein de l'organisation et les informations de recherche pour tous les comptes membres de l'organisation.
- Créez et gérez des règles de suppression qui s'appliquent aux résultats de tous les comptes de l'organisation.
- Activez le scan amélioré Amazon ECR pour tous les membres de l'organisation.
- Consultez la couverture des ressources pour l'ensemble de l'organisation.
- Définissez la durée des nouvelles analyses automatisées des images des conteneurs ECR pour tous les comptes membres de l'organisation. Le paramètre de durée de scan de l'administrateur délégué remplace tous les paramètres précédemment définis par le compte membre. Tous les comptes de l'organisation partagent la durée de réanalyse automatique Amazon ECR des administrateurs délégués. Vous ne pouvez pas définir des durées de nouvelle analyse différentes pour des comptes individuels.
- Spécifiez cinq chemins personnalisés pour l'inspection approfondie d'Amazon Inspector pour Amazon EC2 qui seront utilisés sur tous les comptes de l'organisation. Cela s'ajoute aux cinq chemins personnalisés qu'un administrateur délégué peut définir pour son compte individuel. Pour plus d'informations sur la configuration de chemins personnalisés d'inspection approfondie, consultezChemins personnalisés pour l'inspection approfondie d'Amazon Inspector.
- Activez et désactivez l'inspection approfondie d'Amazon Inspector pour les comptes des membres.
- Exportez les SBOM pour tous les comptes membres de l'organisation.
- Définissez le mode de scan Amazon EC2 pour tous les comptes membres de l'organisation. Pour plus d'informations, consultez Gestion du mode de numérisation.
- Créez et gérez les configurations de scan CIS pour tous les comptes de l'organisation, à l'exception des configurations de scan créées par les comptes membres.

> **Note**
>
> Si le compte d'un membre quitte l'organisation, l'administrateur délégué ne pourra plus voir les configurations de scan planifiées par ce compte.

- Consultez les résultats du scan CIS pour tous les comptes de l'organisation.

Actions relatives aux comptes des membres

Un compte membre peut consulter et récupérer des informations sur son compte dans Amazon Inspector, tandis que les paramètres de son compte sont gérés par l'administrateur délégué. Les comptes membres d'une organisation peuvent effectuer les actions suivantes dans Amazon Inspector :

- Activez Amazon Inspector pour leur propre compte.
- Consultez la couverture des ressources pour leur propre compte.
- Afficher le détail des résultats pour leur propre compte.
- Consultez le paramètre de durée de numérisation automatique de l'image du conteneur ECR pour leur propre compte.
- Spécifiez cinq chemins personnalisés pour l'inspection approfondie d'Amazon Inspector pour EC2 qui seront utilisés pour leur compte individuel. Ces chemins sont analysés en plus des chemins personnalisés que l'administrateur délégué a spécifiés pour l'organisation. Pour plus d'informations sur la configuration des chemins d'inspection approfondie, consultezChemins personnalisés pour l'inspection approfondie d'Amazon Inspector.
- Consultez les chemins personnalisés définis par votre administrateur délégué pour l'inspection approfondie d'Amazon Inspector.
- Exportez les SBOM pour toutes les ressources associées à leur compte.
- Consultez le mode de numérisation de leur compte.
- Créez et gérez les configurations de scan CIS pour leur compte.
- Consultez les résultats de toutes les analyses CIS des ressources de leur compte, y compris celles planifiées par l'administrateur délégué.

> **Note**
>
> Après activation, Amazon Inspector ne peut être désactivé que par un compte d'administrateur délégué.

Désignation d'un administrateur délégué pour Amazon Inspector

Considérations importantes pour les administrateurs délégués

Prenez note des facteurs suivants qui définissent le mode de fonctionnement de l'administrateur délégué dans Amazon Inspector :

Un administrateur délégué peut gérer un maximum de 5 000 membres.

Chaque administrateur délégué Amazon Inspector dispose d'un quota de 5 000 comptes membres. Toutefois, votre organisation peut inclure plus de 5 000 comptes. Si vous dépassez les 5 000 comptes membres, vous recevrez une notification via le Amazon CloudWatch Personal Health Dashboard et un e-mail envoyé au compte administrateur délégué.

Un administrateur délégué est régional.

Contrairement à Amazon InspectorAWS Organizations, c'est un service régional. Cela signifie que vous devez désigner un administrateur délégué, ajouter des comptes membres et activer les types de scan dans chacun des domaines dans lesquels Région AWS vous souhaitez utiliser Amazon Inspector.

Une organisation ne peut avoir qu'un seul administrateur délégué.

Vous ne pouvez avoir qu'un seul administrateur délégué pour Amazon Inspector par organisation. Si vous avez désigné un compte en tant qu'administrateur délégué dans une région, ce compte doit être votre administrateur délégué dans toutes les autres régions.

Le changement d'administrateur délégué ne désactive pas Amazon Inspector pour les comptes des membres.

Si vous supprimez l'administrateur délégué, Amazon Inspector ne sera pas désactivé dans ces comptes et les paramètres de scan ne seront pas affectés.

Toutes les fonctionnalités de votre AWS organisation doivent être activées.

Il s'agit du paramètre par défaut pourAWS Organizations. S'il n'est pas activé, consultez la section Activation de toutes les fonctionnalités de votre organisation.

Autorisations requises pour désigner un administrateur délégué

Vous devez être autorisé à activer Amazon Inspector et à désigner un administrateur délégué Amazon Inspector.

Ajoutez l'instruction suivante à la fin d'une politique IAM pour accorder ces autorisations.

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Désignation d'un administrateur délégué pour votre organisation AWS

La procédure suivante explique comment désigner un administrateur délégué pour votre AWS organisation. Lorsque cette désignation est terminée, Amazon Inspector est activé à la fois pour le compte de gestion des Organizations et pour le compte d'administrateur délégué choisi.

> **Note**
>
> Seul le compte de gestion des Organizations peut désigner un administrateur délégué.

L'activation d'Amazon Inspector pour la première fois crée le rôle lié au service (SLR) `AWSServiceRoleForAmazonInspector` pour le compte. Pour plus d'informations sur la manière dont Amazon Inspector utilise les rôles liés à un service, consultez. Utilisation de rôles liés à un service pour Amazon Inspector Pour plus d'informations sur les rôles liés à un service en général, consultez la section Utilisation des rôles liés à un service dans le guide de l'utilisateur IAM.

Pour désigner un administrateur délégué pour Amazon Inspector

Console

Désignez un administrateur délégué dans la console

1. Connectez-vous à la AWS Management Console à l'aide du compte de gestion AWS Organizations.
2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home, puis utilisez le Région AWS sélecteur en haut à droite pour spécifier la région dans laquelle vous souhaitez désigner un administrateur.
3. Dans le volet Administrateur délégué, entrez l'identifiant de compte à douze chiffres du compte Compte AWS que vous souhaitez désigner comme administrateur délégué Amazon Inspector pour votre organisation. Choisissez ensuite Administration déléguée.
4. (Recommandé) Répétez les étapes précédentes pour chacune d'entre ellesRégion AWS.

API

Désignez un administrateur délégué à l'aide de l'API

- Exécutez l'opération d'EnableDelegatedAdminAccountAPI en utilisant les informations d'identification Compte AWS du compte de gestion des Organizations. Vous pouvez également utiliser le AWS Command Line Interface pour ce faire en exécutant la commande CLI suivante :`aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 11111111111`.

  > **Note**
  >
  > Assurez-vous de spécifier l'identifiant du compte que vous souhaitez définir comme administrateur délégué d'Amazon Inspector.

Après avoir spécifié l'administrateur délégué, vous devez utiliser le compte AWS Organizations de gestion uniquement pour modifier ou supprimer le compte d'administrateur délégué.

Activation des scans Amazon Inspector pour les comptes membres

En tant qu'administrateur délégué de votre organisation, vous pouvez activer le scan Amazon EC2, le scan Amazon ECR, ou les deux, pour tout membre associé au AWS Organizations compte de gestion. Lorsque vous activez les scans pour un compte membre, ce compte est associé à l'administrateur délégué, Amazon Inspector est automatiquement activé et les scans du type choisi démarrent immédiatement. Pour plus d'informations sur les ressources pouvant être analysées et sur la manière de configurer les analyses, consultezAnalyse automatisée des ressources avec Amazon Inspector.

Amazon Inspector propose plusieurs options pour gérer et activer les scans des comptes membres, notamment en autorisant les comptes membres à activer Amazon Inspector. Utilisez l'une des options suivantes pour lancer les scans de vos comptes membres.

Pour activer automatiquement le scan de tous les comptes membres

1. Connectez-vous au compte d'administrateur délégué.
2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home. Utilisez ensuite le Région AWS sélecteur en haut à droite pour spécifier la région dans laquelle vous souhaitez activer le scan de tous les comptes membres.
3. Dans le volet de navigation, sous Paramètres, choisissez Gestion du compte. Le tableau des comptes affiche tous les comptes membres associés au compte AWS Organizations de gestion.
4. Cochez la case en haut du tableau pour sélectionner tous les comptes de cette page. Choisissez ensuite Activer et sélectionnez l'option de type de numérisation de votre choix dans le menu.

   > **Note**
   >
   > Seuls les comptes actuellement visibles sur la page sont sélectionnés. Si vous avez plusieurs pages de comptes, vous devez répéter ce processus sur chaque page. Pour modifier le nombre de comptes affichés sur la page, sélectionnez l'icône représentant une roue dentée.

5. Activez le paramètre Activation automatique de l'Inspecteur pour les nouveaux comptes membres, puis sélectionnez les types de scan pour activer les nouveaux membres ajoutés à votre organisation.
6. (Recommandé) Répétez ces étapes dans chaque région où vous souhaitez scanner les comptes des membres.

Le paramètre Activer automatiquement l'inspecteur pour les nouveaux comptes membres active Amazon Inspector pour tous les futurs membres de votre organisation. Cela permet à votre administrateur délégué Amazon Inspector de gérer tous les nouveaux membres ajoutés à l'organisation. Lorsque le nombre de comptes membres atteint le quota de 5 000, ce paramètre est automatiquement désactivé. Si un compte est supprimé et que le nombre total de membres diminue à moins de 5 000, le paramètre est automatiquement réactivé.

Pour activer les comptes des membres de manière sélective

1. Connectez-vous au compte d'administrateur délégué.
2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home, puis utilisez le Région AWS sélecteur en haut à droite pour spécifier la région dans laquelle vous souhaitez activer le scan de certains comptes membres.
3. Dans le volet de navigation, sous Paramètres, choisissez Gestion du compte. Le tableau des comptes affiche tous les comptes membres associés au compte AWS Organizations de gestion.
4. Sur la page Gestion du compte, cochez la case correspondant à chaque compte membre pour lequel vous souhaitez activer le scan.
5. Sélectionnez Activer.
6. Dans le menu Activer, choisissez les types de scan à activer pour les comptes sélectionnés. Vous pouvez choisir l'une des options de numérisation suivantes :
   - Tous les scans : pour activer tous les types de numérisation.
   - Scan EC2 : pour activer les scans des instances Amazon EC2.
   - Numérisation de conteneurs ECR : pour activer la numérisation d'images de conteneurs ECR.
   - AWS Lambdaanalyse standard : pour activer les analyses des fonctions Lambda.
7. (Recommandé) Répétez ces étapes dans chaque région dans laquelle vous souhaitez activer les scans pour certains membres.

Si votre compte AWS Organizations de gestion a délégué un administrateur pour Amazon Inspector, vous pouvez activer votre propre compte en tant que membre et consulter les détails du scan de votre propre compte.

Pour activer le scan en tant que compte membre

1. Connectez-vous à votre compte.

2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home, puis utilisez le Région AWS sélecteur en haut à droite pour spécifier la région dans laquelle vous souhaitez activer le scan.
3. Dans le volet de navigation, sous Paramètres, choisissez Gestion du compte.
4. Sur la page Gestion du compte, cochez la case correspondant à votre compte.
5. Dans le menu Activer, choisissez les types de numérisation à activer. Vous pouvez choisir l'une des options de numérisation suivantes :
   - Tous les scans : pour activer tous les types de numérisation.
   - Scan EC2 : pour activer les scans des instances Amazon EC2.
   - Numérisation de conteneurs ECR : pour activer la numérisation d'images de conteneurs ECR.
   - AWS Lambdaanalyse standard : pour activer les analyses des fonctions Lambda.
6. (Recommandé) Répétez ces étapes dans chaque région dans laquelle vous souhaitez activer les scans.

Dissociation des comptes membres dans Amazon Inspector

La procédure suivante indique comment dissocier les comptes des membres. Les comptes de membres dissociés restent dans votre AWS Organizations organisation en tant que comptes Amazon Inspector autonomes. L'administrateur délégué d'Amazon Inspector n'est plus autorisé à activer et à gérer Amazon Inspector pour ces comptes. Vous pourrez ajouter à nouveau des comptes dissociés en tant que membres ultérieurement.

> **Note**
>
> La dissociation d'un compte ne désactive pas les scans effectués par Amazon Inspector pour ce compte.

Console

Pour dissocier les comptes des membres à l'aide de la console

1. Connectez-vous au compte d'administrateur délégué.

2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home, puis utilisez le Région AWS sélecteur en haut à droite pour spécifier la région dans laquelle vous souhaitez dissocier un ou plusieurs comptes membres.
3. Dans le volet de navigation, sous Paramètres, choisissez Gestion du compte.
4. Sur la page Gestion du compte, cochez la case correspondant à chaque compte que vous souhaitez dissocier.
5. Dans le menu Actions, choisissez Dissocier le compte.
6. (Recommandé) Répétez ces étapes dans chaque région dans laquelle vous souhaitez dissocier les comptes.

API

Pour dissocier les comptes des membres à l'aide de l'API

Exécutez l'opération DisassociateMember API. Dans la demande, indiquez les identifiants de compte que vous souhaitez dissocier.

Supprimer un administrateur délégué Amazon Inspector

Si vous devez désigner un nouvel administrateur délégué Amazon Inspector, vous pouvez supprimer un administrateur délégué existant en tant que compte de AWS Organizations gestion.

Lorsque vous supprimez un administrateur délégué, cela ne désactive pas Amazon Inspector dans ce compte ni dans les comptes des membres de l'organisation. Les comptes de votre organisation sont convertis en comptes autonomes et conservent les paramètres de numérisation qu'ils avaient avant d'être gérés par un administrateur délégué.

Pour supprimer l'administrateur délégué

1. Connectez-vous à l'AWS Management Consoleaide du compte AWS Organizations de gestion.
2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home, puis utilisez le Région AWS sélecteur en haut à droite pour spécifier la région dans laquelle vous souhaitez supprimer l'administrateur délégué.
3. Dans le volet de navigation, sous Paramètres, choisissez Gestion du compte.
4. Dans la section Administrateur délégué, choisissez Supprimer, puis confirmez votre action.

5. Répétez ces étapes dans chaque région dans laquelle vous avez enregistré cet administrateur délégué.

Lorsque vous ajoutez un nouvel administrateur délégué Amazon Inspector, vous devez associer manuellement les membres de l'organisation au nouveau compte administrateur. Suivez les étapes ci-dessous pour associer les membres de l'organisation au nouveau compte administrateur.

Pour associer des membres à un nouvel administrateur délégué

1. Connectez-vous à l'AWS Management Consoleaide du compte d'administrateur délégué.
2. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home, puis utilisez le Région AWS sélecteur en haut à droite pour spécifier la région dans laquelle vous souhaitez associer des membres au nouvel administrateur délégué.
3. Dans le volet de navigation, sous Paramètres, choisissez Gestion du compte.
4. Sélectionnez tous les comptes répertoriés dans votre organisation en cochant la case supérieure.
5. Dans le menu Actions, choisissez Ajouter un membre.
6. Répétez ces étapes dans chaque région dans laquelle vous souhaitez associer des membres au nouvel administrateur délégué.

Surveillance de l'utilisation et des coûts dans Amazon Inspector

Vous pouvez utiliser la console Amazon Inspector et les opérations d'API pour prévoir les coûts mensuels liés à l'utilisation d'Amazon Inspector dans votre environnement. Si vous êtes l'administrateur Amazon Inspector d'un environnement à comptes multiples, vous pouvez consulter le coût total de l'ensemble de votre environnement et les statistiques de coûts pour chacun de vos comptes membres.

Utilisation de la console d'utilisation

Vous pouvez évaluer l'utilisation et le coût prévisionnel d'Amazon Inspector depuis la console.

Pour accéder aux statistiques d'utilisation

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez surveiller les coûts.
3. Dans le panneau de navigation, choisissez Utilisateurs.

Dans l'onglet Par compte, vous verrez le coût total prévu sur la base de la période de 30 jours indiquée sous Utilisation du compte. Dans le tableau situé sous la colonne Coût projeté, sélectionnez une valeur pour afficher une ventilation de l'utilisation par type de scan pour ce compte. Dans ce volet détaillé, vous pouvez également voir quels types de scan ont un essai gratuit actif pour ce compte.

Si vous êtes l'administrateur délégué d'une organisation, vous verrez une ligne dans le tableau pour chaque compte de votre organisation. Si un compte de votre organisation est dissocié, la console indique son coût prévisionnel sous la forme d'un -.

Dans l'onglet Par type de numérisation, vous pouvez voir une ventilation de l'utilisation réelle réalisée jusqu'à présent au cours de la période de 30 jours en cours par type de numérisation. Il s'agit des informations utilisées pour calculer les coûts prévus dans l'onglet Par compte.

Si vous êtes l'administrateur délégué d'une organisation, vous pouvez voir l'utilisation de chaque compte de votre organisation.

Dans cet onglet, vous pouvez développer l'un des volets suivants pour les statistiques d'utilisation :

Numérisation Amazon EC2

La console d'utilisation d'Amazon Inspector suit les mesures suivantes pour le scan basé sur un agent et le scan sans agent :

- Instances (moyenne) : Amazon Inspector utilise les heures de couverture pour calculer le nombre moyen de ressources pour l'analyse des instances EC2. La moyenne est le nombre total d'heures de couverture divisé par 720 heures (le nombre d'heures sur une période de 30 jours).
- Heures de couverture : pour le scan Amazon EC2, il s'agit du nombre total d'heures pendant lesquelles Amazon Amazon Inspector a fourni une couverture active pour chaque instance EC2 d'un compte au cours des 30 derniers jours. Pour les instances EC2, les heures de couverture sont les heures entre le moment où Amazon Inspector a découvert l'instance et celui où elle est arrêtée ou exclue des analyses par balises. (lorsque vous redémarrez une instance arrêtée ou que vous supprimez une balise d'exclusion, Amazon Inspector reprend la couverture et les heures de couverture pour cette instance continuent de s'accumuler).

Analyses d'instances CIS : nombre total de scans CIS effectués pour les instances du compte.

Numérisation Amazon ECR

Numérisation initiale : somme totale des images numérisées pour la première fois sur le compte au cours des 30 derniers jours.

Numérisations : somme totale des rescans des images du compte au cours des 30 derniers jours. Un nouveau scan est un scan effectué sur une image ECR précédemment scannée par Amazon Inspector. Si vous avez configuré votre référentiel ECR pour une analyse continue, les nouvelles analyses sont effectuées automatiquement lorsqu'Amazon Inspector ajoute un nouveau code CVE (Common Vulnerabilities and Exposures) à sa base de données.

Numérisation Lambda

La console d'utilisation d'Amazon Inspector suit les mesures suivantes pour le scan standard Lambda et le scan du code Lambda :

- Nombre moyen de fonctions Lambda : Amazon Inspector utilise les heures de couverture pour calculer le nombre moyen de fonctions pour l'analyse des fonctions Lambda. La moyenne est le nombre total d'heures de couverture divisé par 720 heures (le nombre d'heures sur une période de 30 jours).

- Heures de couverture : pour l'analyse des fonctions Lambda, il s'agit du nombre total d'heures pendant lesquelles Amazon Amazon Inspector a fourni une couverture active pour chaque fonction Lambda d'un compte au cours des 30 derniers jours. Pour les AWS Lambda fonctions, les heures de couverture sont calculées à partir du moment où Amazon Inspector découvre une fonction jusqu'au moment où elle est supprimée ou exclue des scans. Si une fonction exclue est à nouveau incluse, les heures de couverture de cette fonction continueront de s'accumuler.

Comprendre comment Amazon Inspector calcule les coûts d'utilisation

Les coûts fournis par Amazon Inspector sont des estimations et non des coûts réels. Ils peuvent donc différer de ceux de votre AWS Billing console.

Notez ce qui suit à propos de la façon dont Amazon Inspector calcule les coûts sur la page Utilisation :

- Le coût d'utilisation reflète uniquement la région actuelle. Les prix par type de scan varient selon les AWS régions. Pour connaître les prix exacts par région, consultez les tarifs d'Amazon Inspector
- Toutes les projections d'utilisation sont arrondies au dollar américain le plus proche.
- Les remises ne sont pas incluses dans les coûts prévus.
- Le coût prévu représente le coût total pour la période d'utilisation de 30 jours par type de scan. Si un compte a été utilisé pendant moins de 30 jours, Amazon Inspector prévoit le coût après 30 jours, comme si les ressources actuellement couvertes resteraient couvertes pendant le reste de la période de 30 jours.
- Le coût par type de numérisation est calculé sur la base des éléments suivants :
  - Scan EC2 : le coût reflète le nombre moyen d'instances EC2 couvertes par Amazon Inspector au cours des 30 derniers jours.
  - Numérisation de conteneurs ECR : le coût reflète la somme du nombre de numérisations d'images initiales et de nouvelles analyses d'images au cours des 30 derniers jours.
  - Scan standard Lambda : le coût reflète le nombre moyen de fonctions Lambda couvertes par Amazon Inspector au cours des 30 derniers jours.
  - Numérisation du code Lambda : le coût reflète le nombre moyen de fonctions Lambda couvertes par Amazon Inspector au cours des 30 derniers jours.

À propos de l'essai gratuit d'Amazon Inspector

Lorsque vous activez un type de scan Amazon Inspector, vous êtes automatiquement inscrit à un essai gratuit de 15 jours pour ce type de scan. Chaque type de scan dispose d'un essai gratuit indépendant, qui inclut : le scan EC2, le scan ECR, le scan standard Lambda et le scan du code Lambda.

> **Note**
>
> L'essai gratuit ne s'applique pas à la numérisation CIS.

Si vous désactivez un type de scan pendant l'essai gratuit, l'essai gratuit sera suspendu pour ce type de scan. Si vous réactivez ce service, l'essai gratuit reprendra et vous bénéficierez des jours restants de cet essai gratuit.

Sécurité dans Amazon Inspector

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des 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 AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Inspector, consultez la section AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon Inspector. Les rubriques suivantes expliquent comment configurer Amazon Inspector pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon Inspector.

Rubriques

Protection des données dans Amazon Inspector

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Inspector. 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 en savoir plus 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 en savoir plus 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 Amazon Inspector ou un autre utilisateur Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les

données que vous saisissez 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.

Rubriques

Chiffrement au repos

Amazon Inspector stocke vos données au repos en toute sécurité à l'aide de solutions de AWS chiffrement par défaut. Amazon Inspector chiffre les données, telles que l'inventaire des ressources collecté à l'aide de AWS Systems Manager, l'inventaire des ressources analysé à partir des images Amazon ECR et les résultats de sécurité générés, à l'aide des clés de chiffrement AWS détenues par AWS Key Management Service ().AWS KMS Vous ne pouvez pas afficher, gérer ou utiliser les clés que vous AWS possédez, ni auditer leur utilisation. Cependant, vous n'êtes pas obligé de prendre des mesures ni de modifier de programme pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez la section Clés AWS détenues.

Si vous désactivez Amazon Inspector, celui-ci supprime définitivement toutes les ressources qu'il stocke ou gère pour vous, telles que l'inventaire collecté et les résultats de sécurité.

Chiffrement inexistant pour le code contenu dans vos résultats

Pour l'analyse du code Lambda d'Amazon Inspector, Amazon Inspector s'associe CodeGuru pour analyser votre code afin de détecter les vulnérabilités. Lorsqu'une vulnérabilité est détectée, CodeGuru extrait un extrait de code contenant la vulnérabilité et stocke ce code jusqu'à ce qu'Amazon Inspector demande l'accès. CodeGuru Utilise par défaut une AWS clé propre pour chiffrer le code extrait, mais vous pouvez configurer Amazon Inspector pour utiliser votre propre AWS KMS clé gérée par le client pour le chiffrement.

Le flux de travail suivant explique comment Amazon Inspector utilise la clé que vous configurez pour chiffrer votre code :

1. Vous fournissez une AWS KMS clé à Amazon Inspector à l'aide de l'UpdateEncryptionKeyAPI Amazon Inspector.

2. Amazon Inspector transmet les informations relatives à votre AWS KMS clé à CodeGuru. CodeGuru stocke les informations pour une utilisation future.
3. CodeGuru demande une subvention AWS KMS pour la clé que vous avez configurée dans Amazon Inspector.
4. CodeGuru crée une clé de données cryptée à partir de votre AWS KMS clé et la stocke. Cette clé de données est utilisée pour chiffrer les données de code stockées par CodeGuru.
5. Chaque fois qu'Amazon Inspector demande des données à partir de codes, il CodeGuru utilise l'autorisation pour déchiffrer la clé de données chiffrée, puis utilise cette clé pour déchiffrer les données afin qu'elles puissent être récupérées.

Lorsque vous désactivez le scan du code Lambda, l'autorisation est CodeGuru retirée et la clé de données associée est supprimée.

Autorisations pour le chiffrement du code à l'aide d'une clé gérée par le client

Pour utiliser le chiffrement, vous devez disposer d'une politique autorisant l'accès aux AWS KMS actions, ainsi que d'une déclaration octroyant à Amazon Inspector l' CodeGuru autorisation d'utiliser ces actions par le biais de clés de condition.

Si vous configurez, mettez à jour ou réinitialisez la clé de chiffrement de votre compte, vous devez utiliser une politique d'administration Amazon Inspector, telle queAWS politique gérée : AmazonInspector2FullAccess. Vous devrez également accorder les autorisations suivantes aux utilisateurs en lecture seule qui ont besoin de récupérer des extraits de code à partir de résultats ou de données concernant la clé choisie pour le chiffrement.

Pour KMS, la politique doit vous permettre d'effectuer les actions suivantes :

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

Une fois que vous avez vérifié que vous disposez des AWS KMS autorisations appropriées dans votre politique, vous devez joindre une déclaration autorisant Amazon Inspector CodeGuru à utiliser votre clé pour le chiffrement. Joignez la déclaration de politique suivante :

> **Note**
>
> Remplacez la région par la AWS région dans laquelle le scan du code Lambda d'Amazon Inspector est activé.

```
{
            "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
          "Effect": "Allow",
          "Action": "kms:CreateGrant",
          "Resource": "*",
          "Condition": {
           "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
             "GenerateDataKey",
             "GenerateDataKeyWithoutPlaintext",
             "Encrypt",
             "Decrypt",
             "RetireGrant",
             "DescribeKey"
            ]
           },
           "StringEquals": {
            "kms:ViaService": [
             "codeguru-security.Region.amazonaws.com"
            ]
           }
          }
         },
         {
          "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
          "Effect": "Allow",
          "Action": [
           "kms:Encrypt",
           "kms:Decrypt",
           "kms:RetireGrant",
           "kms:DescribeKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
       ],
       "Resource": "*",
       "Condition": {
        "StringEquals": {
         "kms:ViaService": [
          "inspector2.Region.amazonaws.com",
          "codeguru-security.Region.amazonaws.com"
         ]
        }
       }
      }
```

> **Note**
>
> Lorsque vous ajoutez l'instruction, assurez-vous que la syntaxe est valide. Les stratégies utilisent le format JSON. Cela signifie que vous devez ajouter une virgule avant ou après la déclaration, selon l'endroit où vous l'ajoutez à la politique. Si vous ajoutez l'instruction en tant que dernière instruction, ajoutez une virgule après l'accolade de fermeture pour l'instruction précédente. Si vous l'ajoutez en tant que première instruction ou entre deux instructions existantes, ajoutez une virgule après l'accolade de fermeture de l'instruction.

Configuration du chiffrement à l'aide d'une clé gérée par le client

Pour configurer le chiffrement de votre compte à l'aide d'une clé gérée par le client, vous devez être un administrateur Amazon Inspector avec les autorisations décrites dansAutorisations pour le chiffrement du code à l'aide d'une clé gérée par le client. En outre, vous aurez besoin d'une AWS KMS clé dans la même AWS région que vos résultats, ou d'une clé multirégionale. Vous pouvez utiliser une clé symétrique existante dans votre compte ou créer une clé symétrique gérée par le client à l'aide de la console AWS de gestion ou des AWS KMS API. Pour plus d'informations, voir Création de AWS KMS clés de chiffrement symétriques dans le guide de l' AWS KMS utilisateur.

Utilisation de l'API Amazon Inspector pour configurer le chiffrement

Pour définir une clé de chiffrement, le UpdateEncryptionKeyfonctionnement de l'API Amazon Inspector lorsque vous êtes connecté en tant qu'administrateur Amazon Inspector. Dans la demande d'API, utilisez le `kmsKeyId` champ pour spécifier l'ARN de la AWS KMS clé que vous souhaitez utiliser. Pour `scanType` entrer `CODE` et pour `resourceType` entrer`AWS_LAMBDA_FUNCTION`.

Vous pouvez utiliser UpdateEncryptionKeyl'API pour vérifier quelle AWS KMS clé Amazon Inspector utilise pour le chiffrement.

> **Note**
>
> Si vous essayez de l'utiliser `GetEncryptionKey` alors que vous n'avez pas défini de clé gérée par le client, l'opération renvoie une `ResourceNotFoundException` erreur indiquant qu'une clé AWS détenue est utilisée pour le chiffrement.

Si vous supprimez la clé ou si vous modifiez sa politique de refus d'accès à Amazon Inspector, CodeGuru vous ne pourrez pas accéder aux résultats de vulnérabilité de votre code et le scan du code Lambda échouera pour votre compte.

Vous pouvez l'utiliser `ResetEncryptionKey` pour recommencer à utiliser une clé AWS détenue pour chiffrer le code extrait dans le cadre de vos recherches sur Amazon Inspector.

Chiffrement en transit

AWS chiffre toutes les données en transit entre les systèmes AWS internes et les autres AWS services.

Pour la collecte d'inventaire, Systems Manager collecte des données de télémétrie à partir d'instances EC2 appartenant au client, qu'il renvoie AWS via un canal protégé par le protocole TLS (Transport Layer Security) à des fins d'évaluation. Consultez la section Protection des données dans Systems Manager pour comprendre comment SSM chiffre les données en transit.

De même, les résultats des scans des fonctions Amazon ECR et AWS Lambda envoyés à Security Hub sont chiffrés à l'aide d'un canal protégé par TLS.

Identity and Access Management pour Amazon Inspector

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 les ressources Amazon Inspector. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon Inspector.

Utilisateur du service : si vous utilisez le service Amazon Inspector 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 plus en plus de fonctionnalités d'Amazon Inspector pour effectuer votre travail, il se peut que vous ayez 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 Amazon Inspector, consultezRésolution des problèmes d'identité et d'accès à Amazon Inspector.

Administrateur du service — Si vous êtes responsable des ressources Amazon Inspector au sein de votre entreprise, vous avez probablement un accès complet à Amazon Inspector. C'est à vous de déterminer les fonctionnalités et les ressources d'Amazon Inspector 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 Amazon Inspector, consultezComment Amazon Inspector fonctionne 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 Amazon Inspector. Pour consulter des exemples de politiques basées sur l'identité Amazon Inspector que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector

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, veuillez consulter Multi-factor authentication (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, veuillez consulter 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 en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources 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, une fonction 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, l'action que vous effectuez est susceptible de lancer 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.
  - Fonction du 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 au service apparaissent dans votre Compte AWS fichier 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 Présentation 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 Amazon S3. 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 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.

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 Présentation 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 fonction 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 qui en résultent 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 fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle de service (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 la séance obtenue 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 remplace 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 obtenues 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 Inspector fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon Inspector, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Amazon Inspector.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Inspector

Fonction IAM	Assistance Amazon Inspector
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Amazon Inspector et d'autres fonctionnalités Services AWS fonctionnent avec la plupart des fonctionnalités IAM, consultez Services AWS le guide de l'utilisateur d'IAM concernant leur compatibilité avec IAM.

Politiques basées sur l'identité pour Amazon Inspector

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, veuillez consulter 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 Amazon Inspector

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector

Politiques basées sur les ressources dans Amazon Inspector

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 Amazon S3. 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 Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions politiques pour Amazon Inspector

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 actions Amazon Inspector, consultez la section Actions définies par Amazon Inspector dans le Service Authorization Reference.

Les actions politiques dans Amazon Inspector utilisent le préfixe suivant avant l'action :

```
inspector2
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "inspector2:action1",
      "inspector2:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector

Ressources relatives aux politiques pour Amazon Inspector

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 pour lesquels 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 ressources Amazon Inspector et de leurs ARN, consultez la section Ressources définies par Amazon Inspector dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon Inspector.

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector

Clés de conditions de politique pour Amazon Inspector

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 condition Amazon Inspector, consultez la section Clés de condition pour Amazon Inspector dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon Inspector.

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector

ACL dans Amazon Inspector

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.

ABAC avec Amazon Inspector

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 balises, vous devez fournir les informations de balise 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 basé sur les attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Amazon Inspector

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 Amazon Inspector

Prend en charge les transmissions de sessions d'accès (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, l'action que vous effectuez est susceptible de lancer 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.

Rôles de service pour Amazon Inspector

Prend en charge les fonctions de service	Non

Une fonction du 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 les fonctionnalités d'Amazon Inspector. Modifiez les rôles de service uniquement lorsque Amazon Inspector fournit des instructions à cet effet.

Rôles liés à un service pour Amazon Inspector

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 au service apparaissent dans votre Compte AWS fichier 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 de rôles liés à un service, consultez la section relative à l'Services AWS utilisation d'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 Inspector

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon Inspector. 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 Amazon Inspector, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon Inspector 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 des ressources Amazon Inspector 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 AWS ou Politiques gérées 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 Amazon Inspector

Pour accéder à la console Amazon Inspector, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon Inspector 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 console Amazon Inspector, associez également Amazon Inspector `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.

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": "*"
        }
    ]
}
```

Autoriser l'accès en lecture seule à toutes les ressources Amazon Inspector

Cet exemple montre une politique qui autorise l'accès en lecture seule à toutes les ressources Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector2:Describe*",
                "inspector2:Get*",
                "inspector2:BatchGet*",
                "inspector2:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Autoriser un accès complet à toutes les ressources Amazon Inspector

Cet exemple montre une politique qui autorise un accès complet à toutes les ressources Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour Amazon Inspector

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients.

Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont spécifiques à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonInspector2FullAccess

Vous pouvez associer la politique `AmazonInspector2FullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès complet à Amazon Inspector.

Détails des autorisations

Cette politique inclut les autorisations suivantes.

- `inspector2`— Permet un accès complet aux fonctionnalités d'Amazon Inspector.
- `iam`— Permet à Amazon Inspector de créer le rôle lié au service,. `AmazonInspector2AgentlessServiceRole` Cela est nécessaire pour qu'Amazon Inspector puisse effectuer des opérations telles que récupérer des informations sur vos instances Amazon EC2, les référentiels Amazon ECR et les images de conteneurs, analyser votre réseau VPC et décrire les comptes associés à votre organisation. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon Inspector.
- `organizations`— Permet aux administrateurs d'utiliser Amazon Inspector pour une organisation dans AWS Organizations. Après avoir activé l'accès sécurisé pour Amazon Inspector dans AWS

Organizations, les membres du compte d'administrateur délégué peuvent gérer les paramètres et consulter les résultats au sein de leur organisation.

- `codeguru-security`— Permet aux administrateurs d'utiliser Amazon Inspector pour récupérer des extraits de code d'informations et modifier les paramètres de chiffrement du code stocké par CodeGuru Security. Pour de plus amples informations, veuillez consulter Chiffrement inexistant pour le code contenu dans vos résultats.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:UpdateAccountConfiguration"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "inspector2.amazonaws.com"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
```

```
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politique gérée : AmazonInspector2ReadOnlyAccess

Vous pouvez associer la politique `AmazonInspector2ReadOnlyAccess` à vos identités IAM.

Cette politique accorde des autorisations permettant un accès en lecture seule à Amazon Inspector.

Détails des autorisations

Cette politique inclut les autorisations suivantes.

- `inspector2`— Permet un accès en lecture seule aux fonctionnalités d'Amazon Inspector.
- `organizations`— Permet de consulter les informations relatives à la couverture d'Amazon Inspector AWS Organizations pour une organisation.
- `codeguru-security`— Permet de récupérer des extraits de code depuis CodeGuru Security. Permet également de consulter les paramètres de chiffrement de votre code stocké dans CodeGuru Security.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "inspector2:BatchGet*",
```

```
    "inspector2:List*",
    "inspector2:Describe*",
    "inspector2:Get*",
    "inspector2:Search*",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politique gérée : AmazonInspector2ManagedCisPolicy

Vous pouvez associer la politique `AmazonInspector2ManagedCisPolicy` à vos entités IAM. Cette politique doit être associée à un rôle qui accorde des autorisations à vos instances Amazon EC2 pour exécuter des scans CIS de l'instance. 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 AWS CLI d' AWS API. 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.

Détails des autorisations

Cette politique inclut les autorisations suivantes.

- `inspector2`— Permet d'accéder aux actions utilisées pour exécuter des scans CIS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
```

```
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
            ],
            "Resource": "*",
        }
    ]
}
```

AWS politique gérée : AmazonInspector2ServiceRolePolicy

Vous ne pouvez pas associer `AmazonInspector2ServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Amazon Inspector d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon Inspector.

AWS politique gérée : AmazonInspector2AgentlessServiceRolePolicy

Vous ne pouvez pas associer `AmazonInspector2AgentlessServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Amazon Inspector d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Amazon Inspector.

Amazon Inspector met à jour les politiques AWS gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon Inspector 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 d'historique des documents Amazon Inspector.

Modification	Description	Date
AmazonInspector2 ManagedCisPolicy — Nouvelle politique	Amazon Inspector a ajouté une nouvelle politique gérée que vous pouvez utiliser dans le cadre d'un profil d'instance pour autoriser les scans CIS sur une instance.	23 janvier 2024

Modification	Description	Date
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector de lancer des scans CIS sur des instances cibles.	23 janvier 2024
AmazonInspector2 AgentlessServiceRolePolicy — Nouvelle politique	Amazon Inspector a ajouté une nouvelle politique de rôle liée au service afin de permettre l'analyse sans agent de l'instance EC2.	27 novembre 2023
AmazonInspector2 ReadOnlyAccess — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent aux utilisateurs en lecture seule de récupérer des informations sur les vulnérabilités pour détecter les vulnérabilités des packages.	22 septembre 2023
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector de scanner les configurations réseau des instances Amazon EC2 qui font partie des groupes cibles d'Elastic Load Balancing.	31 août 2023

Modification	Description	Date
AmazonInspector2 ReadOnlyAccess — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent aux utilisateurs en lecture seule d'exporter une nomenclature logicielle (SBOM) pour leurs ressources.	29 juin 2023
AmazonInspector2 ReadOnlyAccess — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent aux utilisateurs en lecture seule de récupérer les détails des paramètres de chiffrement pour les résultats de l'analyse du code Lambda pour leur compte.	13 juin 2023
AmazonInspector2 FullAccess — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent aux utilisateurs de configurer une clé KMS gérée par le client pour chiffrer le code issu du scan du code Lambda.	13 juin 2023
AmazonInspector2 ReadOnlyAccess — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent aux utilisateurs en lecture seule de récupérer les informations relatives à l'état de numérisation du code Lambda et aux résultats de leur compte.	2 mai 2023

Modification	Description	Date
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector de créer des canaux AWS CloudTrail liés à un service dans votre compte lorsque vous activez le scan Lambda. Cela permet à Amazon Inspector de surveiller CloudTrail les événements de votre compte.	30 avril 2023
AmazonInspector2 FullAccess — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent aux utilisateurs de récupérer des informations sur les vulnérabilités détectées dans le code Lambda lors de l'analyse du code Lambda.	21 avril 2023
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector d'envoyer des informations à Amazon EC2 Systems Manager concernant les chemins personnalisés définis par un client pour l'inspection approfondie d'Amazon EC2.	17 avril 2023

Modification	Description	Date
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector de créer des canaux AWS CloudTrail liés à un service dans votre compte lorsque vous activez le scan Lambda. Cela permet à Amazon Inspector de surveiller CloudTrail les événements de votre compte.	30 avril 2023
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector de demander des scans du code du développeur dans AWS Lambda les fonctions et de recevoir des données de scan d'Amazon CodeGuru Security. En outre, Amazon Inspector a ajouté des autorisations permettant de consulter les politiques IAM. Amazon Inspector utilise ces informations pour analyser les fonctions Lambda afin de détecter les vulnérabilités du code.	28 février 2023

Modification	Description	Date
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté une nouvelle déclaration qui permet à Amazon Inspector de récupérer des informations CloudWatch concernant la date à laquelle une AWS Lambda fonction a été invoquée pour la dernière fois. Amazon Inspector utilise ces informations pour concentrer les analyses sur les fonctions Lambda actives au cours des 90 derniers jours dans votre environnement.	20 février 2023
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté une nouvelle déclaration qui permet à Amazon Inspector de récupérer des informations sur AWS Lambda les fonctions, y compris chaque version de couche associée à chaque fonction. Amazon Inspector utilise ces informations pour analyser les fonctions Lambda afin de détecter les failles de sécurité.	28 novembre 2022

Modification	Description	Date
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a ajouté une nouvelle action permettant à Amazon Inspector de décrire les exécutions d'associations SSM. En outre, Amazon Inspector a ajouté un périmètre de ressources supplémentaire pour permettre à Amazon Inspector de créer, mettre à jour, supprimer et démarrer des associations SSM avec des documents SSM `AmazonInspector2` détenus.	31 août 2022
AmazonInspector2 ServiceRolePolicy Mises à jour d'une politique existante	Amazon Inspector a mis à jour le périmètre des ressources de la politique afin de permettre à Amazon Inspector de collecter l'inventaire des logiciels dans d'autres AWS partitions.	12 août 2022
AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante	Amazon Inspector a restructuré le périmètre des ressources des actions permettant à Amazon Inspector de créer, de supprimer et de mettre à jour des associations SSM.	10 août 2022
AmazonInspector2 ReadOnlyAccess — Nouvelle politique	Amazon Inspector a ajouté une nouvelle politique pour autoriser l'accès en lecture seule aux fonctionnalités d'Amazon Inspector.	21 janvier 2022

Modification	Description	Date
AmazonInspector2 FullAccess — Nouvelle politique	Amazon Inspector a ajouté une nouvelle politique permettant un accès complet aux fonctionnalités d'Amazon Inspector.	29 novembre 2021
AmazonInspector2 ServiceRolePolicy — Nouvelle politique	Amazon Inspector a ajouté une nouvelle politique permettant à Amazon Inspector d'effectuer des actions dans d'autres services en votre nom.	29 novembre 2021
Amazon Inspector a commencé à suivre les modifications	Amazon Inspector a commencé à suivre les modifications apportées AWS à ses politiques gérées.	29 novembre 2021

Utilisation de rôles liés à un service pour Amazon Inspector

Amazon Inspector utilise un rôle AWS Identity and Access Management (IAM) lié à un service nommé. `AWSServiceRoleForAmazonInspector2` Ce rôle lié à un service est un rôle IAM directement lié à Amazon Inspector. Il est prédéfini par Amazon Inspector et inclut toutes les autorisations dont Amazon Inspector a besoin pour appeler d'autres Services AWS personnes en votre nom.

Un rôle lié à un service facilite la configuration d'Amazon Inspector, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Amazon Inspector définit les autorisations associées à son rôle lié à un service et, sauf indication contraire, seul Amazon Inspector peut assumer ce 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.

Vous devez configurer les autorisations pour autoriser une entité IAM (telle qu'un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM. Vous ne pouvez supprimer

un rôle lié à un service qu'après avoir supprimé les ressources associées. Cela protège vos ressources Amazon Inspector, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Cliquez sur Oui avec un lien pour consulter la documentation relative aux rôles liés à un service pour ce service.

Autorisations de rôle liées à un service pour Amazon Inspector

Amazon Inspector utilise le rôle lié au service nommé. `AWSServiceRoleForAmazonInspector2` Ce rôle lié au service fait confiance au `inspector2.amazonaws.com` service pour assumer le rôle.

La politique d'autorisation pour le rôle, qui est nommé`AmazonInspector2ServiceRolePolicy`, permet à Amazon Inspector d'effectuer des tâches telles que :

- Utilisez les actions Amazon Elastic Compute Cloud (Amazon EC2) pour récupérer des informations sur vos instances et les chemins réseau.
- Utilisez AWS Systems Manager des actions pour récupérer l'inventaire de vos instances Amazon EC2 et pour récupérer des informations sur les packages tiers à partir de chemins personnalisés.
- Utilisez cette AWS Systems Manager `SendCommand` action pour appeler des scans CIS pour les instances cibles.
- Utilisez les actions Amazon Elastic Container Registry pour récupérer des informations sur les images de vos conteneurs.
- Utilisez AWS Lambda des actions pour récupérer des informations sur vos fonctions Lambda.
- Utilisez AWS Organizations des actions pour décrire les comptes associés.
- Utilisez CloudWatch des actions pour récupérer des informations sur la dernière fois que vos fonctions Lambda ont été invoquées.
- Utilisez certaines actions IAM pour récupérer des informations sur vos politiques IAM susceptibles de créer des failles de sécurité dans votre code Lambda.
- Utilisez les actions de CodeGuru sécurité pour analyser le code dans vos fonctions Lambda. Amazon Inspector utilise les actions CodeGuru de sécurité suivantes :
  - codeguru-security : CreateScan — Accorde l'autorisation de créer un scan de sécurité. CodeGuru

- codeguru-security : GetScan — Autorise à récupérer CodeGuru les métadonnées du scan de sécurité.
- codeguru-security : ListFindings — Accorde l'autorisation de récupérer les résultats générés par Security. CodeGuru
- codeguru-security : DeleteScansByCategory — Autorise CodeGuru Security à supprimer les scans initiés par Amazon Inspector.
- codeguru-security : BatchGetFindings — Autorise à récupérer un lot de résultats spécifiques générés par Security. CodeGuru

- Utilisez certaines actions Elastic Load Balancing pour effectuer des scans du réseau des instances EC2 qui font partie des groupes cibles d'Elastic Load Balancing.

Le rôle est configuré selon la politique d'autorisation suivante.

```
    {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "TirosPolicy",
  "Effect": "Allow",
  "Action": [
   "directconnect:DescribeConnections",
   "directconnect:DescribeDirectConnectGatewayAssociations",
   "directconnect:DescribeDirectConnectGatewayAttachments",
   "directconnect:DescribeDirectConnectGateways",
   "directconnect:DescribeVirtualGateways",
   "directconnect:DescribeVirtualInterfaces",
   "ec2:DescribeAvailabilityZones",
   "ec2:DescribeCustomerGateways",
   "ec2:DescribeInstances",
   "ec2:DescribeInternetGateways",
   "ec2:DescribeManagedPrefixLists",
   "ec2:DescribeNatGateways",
   "ec2:DescribeNetworkAcls",
   "ec2:DescribeNetworkInterfaces",
   "ec2:DescribePrefixLists",
   "ec2:DescribeRegions",
   "ec2:DescribeRouteTables",
   "ec2:DescribeSecurityGroups",
   "ec2:DescribeSubnets",
```

```
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "PackageVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "ecr:BatchGetImage",
    "ecr:BatchGetRepositoryScanningConfiguration",
    "ecr:DescribeImages",
```

```
    "ecr:DescribeRegistry",
    "ecr:DescribeRepositories",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:GetRegistryScanningConfiguration",
    "ecr:ListImages",
    "ecr:PutRegistryScanningConfiguration",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "ssm:DescribeAssociation",
    "ssm:DescribeAssociationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:ListAssociations",
    "ssm:ListResourceDataSync"
   ],
   "Resource": "*"
  },
  {
   "Sid": "LambdaPackageVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "lambda:ListFunctions",
    "lambda:GetFunction",
    "lambda:GetLayerVersion",
    "cloudwatch:GetMetricData"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GatherInventory",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce",
    "ssm:DeleteAssociation",
    "ssm:UpdateAssociation"
   ],
   "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonInspector2-*",
    "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:aws:ssm:*:*:managed-instance/*",
    "arn:aws:ssm:*:*:association/*"
```

```
    ]
   },
   {
    "Sid": "DataSyncCleanup",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateResourceDataSync",
     "ssm:DeleteResourceDataSync"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
    ]
   },
   {
    "Sid": "ManagedRules",
    "Effect": "Allow",
    "Action": [
     "events:PutRule",
     "events:DeleteRule",
     "events:DescribeRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": [
     "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
    ]
   },
   {
    "Sid": "LambdaCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "codeguru-security:CreateScan",
     "codeguru-security:GetAccountConfiguration",
     "codeguru-security:GetFindings",
     "codeguru-security:GetScan",
     "codeguru-security:ListFindings",
     "codeguru-security:BatchGetFindings",
     "codeguru-security:DeleteScansByCategory"
    ],
    "Resource": [
     "*"
    ]
   },
```

```
{
 "Sid": "CodeGuruCodeVulnerabilityScanning",
 "Effect": "Allow",
 "Action": [
  "iam:GetRole",
  "iam:GetRolePolicy",
  "iam:GetPolicy",
  "iam:GetPolicyVersion",
  "iam:ListAttachedRolePolicies",
  "iam:ListPolicies",
  "iam:ListPolicyVersions",
  "iam:ListRolePolicies",
  "lambda:ListVersionsByFunction"
 ],
 "Resource": [
  "*"
 ],
 "Condition": {
  "ForAnyValue:StringEquals": {
   "aws:CalledVia": [
    "codeguru-security.amazonaws.com"
   ]
  }
 }
},
{
 "Sid": "Ec2DeepInspection",
 "Effect": "Allow",
 "Action": [
  "ssm:PutParameter",
  "ssm:GetParameters",
  "ssm:DeleteParameter"
 ],
 "Resource": [
  "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
 ],
 "Condition": {
  "StringEquals": {
   "aws:ResourceAccount": "${aws:PrincipalAccount}"
  }
 }
},
{
 "Sid": "AllowManagementOfServiceLinkedChannel",
```

```
    "Effect": "Allow",
    "Action": [
     "cloudtrail:CreateServiceLinkedChannel",
     "cloudtrail:DeleteServiceLinkedChannel"
    ],
    "Resource": [
     "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowListServiceLinkedChannels",
    "Effect": "Allow",
    "Action": [
     "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToRunInvokeCisSpecificDocuments",
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand",
     "ssm:GetCommandInvocation"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
    ]
   },
   {
    "Sid": "AllowToRunCisCommandsToSpecificResources",
    "Effect": "Allow",
    "Action": [
```

```
     "ssm:SendCommand"
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToPutCloudwatchMetricData",
    "Effect": "Allow",
    "Action": [
     "cloudwatch:PutMetricData"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "cloudwatch:namespace": "AWS/Inspector2"
     }
    }
   }
  ]
}
```

Création d'un rôle lié à un service pour Amazon Inspector

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez Amazon Inspector dans le AWS Management Console AWS CLI, le ou l' AWS API, Amazon Inspector crée pour vous le rôle lié au service.

Modification d'un rôle lié à un service pour Amazon Inspector

Amazon Inspector ne vous permet pas de modifier le rôle `AWSServiceRoleForAmazonInspector2` lié au service. Une fois qu'un rôle lié à un service est créé, vous ne pouvez pas modifier le nom du rôle car différentes entités peuvent y faire référence. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Amazon Inspector

Si vous n'avez plus besoin d'utiliser Amazon Inspector, nous vous recommandons de supprimer le rôle `AWSServiceRoleForAmazonInspector2` lié au service. Avant de pouvoir supprimer le rôle, vous devez désactiver Amazon Inspector dans chaque Région AWS cas où il est activé. Lorsque vous désactivez Amazon Inspector, le rôle n'est pas supprimé pour vous. Par conséquent, si vous réactivez Amazon Inspector, celui-ci pourra utiliser le rôle existant. De cette façon, vous pouvez éviter d'avoir une entité inutilisée qui n'est pas activement surveillée ou maintenue. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

Si vous supprimez ce rôle lié à un service et que vous devez ensuite le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous activez Amazon Inspector, Amazon Inspector recrée le rôle lié au service pour vous.

> **Note**
>
> Si le service Amazon Inspector utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Dans ce cas, attendez quelques minutes, puis recommencez l'opération.

Vous pouvez utiliser la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForAmazonInspector2` service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Autorisations de rôle liées au service pour les scans sans agent Amazon Inspector

Le scan sans agent Amazon Inspector utilise le rôle lié au service nommé. `AWSServiceRoleForAmazonInspector2Agentless` Ce reflex permet à Amazon Inspector de créer un instantané du volume Amazon EBS dans votre compte, puis d'accéder aux données de cet instantané. Ce rôle lié au service fait confiance au `agentless.inspector2.amazonaws.com` service pour assumer le rôle.

> **Important**
>
> Les instructions de ce rôle lié au service empêchent Amazon Inspector d'effectuer des scans sans agent sur toute instance EC2 que vous avez exclue des scans à l'aide de la balise. `InspectorEc2Exclusion` En outre, les instructions empêchent Amazon Inspector d'accéder aux données chiffrées d'un volume lorsque la clé KMS utilisée pour le chiffrer

possède le `InspectorEc2Exclusion` tag. Pour de plus amples informations, veuillez consulter Exclure les instances des scans Amazon Inspector.

La politique d'autorisation pour le rôle, qui est nomméAmazonInspector2AgentlessServiceRolePolicy, permet à Amazon Inspector d'effectuer des tâches telles que :

- Utilisez les actions Amazon Elastic Compute Cloud (Amazon EC2) pour récupérer des informations sur vos instances, volumes et instantanés EC2.
  - Utilisez les actions de balisage Amazon EC2 pour étiqueter les instantanés à numériser à l'aide de la clé de balise. `InspectorScan`
  - Utilisez les actions de capture instantanée Amazon EC2 pour créer des instantanés, les étiqueter avec la clé de `InspectorScan` balise, puis supprimer les instantanés des volumes Amazon EBS marqués avec la clé de balise. `InspectorScan`
- Utilisez les actions Amazon EBS pour récupérer des informations à partir de clichés marqués avec la `InspectorScan` clé de balise.
- Utilisez certaines actions de AWS KMS déchiffrement pour déchiffrer les instantanés chiffrés à l'aide de clés gérées par AWS KMS le client. Amazon Inspector ne déchiffre pas les instantanés lorsque la clé KMS utilisée pour les chiffrer est étiquetée avec la balise. `InspectorEc2Exclusion`

Le rôle est configuré selon la politique d'autorisation suivante.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstanceIdentification",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  },
```

```
{
 "Sid": "GetSnapshotData",
 "Effect": "Allow",
 "Action": [
  "ebs:ListSnapshotBlocks",
  "ebs:GetSnapshotBlock"
 ],
 "Resource": "arn:aws:ec2:*:*:snapshot/*",
 "Condition": {
  "StringLike": {
   "aws:ResourceTag/InspectorScan": "*"
  }
 }
},
{
 "Sid": "CreateSnapshotsAnyInstanceOrVolume",
 "Effect": "Allow",
 "Action": "ec2:CreateSnapshots",
 "Resource": [
  "arn:aws:ec2:*:*:instance/*",
  "arn:aws:ec2:*:*:volume/*"
 ]
},
{
 "Sid": "DenyCreateSnapshotsOnExcludedInstances",
 "Effect": "Deny",
 "Action": "ec2:CreateSnapshots",
 "Resource": "arn:aws:ec2:*:*:instance/*",
 "Condition": {
  "StringEquals": {
   "ec2:ResourceTag/InspectorEc2Exclusion": "true"
  }
 }
},
{
 "Sid": "CreateSnapshotsOnAnySnapshotOnlyWithTag",
 "Effect": "Allow",
 "Action": "ec2:CreateSnapshots",
 "Resource": "arn:aws:ec2:*:*:snapshot/*",
 "Condition": {
  "Null": {
   "aws:TagKeys": "false"
  },
  "ForAllValues:StringEquals": {
```

```
      "aws:TagKeys": "InspectorScan"
     }
    }
   },
   {
    "Sid": "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
      "ec2:CreateAction": "CreateSnapshots"
     },
     "Null": {
      "aws:TagKeys": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": "InspectorScan"
     }
    }
   },
   {
    "Sid": "DeleteOnlySnapshotsTaggedForScanning",
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
      "ec2:ResourceTag/InspectorScan": "*"
     }
    }
   },
   {
    "Sid": "DenyKmsDecryptForExcludedKeys",
    "Effect": "Deny",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
```

```
    "Sid": "DecryptSnapshotBlocksVolContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "vol-*"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksSnapContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "snap-*"
     }
    }
   },
   {
    "Sid": "DescribeKeysForEbsOperations",
    "Effect": "Allow",
    "Action": "kms:DescribeKey",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com"
     }
    }
   },
   {
```

```
    "Sid": "ListKeyResourceTags",
    "Effect": "Allow",
    "Action": "kms:ListResourceTags",
    "Resource": "arn:aws:kms:*:*:key/*"
   }
  ]
}
```

Création d'un rôle lié à un service pour le scan sans agent

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez Amazon Inspector dans le AWS Management Console AWS CLI, le ou l' AWS API, Amazon Inspector crée pour vous le rôle lié au service.

Modification d'un rôle lié à un service pour une analyse sans agent

Amazon Inspector ne vous permet pas de modifier le rôle `AWSServiceRoleForAmazonInspector2Agentless` lié au service. Une fois qu'un rôle lié à un service est créé, vous ne pouvez pas modifier le nom du rôle car différentes entités peuvent y faire référence. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, 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 une analyse sans agent

Si vous n'avez plus besoin d'utiliser une fonction 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 supprimer le `AWSServiceRoleForAmazonInspector2Agentless` rôle, vous devez définir votre mode de numérisation sur un mode agent dans toutes les régions où le scan sans agent est disponible. Pour plus d'informations, voir [lien de réglage du mode de numérisation à déterminer].

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForAmazonInspector2Agentless service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Résolution des problèmes d'identité et d'accès à Amazon Inspector

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon Inspector et IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans Amazon Inspector

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 `inspector2:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector2: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 `inspector2:`*`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 effectuer 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 à Amazon Inspector.

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 Amazon Inspector. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction 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 stratégies 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 souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon Inspector

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 Amazon Inspector prend en charge ces fonctionnalités, consultezComment Amazon Inspector fonctionne 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 découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des stratégies basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les stratégies basées sur les ressources dans le Guide de l'utilisateur IAM.

Surveillance d'Amazon Inspector

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Inspector et de vos autres AWS solutions. AWS fournit des outils de surveillance pour surveiller Amazon Inspector, signaler un problème et prendre des mesures automatiques le cas échéant :

- 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 axées sur les événements. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.
- AWS CloudTrail capture les appels d'API et les événements associés effectués par votre Compte AWS ou au nom de ce dernier. CloudTrail envoie ensuite les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Journalisation des appels d'API Amazon Inspector à l'aide de AWS CloudTrail

Amazon Inspector est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur ou un rôle IAM, ou un Service AWS, dans Amazon Inspector. CloudTrail capture tous les appels d'API pour Amazon Inspector sous forme d'événements. Les appels capturés incluent des appels provenant de la console Amazon Inspector et des appels aux opérations de l'API Amazon Inspector. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon Inspector. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les

plus récents dans la console CloudTrail dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer :

- La demande qui a été envoyée à Amazon Inspector.
- Adresse IP à partir de laquelle la demande a été effectuée.
- la personne ayant formulé la requête ;
- Quand la demande a été faite.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations Amazon Inspector dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Amazon Inspector, elle est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez consulter, 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 survenus dans votre environnement Compte AWS, y compris des événements relatifs à Amazon Inspector, créez un suivi. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. 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 en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les rubriques suivantes :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux provenant de plusieurs comptes
- Réception de fichiers CloudTrail journaux provenant de plusieurs régions

Toutes les actions d'Amazon Inspector sont enregistrées par CloudTrail. Toutes les actions qu'Amazon Inspector peut effectuer sont documentées dans le Amazon Inspector API Reference. Par exemple, les appels adressés aux actions `CreateFindingsReport` `ListCoverage`,

`UpdateOrganizationConfiguration` génèrent des entrées dans les fichiers journaux CloudTrail .

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 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 requête a été effectuée par un autre Service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal Amazon Inspector

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 d'une source quelconque. Les événements comprennent les 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.

Informations relatives à Amazon Inspector Scan dans CloudTrail

Amazon Inspector Scan est intégré à CloudTrail. Toutes les opérations de l'API Amazon Inspector Scan sont enregistrées en tant qu'événements de gestion. Pour obtenir la liste des opérations d'API Amazon Inspector Scan auxquelles Amazon Inspector se connecte CloudTrail, consultez Amazon Inspector Scan dans le manuel Amazon Inspector API Reference.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`ScanSbom`action :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:akua_mansa",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/akua_mansa",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-17T15:22:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-17T16:02:34Z",
    "eventSource": "gamma-inspector-scan.amazonaws.com",
    "eventName": "ScanSbom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "aws-sdk-java/2.20.162 Mac_OS_X/13.5.2 OpenJDK_64-
Bit_Server_VM/17.0.8+7-LTS Java/17.0.8 vendor/Amazon.com_Inc. io/sync http/
UrlConnection cfg/retry-mode/legacy",
    "requestParameters": {
        "sbom": {
            "specVersion": "1.5",
            "metadata": {
                "component": {
                    "name": "debian",
                    "type": "operating-system",
                    "version": "9"
                }
            },
            "components": [
                {
                    "name": "packageOne",
                    "purl": "pkg:deb/debian/packageOne@1.0.0?arch=x86_64&distro=9",
                    "type": "application"
                }
            ],
            "bomFormat": "CycloneDX"
        }
```

```
    },
    "responseElements": null,
    "requestID": "f041a27f-f33e-4f70-b09b-5fbc5927282a",
    "eventID": "abc8d1e4-d214-4f07-bc56-8a31be6e36fe",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Validation de conformité pour Amazon Inspector

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 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.
- 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 Inspector

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. 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.

Sécurité de l'infrastructure dans Amazon Inspector

En tant que service géré, Amazon Inspector est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon Inspector via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et 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.

Réponse aux incidents dans Amazon Inspector

La sécurité est la priorité absolue chez AWS. Dans le cadre du modèle de responsabilité partagée du AWS cloud, AWS gère un centre de données, un réseau et une architecture logicielle qui répondent aux exigences des organisations les plus sensibles en matière de sécurité. AWS est responsable de toute réponse aux incidents concernant le AWS Config service lui-même. De plus, en tant que AWS client, vous partagez la responsabilité du maintien de la sécurité dans le cloud. Cela signifie que vous contrôlez la sécurité que vous choisissez de mettre en œuvre à partir des AWS outils et fonctionnalités auxquels vous avez accès, et que vous êtes responsable de la réponse aux incidents de votre côté dans le cadre du modèle de responsabilité partagée.

En établissant une base de sécurité répondant aux objectifs de vos applications exécutées dans le cloud, vous êtes en mesure de détecter les écarts auxquels vous pouvez réagir. La réponse aux incidents de sécurité étant un sujet complexe, nous vous encourageons à consulter les ressources suivantes afin de mieux comprendre l'impact de la réponse aux incidents (IR) et de vos choix sur les objectifs de votre entreprise : guide de réponse aux incidents de AWS sécurité, livre blanc sur les meilleures pratiques de AWS sécurité et livre blanc sur la perspective de sécurité du cadre d'adoption du AWS cloud (CAF).

Amazon Inspector Container Amazon er

Amazon Inspector s'intègre à d'autres AWS services. Ces services peuvent ingérer des données provenant d'Amazon Inspector pour vous permettre de visualiser vos résultats d'une nouvelle manière. Consultez les options d'intégration suivantes pour en savoir plus sur la façon dont ce service est configuré pour fonctionner avec Amazon Inspector.

Intégration d'Amazon Inspector à Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) est un registre de conteneur géré Docker Registry (Amazon ECR) est un registre de conteneur géré Docker Registry (Amazon ECR) est un registre de conteneur géré Docker Registry (Amazon ECR) est un registre de conteneur Amazon ECR héberge vos images de conteneur dans une architecture hautement disponible et scalable. Vous pouvez utiliser Amazon Inspector pour scanner des images de conteneurs résidant dans vos référentiels Amazon ECR à la recherche de packages de système d'exploitation et de packages de langage de programmation vulnérables.

Pour plus d'informations sur l'utilisation d'Amazon ECR avec Amazon ECR avec Amazon Classic er avec Amazon ECR avec Amazon ECR avec Amazon Intégration d'Amazon Inspector à Amazon Elastic Container Registry (Amazon ECR)

Intégration d'Amazon Inspector avec AWS Security Hub

AWS Security Hubcollecte des données de sécurité provenant de vos AWS comptes, services et autres produits pris en charge afin d'évaluer l'état de sécurité de votre environnement conformément aux normes et aux meilleures pratiques du secteur. En plus d'évaluer votre niveau de sécurité, Security Hub crée un emplacement central pour les résultats de tous vos AWS services intégrés et des produits de votre réseau de AWS partenaires. L'activation de Security Hub avec Amazon Inspector permet automatiquement à Security Hub d'ingérer les données de résultats d'Amazon Inspector.

Pour plus d'informations sur l'utilisation de sécurité Hub avec Amazon Hub avec Amazon Hub avec Amazon Hub, veuillez consulterIntégration d'Amazon Inspector avec AWS Security Hub.

Intégration d'Amazon Inspector à Amazon Elastic Container Registry (Amazon ECR)

Amazon ECR est un registre de conteneurs entièrement géré qui prend en charge les images et artefacts Docker et OCI. AWS Si vous utilisez Amazon ECR, vous pouvez activer le scan amélioré pour votre registre afin de permettre à Amazon Inspector de détecter automatiquement les images de vos conteneurs et de les scanner pour détecter les packages de système d'exploitation et de langage de programmation vulnérables.

Cette intégration vous permet de consulter les résultats d'Amazon Inspector relatifs aux images de conteneurs dans la console Amazon ECR. De plus, depuis la console Amazon ECR, vous pouvez gérer la fréquence des scans et affiner l'étendue des scans en créant des filtres d'inclusion.

Activation de l'intégration

Vous pouvez activer l'intégration en activant le scan Amazon Inspector via la console ou l'API Amazon Inspector, ou en configurant votre référentiel pour utiliser le scan amélioré avec Amazon Inspector via la console ou l'API Amazon ECR.

Pour plus d'informations sur l'activation de l'intégration via Amazon Inspector, consultezAnalyse automatisée des ressources avec Amazon Inspector.

Pour plus d'informations sur l'activation et la configuration de la numérisation améliorée dans Amazon ECR, consultez la section Numérisation améliorée dans le guide de l'utilisateur d'Amazon ECR.

Utilisation de l'intégration avec un environnement multi-comptes

Si vous êtes membre d'un environnement multi-comptes, vous pouvez activer le scan amélioré via Amazon ECR. Cependant, une fois activé, il ne peut être désactivé que par votre administrateur délégué Amazon Inspector. S'il est désactivé, il revient au scan de base. Pour plus d'informations, consultez Désactivation d'Amazon Inspector.

Intégration d'Amazon Inspector avec AWS Security Hub

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 les données de sécurité à partir de AWS comptes, de services et de produits de sécurité de sécurité de sécurité à partir des comptes, des services et des produits Vous pouvez

utiliser les informations qu'il fournit pour analyser les tendances en matière de sécurité et pour identifier les problèmes de sécurité prioritaires en matière de sécurité.

L'intégration d'Amazon Inspector avec Security Hub vous permet d'envoyer les résultats d'Amazon Inspector à Security Hub. Security Hub peut ensuite inclure ces résultats dans son analyse de votre posture de sécurité.

Dans AWS Security Hub, les problèmes de sécurité sont suivis en tant que résultats. Certains résultats proviennent de problèmes qui sont détectés par d'autres AWS services ou par des produits 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 les résultats. Pour plus d'informations sur les résultats dans Security Hub, consultez la section Affichage des résultats dans le Guide de AWS Security Hub l'utilisateur. Vous pouvez également suivre le statut d'une analyse dans un résultat. Consultez Prendre des mesures à la suite des résultats dans le Guide de l'utilisateur AWS Security Hub.

Tous les résultats dans 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.

Security Hub archivera les résultats d'Amazon Inspector une fois que ces résultats auront été traités et clôturés dans Amazon Inspector.

Affichage des résultats d'Amazon Inspector dans AWS Security Hub

Les résultats d'Amazon Inspector Classic et du nouvel Amazon Inspector sont disponibles dans le même panneau de Security Hub. Toutefois, vous pouvez filtrer les résultats du nouvel Amazon Inspector en ajoutant un `"aws/inspector/ProductVersion": "2"` à la barre de filtres. L'ajout de ce filtre exclut les résultats d'Amazon Inspector Classic du tableau de bord de Security Hub.

Exemple de recherche tiré d'Amazon Inspector

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "ProductName": "Inspector",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
```

```
  "GeneratorId": "AWSInspector",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ],
  "FirstObservedAt": "2023-01-31T20:25:38Z",
  "LastObservedAt": "2023-05-04T18:18:43Z",
  "CreatedAt": "2023-01-31T20:25:38Z",
  "UpdatedAt": "2023-05-04T18:18:43Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "CVE-2022-34918 - kernel",
  "Description": "An issue was discovered in the Linux kernel through 5.18.9. A type
 confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a
 local attacker to escalate privileges, a different vulnerability than CVE-2022-32250.
 (The attacker can obtain root access, but must start with an unprivileged user
 namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data
 in net/netfilter/nf_tables_api.c.",
  "Remediation": {
    "Recommendation": {
      "Text": "Remediation is available. Please refer to the Fixed version in the
 vulnerability details section above. For detailed remediation guidance for each of the
 affected packages, refer to the vulnerabilities section of the detailed finding JSON."
    }
  },
  "ProductFields": {
    "aws/inspector/FindingStatus": "ACTIVE",
    "aws/inspector/inspectorScore": "7.8",
    "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform":
 "AMAZON_LINUX_2",
    "aws/inspector/ProductVersion": "2",
    "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
      "Partition": "aws",
```

```
      "Region": "us-east-1",
      "Tags": {
        "Patch Group": "SSM",
        "Name": "High-SEv-Test"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-0cff7528ff583bf9a",
          "IpV4Addresses": [
            "52.87.229.97",
            "172.31.57.162"
          ],
          "KeyName": "ACloudGuru",
          "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-9c934cb1",
          "LaunchedAt": "2022-07-26T21:49:46Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "Vulnerabilities": [
    {
      "Id": "CVE-2022-34918",
      "VulnerablePackages": [
        {
          "Name": "kernel",
          "Version": "5.10.118",
          "Epoch": "0",
          "Release": "111.515.amzn2",
          "Architecture": "X86_64",
          "PackageManager": "OS",
          "FixedInVersion": "0:5.10.130-118.517.amzn2",
          "Remediation": "yum update kernel"
        }
      ],
      "Cvss": [
```

```
        {
          "Version": "2.0",
          "BaseScore": 7.2,
          "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD",
          "Adjustments": []
        }
      ],
      "Vendor": {
        "Name": "NVD",
        "Url": "https://nvd.nist.gov/vuln/detail/CVE-2022-34918",
        "VendorSeverity": "HIGH",
        "VendorCreatedAt": "2022-07-04T21:15:00Z",
        "VendorUpdatedAt": "2022-10-26T17:05:00Z"
      },
      "ReferenceUrls": [
        "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?
id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6",
        "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-
d86f4869f452@randorisec.fr/T/",
        "https://www.debian.org/security/2022/dsa-5191"
      ],
      "FixAvailable": "YES"
    }
  ],
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
```

```
  },
  "ProcessedAt": "2023-05-05T20:28:38.822Z"
}
```

Activet configuration de l'intégration de intégration de l'intégration

Pour utiliser l'intégration d'Amazon Inspector avecAWS Security Hub, vous devez activer Security Hub avec l'intégration d'Amazon Inspector avec Amazon Inspector avec, vous Pour plus d'informations sur la façon d'activer Security Hub, veuillez consulter Configuration de Security Hub dans le Guide de AWS Security Hub l'utilisateur.

Lorsque vous activez à la fois Amazon Inspector et Security Hub, l'intégration est activée automatiquement et Amazon Inspector commence à envoyer les résultats à Security Hub. Amazon Inspector envoie tous les résultats qu'il génère à Security Hub dans le format Security Finding Format (ASFF) Amazon Inspector envoie tous les résultats à AWSSecurity Hub dans le format Security Finding Format (ASFF)

Arrêt de la publication des résultats pour AWS Security Hub

Comment arrêter l'envoi des résultats de l'envoi des résultats

Pour arrêter l'envoi des résultats à Security Hub, vous pouvez utiliser la console Security Hub ou l'API.

Veuillez consulter Désactivation et activation du flux de résultats à partir 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 Hubutilisateur.

Systèmes d'exploitation et langages de programmation pris en charge par Amazon Inspector

Amazon Inspector peut scanner les applications logicielles installées sur les instances Amazon Elastic Compute Cloud (Amazon EC2), les images de conteneurs stockées dans les référentiels Amazon Elastic Container Registry (Amazon ECR) et les fonctions. AWS Lambda Pour les images de conteneurs ECR, Amazon Inspector peut détecter les vulnérabilités du système d'exploitation et des packages de langage de programmation. Pour les fonctions Lambda, Amazon Inspector peut détecter les vulnérabilités du code. Lorsqu'Amazon Inspector analyse les ressources, il utilise son propre moteur d'analyse spécialement conçu et extrait plus de 50 flux de données pour générer des résultats sur les vulnérabilités et expositions courantes (CVE). Les sources incluent les avis de sécurité des fournisseurs, le NVD, le MITRE, les flux open source, les recherches internes et les flux de données sous licence.

Pour qu'Amazon Inspector puisse scanner une ressource, celle-ci doit exécuter un système d'exploitation compatible ou utiliser un langage de programmation compatible. Les rubriques de cette section répertorient les systèmes d'exploitation, les environnements d'exécution et les langages de programmation actuellement pris en charge par Amazon Inspector pour différents types de ressources et de scans. Ils répertorient également les systèmes d'exploitation précédemment pris en charge par Amazon Inspector, mais qui ont depuis été abandonnés par les fournisseurs. Amazon Inspector ne peut fournir qu'une assistance limitée pour un système d'exploitation une fois qu'un fournisseur a mis fin au support du système d'exploitation.

Rubriques

Systèmes d'exploitation pris en charge : Amazon EC2 scanning

Le tableau suivant répertorie les systèmes d'exploitation actuellement pris en charge par Amazon Inspector pour les scans des instances Amazon EC2. Il répertorie également la source des avis de sécurité du fournisseur pour chacun d'entre eux et indique si le système d'exploitation peut être scanné à l'aide de la méthode de numérisation avec ou sans agent. Pour plus d'informations sur les méthodes de numérisation, reportez-vous Numérisation basée sur un agent aux sections etNumérisation sans agent.

> **Note**
>
> Les détections du système d'exploitation Linux ne sont prises en charge que pour le référentiel du gestionnaire de packages par défaut et n'incluent pas les applications tierces, les référentiels de support étendu (par exemple, BYOS RHEL, PAYG RHEL et RHEL pour SAP) et les référentiels facultatifs, tels que Red Hat Application Streams.

Système d'exploitation	Version	Conseils de sécurité destinés aux fournisseurs	Support de numérisation sans agent	Support de numérisation basé sur un agent
AlmaLinux	8	ALSA	Oui	Oui
AlmaLinux	9	ALSA	Oui	Oui
Amazon Linux (AL2)	AL2	HÉLAS	Oui	Oui
Amazon Linux 2023 (AL2023)	AL2023	HÉLAS	Oui	Oui
Bottlerocket	1.7.0 et versions ultérieures	GHSA, CVE	Non	Oui
CentOS Linux (CentOS)	7	CESA	Oui	Oui

Système d'exploitation	Version	Conseils de sécurité destinés aux fournisseurs	Support de numérisation sans agent	Support de numérisation basé sur un agent
Serveur Debian (Buster)	10	DSA	Oui	Oui
Serveur Debian (Bullseye)	11	DSA	Oui	Oui
Serveur Debian (Bookworm)	12	DSA	Oui	Oui
Fedora	38	CVE	Oui	Oui
Fedora	39	CVE	Oui	Oui
OpenSUSE	15,5	CVE	Oui	Oui
Oracle Linux (Oracle)	7	ELSA	Oui	Oui
Oracle Linux (Oracle)	8	ELSA	Oui	Oui
Oracle Linux (Oracle)	9	ELSA	Oui	Oui
Red Hat Enterprise Linux (RHEL)	7	RHSA	Oui	Oui
Red Hat Enterprise Linux (RHEL)	8	RHSA	Oui	Oui

Système d'exploitation	Version	Conseils de sécurité destinés aux fournisseurs	Support de numérisation sans agent	Support de numérisation basé sur un agent
Red Hat Enterprise Linux (RHEL)	9	RHSA	Oui	Oui
Rocky Linux	8	RLSA	Oui	Oui
Rocky Linux	9	RLSA	Oui	Oui
SUSE Linux Enterprise Server (SLES)	12.4	GROTTE DE SUSE	Oui	Oui
SUSE Linux Enterprise Server (SLES)	12,5	GROTTE DE SUSE	Oui	Oui
SUSE Linux Enterprise Server (SLES)	15,3	GROTTE DE SUSE	Oui	Oui
SUSE Linux Enterprise Server (SLES)	15,4	GROTTE DE SUSE	Oui	Oui
SUSE Linux Enterprise Server (SLES)	15,5	GROTTE DE SUSE	Oui	Oui
Ubuntu (Fidèle)	14,04 (ESM)	USB, Ubuntu Pro	Oui	Oui
Ubuntu (Xenial)	16,04 (ESM)	USB, Ubuntu Pro	Oui	Oui
Ubuntu (Bionic)	18,04 (ESM)	USB, Ubuntu Pro	Oui	Oui

Système d'exploitation	Version	Conseils de sécurité destinés aux fournisseurs	Support de numérisation sans agent	Support de numérisation basé sur un agent
Ubuntu (Focal)	20.04 (LITRES)	USN	Oui	Oui
Ubuntu (Jammy)	22.04 (LITRES)	USN	Oui	Oui
Ubuntu (Minotaure mantique)	23,10	USN	Oui	Oui
Windows Server	2016	MSKB	Non	Oui
Windows Server	2019	MSKB	Non	Oui
Windows Server	2022	MSKB	Non	Oui
macOS (Mojave)	10.14	APPLE-SA	Non	Oui
macOS (Catalina)	10.15	APPLE-SA	Non	Oui
macOS (Big Sur)	11	APPLE-SA	Non	Oui
macOS (Monterey)	12	APPLE-SA	Non	Oui
macOS (Ventura)	13	APPLE-SA	Non	Oui

Langages de programmation pris en charge : Amazon EC2 Deep Inspection

Amazon Inspector prend actuellement en charge les langages de programmation suivants lors de l'analyse des instances Linux Amazon EC2 à la recherche de vulnérabilités dans des progiciels tiers :

- Java

- JavaScript
- Python

Amazon Inspector utilise Systems Manager Distributor pour déployer le plug-in utilisé pour l'inspection approfondie dans votre instance Amazon EC2. Systems Manager Distributor prend en charge les systèmes d'exploitation répertoriés dans la catégorie Plateformes et architectures de packages pris en charge dans le guide Systems Manager. Le système d'exploitation de votre instance Amazon EC2 doit être pris en charge par Systems Manager Distributor et Amazon Inspector pour qu'Amazon Inspector puisse effectuer des analyses d'inspection approfondies.

> **Note**
>
> L'inspection approfondie n'est pas prise en charge pour les systèmes d'exploitation Bottlerocket.

Systèmes d'exploitation pris en charge : scan CIS

Le tableau suivant répertorie les systèmes d'exploitation actuellement pris en charge par Amazon Inspector pour les scans CIS. Le tableau inclut également la version de référence CIS utilisée pour effectuer des analyses de ce système d'exploitation.

Système d'exploitation	Version	Version de référence CIS
Amazon Linux 2	AL2	2.0.0
Amazon Linux 2023	AL2023	1.0.0
Windows Server	2019	2.0.0
Windows Server	2022	2.0.0

Systèmes d'exploitation pris en charge : numérisation Amazon ECR avec Amazon Inspector

Amazon Inspector prend actuellement en charge l'analyse des systèmes d'exploitation suivants lors de la numérisation d'images de conteneurs dans les référentiels Amazon ECR :. Le tableau répertorie également la source des avis de sécurité du fournisseur pour chaque système d'exploitation.

Système d’exploitation	Version	Conseils de sécurité destinés aux fournisseurs
Alpine Linux (Alpine)	3.16	Alpine SecDB
Alpine Linux (Alpine)	3.17	Alpine SecDB
Alpine Linux (Alpine)	3.18	Alpine SecDB
Alpine Linux (Alpine)	3.19	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
CentOS Linux (CentOS)	7	CESA
Debian Server (Buster)	10	DSA
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA
Fedora	38	CVE
Fedora	39	CVE
OpenSUSE	15.5	CVE

Système d'exploitation	Version	Conseils de sécurité destinés aux fournisseurs
Oracle Linux (Oracle)	7	ELSA
Oracle Linux (Oracle)	8	ELSA
Oracle Linux (Oracle)	9	ELSA
Photon OS	3	PHSA
Photon OS	4	PHSA
Photon OS	5	PHSA
Red Hat Enterprise Linux (RHEL)	7	RHSA
Red Hat Enterprise Linux (RHEL)	8	RHSA
Red Hat Enterprise Linux (RHEL)	9	RHSA
Rocky Linux	8	RLSA
Rocky Linux	9	RLSA
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12.5	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE

Système d'exploitation	Version	Conseils de sécurité destinés aux fournisseurs
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE
Ubuntu (Trusty)	14.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Focal)	20.04 (LTS)	USN
Ubuntu (Jammy)	22.04 (LTS)	USN
Ubuntu (Mantic Minotaur)	23.10	USN

Langages de programmation pris en charge : Amazon ECR scan

Amazon Inspector prend actuellement en charge les langages de programmation suivants lors de la numérisation d'images de conteneurs dans les référentiels Amazon ECR :

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

Runtimes pris en charge : analyse standard Amazon Inspector Lambda

L'analyse standard Amazon Inspector Lambda prend actuellement en charge les langages de programmation suivants lors de l'analyse des fonctions Lambda à la recherche de vulnérabilités dans des progiciels tiers :

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

Runtimes pris en charge : analyse du code Lambda par Amazon Inspector

L'analyse de code Lambda par Amazon Inspector prend actuellement en charge les langages de programmation suivants lors de l'analyse des fonctions Lambda pour détecter des vulnérabilités dans le code :

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Ruby
  - ruby2.7
  - ruby3.2

Systèmes d'exploitation abandonnés

Le support standard du fournisseur pour les systèmes d'exploitation répertoriés dans les tableaux suivants a été interrompu par le fournisseur. Dans les tableaux, la colonne Discontinué indique à quel moment le fournisseur a interrompu le support standard d'un système d'exploitation.

Amazon Inspector a précédemment fourni un support complet pour ces systèmes d'exploitation et continuera à scanner les instances Amazon EC2 et les images des conteneurs Amazon ECR qui les exécutent. Toutefois, conformément à la politique du fournisseur, les systèmes d'exploitation ne sont plus mis à jour avec des correctifs et, dans de nombreux cas, de nouveaux avis de sécurité ne sont plus publiés à leur sujet. En outre, certains fournisseurs suppriment les alertes de sécurité et les détections existantes de leurs flux lorsqu'un système d'exploitation concerné atteint la fin du support standard. Par conséquent, Amazon Inspector peut cesser de générer des résultats pour les CVE connus. Tous les résultats générés par Amazon Inspector concernant un système d'exploitation abandonné doivent être utilisés à titre informatif uniquement.

En tant que bonne pratique en matière de sécurité et pour continuer à bénéficier d'une couverture Amazon Inspector, nous vous encourageons à passer à une version actuelle et prise en charge d'un système d'exploitation.

Systèmes d'exploitation abandonnés : analyse Amazon EC2

Système d'exploitation	Version	Interrompu
Amazon Linux (AL1)	2012	31 décembre 2021
CentOS Linux (CentOS)	8	31 décembre 2021
Serveur Debian (Stretch)	9	30 juin 2022
Fedora	35	13 décembre 2022
Fedora	36	16 mai 2023
Fedora	37	5 décembre 2023
OpenSUSE	15.3	1er décembre 2022
OpenSUSE	15,4	7 décembre 2023

Système d'exploitation	Version	Interrompu
openSUSE Leap (SUSE Leap)	15,2	1er décembre 2021
Oracle Linux (Oracle)	6	1er mars 2021
SUSE Linux Enterprise Server (SLES)	12	1 juillet 2019
SUSE Linux Enterprise Server (SLES)	12.1	31 mai 2020
SUSE Linux Enterprise Server (SLES)	12.2	31 mars 2021
SUSE Linux Enterprise Server (SLES)	12.3	30 juin 2022
SUSE Linux Enterprise Server (SLES)	15	31 décembre 2019
SUSE Linux Enterprise Server (SLES)	15.1	31 janvier 2021
SUSE Linux Enterprise Server (SLES)	15,2	31 décembre 2021
Ubuntu (Groovy)	20,10	22 juillet 2021
Ubuntu (Hirsute)	21,04	20 janvier 2022
Ubuntu (Impish)	21,10	31 juillet 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024
Windows Server	2012	10 octobre 2023
Windows Server	2012 R2	10 octobre 2023

Systèmes d'exploitation abandonnés : analyse Amazon ECR

Système d'exploitation	Version	Interrompu
Alpine Linux (Alpine)	3,12	1er mai 2022
Alpine Linux (Alpine)	3.13	1er novembre 2022
Alpine Linux (Alpine)	3.14	May 1, 2023
Alpine Linux (Alpine)	3.15	November 1, 2023
Amazon Linux (AL1)	2012	31 décembre 2021
CentOS Linux (CentOS)	8	31 décembre 2021
Serveur Debian (Stretch)	9	30 juin 2022
Fedora	35	13 décembre 2022
Fedora	36	16 mai 2023
OpenSUSE	15.3	1er décembre 2022
OpenSUSE	15.4	December 7, 2023
openSUSE Leap (SUSE Leap)	15,2	1er décembre 2021
Oracle Linux (Oracle)	6	1er mars 2021
SUSE Linux Enterprise Server (SLES)	12	1 juillet 2019
SUSE Linux Enterprise Server (SLES)	12.1	31 mai 2020
SUSE Linux Enterprise Server (SLES)	12.2	31 mars 2021
SUSE Linux Enterprise Server (SLES)	12.3	30 juin 2022

Système d'exploitation	Version	Interrompu
SUSE Linux Enterprise Server (SLES)	15	31 décembre 2019
SUSE Linux Enterprise Server (SLES)	15.1	31 janvier 2021
SUSE Linux Enterprise Server (SLES)	15,2	31 décembre 2021
Ubuntu (Groovy)	20,10	22 juillet 2021
Ubuntu (Hirsute)	21,04	20 janvier 2022
Ubuntu (Impish)	21,10	31 juillet 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024

Désactivation d'Amazon Inspector

Vous pouvez désactiver Amazon Inspector dans n'importe quel endroit à l'aide Région AWS de la console ou de l'API Amazon Inspector. Suivez les instructions à la fin de cette rubrique pour désactiver Amazon Inspector. Si vous désactivez tous les scans Amazon Inspector pour unCompte AWS, Amazon Inspector est automatiquement désactivé pour ce compte. Pour plus d'informations sur la désactivation des types de scans pour différentes ressources, consultezAnalyse automatisée des ressources avec Amazon Inspector.

Une fois Amazon Inspector désactivé pour un compte, tous les types de scan sont désactivés pour ce compte dans cette région. En outre, tous les paramètres de scan, les règles de suppression, les filtres et les résultats d'Amazon Inspector relatifs au compte de cette région sont supprimés.

L'utilisation d'Amazon Inspector ne vous est pas facturée lorsque celui-ci est désactivé pour votre compte dans cette région. Après avoir désactivé Amazon Inspector, vous pouvez choisir de le réactiver ultérieurement.

> **Note**
>
> Avant de désactiver Amazon Inspector, nous vous recommandons d'exporter vos résultats. Pour plus d'informations, consultez Exportation de rapports de résultats depuis Amazon Inspector.

Lorsque vous désactivez le scan Amazon EC2 par Amazon Inspector, les associations SSM suivantes utilisées par Amazon Inspector sont supprimées :

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`. En outre, le plug-in Amazon Inspector SSM installé via cette association est supprimé de tous vos Windows hôtes. Pour plus d'informations, consultez WindowsInstances de numérisation.

Prérequis

En fonction de votre type de compte, vous devrez peut-être prendre les mesures supplémentaires suivantes avant de désactiver Amazon Inspector :

- Si vous possédez un compte Amazon Inspector autonome, vous pouvez le désactiver à tout moment.
- Si vous êtes membre dans un environnement multi-comptes Amazon Inspector, vous ne pouvez pas désactiver votre propre service. Vous devez contacter l'administrateur délégué de votre organisation pour désactiver votre service.
- Si vous êtes un administrateur délégué, vous devez dissocier tous les comptes de vos membres avant de pouvoir désactiver Amazon Inspector. Pour plus d'informations, consultez Dissociation des comptes membres dans Amazon Inspector.

> **Note**
>
> La dissociation d'un compte ne désactive pas Amazon Inspector pour ce compte, mais un compte de membre dissocié devient un compte autonome.

> **Note**
>
> Lorsque vous désactivez Amazon Inspector en tant qu'administrateur délégué, la fonctionnalité d'activation automatique est désactivée pour votre organisation.

Désactiver Amazon Inspector

Console

Pour désactiver Amazon Inspector

1. Ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/v2/home.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, choisissez la région dans laquelle vous souhaitez désactiver Amazon Inspector.
3. Dans le volet de navigation, sélectionnez Paramètres généraux.
4. Choisissez Deactivate Inspector.
5. Lorsque vous êtes invité à confirmer, entrez deactivate dans la zone de texte, puis choisissez Deactivate Inspector.

6. (Recommandé) Répétez ces étapes dans chaque région pour laquelle vous souhaitez désactiver Amazon Inspector.

API

Exécutez l'opération Disable API. Dans la demande, indiquez les identifiants de compte que vous désactivez et indiquez `EC2, ECR, LAMBDA` `resourceTypes` pour désactiver tous les scans, ce qui désactivera le compte.

Quotas pour Amazon Inspector

Votre AWS compte dispose des quotas suivants pour Amazon Inspector par région.

Ressource	Par défaut	Commentaires
Règles de suppression	500	Le nombre maximum de règles de suppression enregistrées par AWS compte et par région. Vous ne pouvez pas demander d'augmentation de quota.
Conclusions du réseau Amazon EC2	10 000	Le nombre maximum de découvertes sur le réseau Amazon EC2 par compte. AWS Vous ne pouvez pas demander d'augmentation de quota.
Comptes membres	10 000	Le nombre maximum de comptes membres associés à un compte d'administrateur délégué Amazon Inspector. Cette limite est basée surAWS Organizations, voir Quotas pour AWS Organizations.

Ressource	Par défaut	Commentaires
Configurations de numérisation CIS	500	Nombre maximal de configurations de scan CIS. Vous ne pouvez pas demander d'augmentation de quota.

Pour obtenir la liste des quotas associés à Amazon Inspector Classic, consultez la section Quotas de service Amazon Inspector dans le Références générales AWS.

Pour obtenir la liste des quotas associés aux Organizations, consultez la section Quotas de service Organizations dans le Références générales AWS.

Régions et points de terminaison

Le scan sans agent Amazon Inspector pour Amazon EC2 est disponible en version préliminaire. Votre utilisation de la fonctionnalité de numérisation sans agent Amazon EC2 est soumise à la section 2 des conditions de AWSservice (« Bêtas et aperçus »).

Pour savoir Régions AWS où Amazon Inspector est disponible, consultez la section Points de terminaison Amazon Inspector dans le Référence générale d'Amazon Web Services.

Points de terminaison pour l'API Amazon Inspector Scan

Le tableau suivant indique les points de terminaison régionaux qui peuvent être utilisés lors de l'appel de l'API Amazon Inspector Scan. Lorsque vous utilisez l'API, vous devez fournir le point de terminaison et la région correspondante pour la AWS région dans laquelle vous êtes actuellement authentifié.

La convention de dénomination des points de terminaison Amazon Inspector Scan est`inspector-scan.`*`region`*`.amazonaws.com`. Par exemple, si vous êtes authentifié`us-west-2`, vous utiliserez le point de terminaison `inspector-scan.us-west-2.amazonaws.com` pour appeler l'`inspector-scan`API.

Nom de la région	Région	Point de terminaison	Protocole
USA Est (Ohio)	us-east-2	inspector-scan.us-east-2.amazonaws.com inspector-scan-fips.us-east-2.amazonaws.com	HTTPS
US East (Virginie du Nord)	us-east-1	inspector-scan.us-east-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
		inspector-scan-fips.us-east-1.amazonaws.com	
USA Ouest (Californie du Nord)	us-west-1	inspector-scan.us-west-1.amazonaws.com inspector-scan-fips.us-west-1.amazonaws.com	HTTPS
USA Ouest (Oregon)	us-west-2	inspector-scan.us-west-2.amazonaws.com inspector-scan-fips.us-west-2.amazonaws.com	HTTPS
Afrique (Le Cap)	af-south-1	inspector-scan.af-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	inspector-scan.ap-east-1.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	inspector-scan.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Mumbai)	ap-south-1	inspector-scan.ap-south-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asie-Pacifique (Osaka)	ap-northeast-3	inspector-scan.ap-northeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Séoul)	ap-northeast-2	inspector-scan.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	inspector-scan.ap-southeast-1.amazonaws.com	HTTPS
Asie-Pacifique (Sydney)	ap-southeast-2	inspector-scan.ap-southeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Tokyo)	ap-northeast-1	inspector-scan.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centre)	ca-central-1	inspector-scan.ca-central-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	inspector-scan.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	inspector-scan.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	inspector-scan.eu-west-2.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Milan)	eu-south-1	inspector-scan.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	inspector-scan.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	inspector-scan.eu-north-1.amazonaws.com	HTTPS
Europe (Zurich)	eu-central-2	inspector-scan.eu-central-2.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	inspector-scan.me-south-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	inspector-scan.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	inspecteur-scan.us-gov-east-1.amazonaws.com inspector-scan-fips. us-gov-east-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
AWS GovCloud (US-Ouest)	us-gov-west-1	inspecteur-scan.us-gov-west-1.amazonaws.com inspector-scan-fips. us-gov-west-1.amazonaws.com	HTTPS

Disponibilité des fonctionnalités propres à la région

Cette section décrit la disponibilité des fonctionnalités d'Amazon Inspector parRégion AWS.

Numérisation EC2 sans agent pour les régions Amazon EC2

Le tableau suivant indique les domaines dans Régions AWS lesquels le scan sans agent pour Amazon EC2 est actuellement disponible.

Nom de la région	Code région
US East (Virginie du Nord)	us-east-1
USA Ouest (Oregon)	us-west-2
Europe (Irlande)	eu-west-1

Régions de numérisation de code Lambda

Le tableau suivant indique les Régions AWS endroits où le scan de code Lambda est actuellement disponible.

Nom de la région	Code région
US East (Virginie du Nord)	us-east-1
USA Ouest (Oregon)	us-west-2

Nom de la région	Code région
USA Est (Ohio)	us-east-2
Asie-Pacifique (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Europe (Francfort)	eu-central-1
Europe (Irlande)	eu-west-1
Europe (Londres)	eu-west-2
Europe (Stockholm)	eu-north-1
Asie-Pacifique (Singapour)	ap-southeast-1

Régions AWS GovCloud (US)

Pour obtenir les dernières informations, consultez Amazon Inspector dans le guide de AWS GovCloud (US) l'utilisateur.

Historique du document pour le guide de l'utilisateur d'Amazon Inspector

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version d'Amazon Inspector. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Fonctionnalités mises à jour	Amazon Inspector fait passer la période de conservation des résultats fermés de 30 jours à 7 jours. Pour plus d'informations, consultez Comprendre les résultats dans Amazon Inspector.	12 février 2024
Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2ServiceRolePolicypolitique. La nouvelle instruction permet à Amazon Inspector de lancer des scans CIS pour votre instance.	23 janvier 2024
Nouvelle politique	Amazon Inspector a ajouté une nouvelle politique, la AmazonInspector2ManagedCisPolicypolitique, que vous pouvez utiliser dans le cadre d'un profil d'instance pour autoriser les scans CIS sur une instance.	23 janvier 2024
Nouvelle fonctionnalité	Amazon Inspector actualise désormais la durée de	23 janvier 2024

	nouvelle numérisation ECR des images du conteneur lorsque vous les extrayez. Pour modifier la durée de votre nouvelle numérisation en fonction des dates d'envoi ou d'extraction, voir Configuration de la durée de nouvelle numérisation ECR.	
Nouvelle fonctionnalité	Amazon Inspector peut désormais exécuter des scans du Center for Internet Security (CIS) sur les instances EC2. Pour plus d'informations, consultez Amazon Inspector CIS scans.	23 janvier 2024
Nouvelle fonctionnalité	Amazon Inspector peut désormais numériser des images de conteneurs dans vos pipelines CI/CD. Pour plus d'informations, consultez la section Intégration de CI/CD à Amazon Inspector.	30 novembre 2023
Nouvelle politique	Amazon Inspector a ajouté une nouvelle politique qui permet à Amazon Inspector de scanner les instantanés Amazon EBS depuis votre instance EC2 pour une analyse sans agent. Pour plus d'informations sur cette politique, consultez la section Analyse sans agent.	27 novembre 2023

Nouvelle fonctionnalité	Amazon Inspector prend désormais en charge l'analyse des instances Linux Amazon EC2 prises en charge sans agents SSM via une analyse sans agent. Pour plus d'informations, consultez la section Numérisation sans agent.	27 novembre 2023
Nouvelles ressources prises en charge	Amazon Inspector prend désormais en charge l'analyse des instances macOS Amazon EC2. Voir Systèmes d'exploitation pris en charge : Amazon EC2 analyse les versions de macOS prises en charge.	5 octobre 2023
Nouvelles régions	Amazon Inspector est désormais disponible en Asie-Pacifique (Jakarta), en Afrique (Le Cap), en Asie-Pacifique (Osaka) et en Europe (Zurich).	29 septembre 2023
Nouvelle fonction	Vous pouvez désormais exclure les instances EC2 des scans Amazon Inspector à l'aide de balises d'exclusion.	14 septembre 2023
Nouvelle fonction	Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector de scanner les configurations réseau des instances Amazon EC2 qui font partie des groupes cibles d'Elastic Load Balancing.	31 août 2023

Nouvelle fonction	Amazon Inspector fournit désormais des informations détaillées sur les vulnérabilités pour détecter les vulnérabilités des packages.	31 juillet 2023
Fonctionnalités mises à jour	Amazon Inspector a ajouté de nouvelles autorisations qui permettent aux utilisateurs en lecture seule d'exporter une nomenclature logicielle (SBOM) pour leurs ressources.	29 juin 2023
Nouvelle fonction	Vous pouvez désormais exporter le SBOM pour les ressources analysées par Amazon Inspector.	13 juin 2023
Nouvelle fonction	Le scan de code Lambda est désormais généralement disponible. De nouvelles fonctionnalités ont été ajoutées pour vous permettre de chiffrer le code identifié dans les résultats de votre analyse de code Lambda. En outre, le scan de code Lambda propose désormais des suggestions de réécriture corrective de votre code.	13 juin 2023

Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2ReadOnlyAccesspolitique. Les nouvelles instructions permettent aux utilisateurs en lecture seule de récupérer des informations sur l'état et les résultats de l'analyse du code Lambda pour leur compte.	2 mai 2023
Nouvelle fonction	Amazon Inspector a ajouté une fonction de recherche dans la base de données des vulnérabilités qui vous permet de vérifier si Amazon Inspector couvre un CVE spécifique.	1er mai 2023
Fonctionnalités mises à jour	Amazon Inspector a ajouté de nouvelles autorisations à la AmazonInspector2ServiceRolePolicypolitique qui permettent à Amazon Inspector de créer des canaux AWS CloudTrail liés à un service dans votre compte lorsque vous activez le scan Lambda. Cela permet à Amazon Inspector de surveiller CloudTrail les événements de votre compte.	30 avril 2023

Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2FullAccesspolitique. La nouvelle déclaration permet aux utilisateurs de récupérer des informations détaillées sur les vulnérabilités du code détectées lors de l'analyse du code Lambda.	17 avril 2023
Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2ServiceRolePolicypolitique. La nouvelle déclaration permet à Amazon Inspector d'envoyer des informations à Amazon EC2 Systems Manager concernant les chemins personnalisés que vous avez définis pour l'inspection approfondie d'Amazon EC2.	17 avril 2023
Nouvelle fonction	Amazon Inspector ajoute une prise en charge supplémentaire pour les instances Linux EC2 sous la forme d'une inspection approfondie d'Amazon Inspector, qui analyse vos instances pour détecter les vulnérabilités des packages dans les packages de langage de programmation d'applications.	17 avril 2023

Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2ServiceRolePolicypolitique. Les nouvelles instructions permettent à Amazon Inspector de demander des scans du code du développeur dans AWS Lambda les fonctions et de recevoir des données de scan d'Amazon CodeGuru Security. Amazon Inspector a également ajouté des autorisations permettant de consulter les politiques IAM. Amazon Inspector utilise ces informations pour analyser les fonctions Lambda afin de détecter les vulnérabilités du code.	28 février 2023
Nouvelle fonction	Amazon Inspector ajoute une prise en charge supplémentaire pour les fonctions Lambda sous la forme d'un scan de code Lambda, qui analyse le code de développeur de vos fonctions Lambda pour détecter les failles de sécurité.	28 février 2023

Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2ServiceRolePolicypolitique. La nouvelle instruction permet à Amazon Inspector de CloudWatch récupérer des informations relatives à la date à laquelle une AWS Lambda fonction a été invoquée pour la dernière fois. Elle utilise ces informations pour concentrer les analyses sur les fonctions Lambda de votre environnement qui ont été actives au cours des 90 derniers jours.	20 février 2023
Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2ServiceRolePolicypolitique. La nouvelle déclaration permet à Amazon Inspector de récupérer des informations sur vos AWS Lambda fonctions. Amazon Inspector utilise ces informations pour analyser vos fonctions Lambda afin de détecter les failles de sécurité.	28 novembre 2022
Nouvelle fonction	Amazon Inspector ajoute la prise en charge des AWS Lambdafonctions de numérisation.	28 novembre 2022

Contenu mis à jour	Ajout de procédures, d'exemples de politiques et de conseils pour exporter les rapports de résultats d'Amazon Inspector vers un bucket Amazon Simple Storage Service (Amazon S3).	14 octobre 2022
Nouveau contenu	Ajout d'informations sur l'évaluation de la couverture de votre AWS environnement par Amazon Inspector à l'aide de la console Amazon Inspector. Les informations incluent des descriptions des valeurs d'état pour les ressources individuelles de votre environnement.	7 octobre 2022

Nouvelle fonction	Amazon Inspector fournit désormais des informations supplémentaires sur la manière de remédier aux vulnérabilités des packages. De nouveaux champs ont été ajoutés aux informations de recherche. Les nouveaux champs fournissent un contexte indiquant si un correctif est disponible par le biais d'une mise à jour du package. Si un correctif est disponible, la section Remédiation suggérée d'une recherche indique les commandes que vous pouvez exécuter pour effectuer le correctif.	2 septembre 2022

Fonctionnalités mises à jour	Amazon Inspector a ajouté une nouvelle action à la AmazonInspector2ServiceRolePolicypolitique. La nouvelle action permet à Amazon Inspector de décrire les exécutions d'associations SSM. Amazon Inspector a également ajouté un périmètre de ressources supplémentaire pour permettre à Amazon Inspector de créer, mettre à jour, supprimer et démarrer des associations SSM avec des documents SSM `AmazonInspector2` détenus.	31 août 2022
Nouvelle fonction	Amazon Inspector prend désormais en charge les scans pour Windows les instances. Amazon Inspector peut désormais scanner les instances gérées par SSM exécutant des systèmes Windows d'exploitation pris en charge. Les scans des Windows hôtes sont effectués par le plugin Amazon Inspector SSM, qui est installé et invoqué via de nouvelles associations SSM créées automatiquement par Amazon Inspector.	31 août 2022

Fonctionnalités mises à jour	Amazon Inspector a mis à jour le périmètre des ressources de la AmazonInspector2ServiceRolePolicypolitique afin de permettre à Amazon Inspector de collecter l'inventaire des logiciels dans d'autres AWS partitions.	12 août 2022
Fonctionnalités mises à jour	Dans cette AmazonInspector2ServiceRolePolicypolitique, Amazon Inspector a restructuré le périmètre des ressources des actions permettant à Amazon Inspector de créer, de supprimer et de mettre à jour des associations SSM.	10 août 2022

Nouvelle fonction	Amazon Inspector prend désormais en charge la modification de votre paramètre de durée de nouvelle analyse automatique ECR. Le paramètre de durée de numérisation automatiq ue Amazon ECR détermine la durée pendant laquelle Amazon Inspector surveille en permanence les images introduites dans des référenti els. Lorsqu'une image est plus ancienne que la durée de numérisation, Amazon Inspector ne numérise plus l'image et ferme tous les résultats existants. La durée de réanalyse automatique de tous les nouveaux comptes sera automatiquement définie sur la durée de vie. Les comptes créés précédemment bénéficiaient d'une durée de réanalyse automatique ECR de 30 jours, mais vous pouvez désormais choisir entre une durée de 30 jours, 180 jours ou à vie pour les scans.	25 juin 2022

Nouvelles fonctionnalités	Amazon Inspector a ajouté une nouvelle politique AWS gérée, la AmazonInspector2ReadOnlyAccesspolitique, pour autoriser l'accès en lecture seule aux fonctionnalités d'Amazon Inspector.	21 janvier 2022
Disponibilité générale	Il s'agit de la première version publique du guide de l'utilisateur d'Amazon Inspector.	29 novembre 2021

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.