aws

Guide de l’utilisateur

# Amazon Inspector

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Inspector: Guide de l’utilisateur

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

# Table of Contents

# Qu'est-ce qu'Amazon Inspector ?

Amazon Inspector est un service de gestion des vulnérabilités qui découvre automatiquement les charges de travail et les analyse en permanence pour détecter les vulnérabilités logicielles et les risques d'exposition involontaire au réseau. Amazon Inspector découvre et analyse les EC2 instances Amazon, les images de conteneurs dans Amazon ECR et les fonctions Lambda. Lorsqu'Amazon Inspector détecte une vulnérabilité logicielle ou une exposition involontaire au réseau, il crée une constatation, qui consiste en un rapport détaillé sur le problème. Vous pouvez gérer les résultats dans la console ou l'API Amazon Inspector.

Rubriques



## Caractéristiques d'Amazon Inspector

Gérez de manière centralisée plusieurs comptes Amazon Inspector

Si votre AWS environnement comporte plusieurs comptes, vous pouvez le gérer de manière centralisée par le biais d'un seul compte en utilisant AWS Organizations. En utilisant cette approche, vous pouvez désigner un compte comme compte d'administrateur délégué pour 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 futurs membres chaque fois qu'ils rejoignent votre organisation. Le compte d'administrateur délégué Amazon Inspector peut gérer les données relatives aux résultats et certains paramètres pour les membres de l'organisation. Cela inclut l'affichage des détails des résultats agrégés pour tous les comptes membres, l'activation ou la désactivation des scans pour les comptes membres et l'examen des ressources numérisées au sein de l' AWS organisation.

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

Avec Amazon Inspector, vous n'avez pas besoin de planifier ou de configurer manuellement les scans d'évaluation. Amazon Inspector découvre et commence à analyser automatiquement vos ressources éligibles. Amazon Inspector continue d'évaluer votre environnement tout au long du cycle de vie de vos ressources en réanalysant automatiquement les ressources en réponse à

des modifications susceptibles d'introduire une nouvelle vulnérabilité, telles que l'installation d'un nouveau package dans une EC2 instance, l'installation d'un correctif et la publication d'une nouvelle vulnérabilité et exposition commune (CVE) ayant un impact sur la ressource. Contrairement aux logiciels de numérisation de sécurité traditionnels, Amazon Inspector a un impact minimal sur les performances de votre flotte.

Lorsque des vulnérabilités ou des chemins réseau ouverts sont identifiés, Amazon Inspector produit un résultat que vous pouvez examiner. Le résultat inclut des informations complètes sur la vulnérabilité, la ressource affectée et des recommandations de correction. Si vous corrigez un résultat de manière appropriée, Amazon Inspector détecte automatiquement le correctif et ferme le résultat.

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

Dans la mesure où Amazon Inspector collecte des informations sur votre environnement par le biais de scans, il fournit des scores de gravité spécifiquement adaptés à votre environnement. Amazon Inspector examine les indicateurs 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 réduire le score Amazon Inspector d'une recherche concernant une EC2 instance Amazon 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 est une modification du score CVSS (Common Vulnerability Scoring System) de base fourni par le NVD.

Identifiez les résultats à fort impact grâce au 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. Depuis le tableau de bord, vous pouvez accéder aux détails détaillés d'une constatation. Le tableau de bord contient des informations rationalisées sur la couverture des scans dans votre environnement, vos résultats les plus critiques et les ressources qui en contiennent le plus. Le panneau de correction basé sur les risques du tableau de bord Amazon Inspector présente les résultats qui affectent 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 de passer en revue 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 le détail des résultats individuels.

Vous pouvez consulter les résultats regroupés par catégorie ou par type de vulnérabilité. Dans chaque affichage, 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 pour 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.

Surveiller et traiter 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 la forme d'événements de recherche. EventBridge est un service de bus d'événements sans serveur qui peut acheminer les données de résultats vers des cibles telles que 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 existants en matière de sécurité et de conformité. 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 niveau de sécurité dans l'ensemble de votre AWS environnement et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub vous permet de surveiller et de traiter plus facilement vos résultats dans le cadre d'une analyse plus large du niveau de sécurité de votre entreprise dans AWS.

# Accès à Amazon Inspector

Amazon Inspector est disponible dans la plupart des cas Régions AWS. Pour obtenir la liste des régions dans lesquelles Amazon Inspector est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Inspector dans le manuel Amazon Web Services General Reference. Pour en savoir plus Régions AWS, consultez la section Gestion Régions AWS dans le manuel Amazon Web Services General Reference. Dans chaque région, vous pouvez utiliser Amazon Inspector de la manière suivante.

AWS Console de gestion

AWS Management Console Il 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 tâches Amazon Inspector depuis la console Amazon Inspector.

### AWS outils de ligne de commande

Grâce aux outils de ligne de AWS commande, vous pouvez émettre des commandes sur la ligne de commande de votre système pour effectuer des tâches Amazon Inspector. L'utilisation de la ligne de commande peut être plus rapide et plus pratique que celle de la console. Les outils de ligne de commande sont également utiles si vous souhaitez créer des scripts exécutant des tâches .

AWS fournit deux ensembles d'outils de ligne de commande : le AWS Command Line Interface (AWS CLI) et le Outils AWS pour PowerShell. Pour plus d'informations sur l'installation et l'utilisation de AWS CLI, consultez le Guide de l'utilisateur de l'interface de ligne de AWS commande. Pour plus d'informations sur l'installation et l'utilisation des outils pour PowerShell, consultez le guide de Outils AWS pour PowerShell l'utilisateur.

### AWS SDKs

AWS fournit SDKs des bibliothèques et des exemples de code pour divers langages de programmation et plateformes, notamment Java, Go, Python, C++ et .NET. Ils SDKs fournissent un accès pratique et programmatique à Amazon Inspector et à d'autres Services AWS. Ils gèrent également des tâches telles que la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations sur l'installation et l'utilisation du AWS SDKs, voir Outils sur lesquels s'appuyer AWS.

### API REST Amazon Inspector

L'API REST Amazon Inspector vous donne un accès complet et programmatique à votre compte et à vos ressources Amazon Inspector. Avec cette API, vous pouvez envoyer des requêtes HTTPS directement à Amazon Inspector. Cependant, contrairement aux outils de ligne de AWS commande SDKs, l'utilisation de cette API nécessite que votre application gère des détails de bas niveau tels que la génération d'un hachage pour signer une demande.

# Commencer à utiliser Amazon Inspector

Cette section fournit des informations à prendre en compte avant d'activer Amazon Inspector ainsi qu'un didacticiel de démarrage expliquant comment activer Amazon Inspector et consulter vos résultats dans la console Amazon Inspector et avec l'API Amazon Inspector.

Rubriques



## Avant d'activer Amazon Inspector

Avant d'activer Amazon Inspector, prenez en compte les points suivants :

Amazon Inspector est un service régional

Vos données sont stockées dans l' Région AWS endroit où vous activez Amazon Inspector. Répétez les étapes décrites dans la première partie du didacticiel de mise en route pour tous les Régions AWS sites où vous prévoyez d'utiliser Amazon Inspector.

Amazon Inspector crée les rôles liés au service AWSService RoleForAmazonInspector 2 et 2Agentless AWSService RoleForAmazonInspector

Un rôle lié à un service est un rôle dans AWS Identity and Access Management (IAM) lié à un service. AWS AWSServiceRoleForAmazonInspector2 et AWSServiceRoleForAmazonInspector2Agentless permettent à Amazon Inspector d'accéder aux données Services AWS nécessaires pour effectuer des évaluations de sécurité.

Les identités IAM dotées d'autorisations d'administrateur peuvent activer Amazon Inspector

Protégez vos informations d'identification en créant des utilisateurs avec IAM ou AWS IAM Identity Center. Cela vous permet de vous assurer que les utilisateurs disposent uniquement des autorisations requises pour gérer Amazon Inspector. Pour plus d'informations, consultez la section Politique AWS gérée : AmazonInspectorFullAccess.

La numérisation hybride est automatiquement activée

Le scan hybride inclut le scan basé sur un agent et le scan sans agent. Par défaut, Amazon Inspector utilise ces méthodes de scan sur toutes les EC2 instances Amazon éligibles. Pour plus d'informations, consultez Scanner EC2 des instances Amazon avec Amazon Inspector.

Le scan Amazon ECR et le scan par fonction Lambda ne nécessitent pas l'agent SSM

L'analyse basée sur un agent utilise l'agent SSM pour collecter l'inventaire des logiciels. L'analyse sans agent utilise les instantanés Amazon EBS pour collecter l'inventaire des logiciels.

> **Note**
>
> Par défaut, l'agent SSM est déjà installé dans les EC2 instances Amazon basées sur Amazon Machine Images. Toutefois, il se peut que vous deviez activer l'agent SSM manuellement dans certains cas. Pour plus d'informations, consultez la section Utilisation de l'agent SSM dans le guide de l'AWS Systems Manager utilisateur.

Les coûts mensuels sont basés sur les charges de travail numérisées

Pour plus d'informations, consultez la Tarification d'Amazon Inspector.

# Tutoriel de démarrage : Activation d'Amazon Inspector

Cette rubrique explique comment activer Amazon Inspector pour un environnement de compte autonome (compte membre) et un environnement multi-comptes (compte administrateur délégué). Lorsque vous activez Amazon Inspector, celui-ci commence automatiquement à détecter les charges de travail et à les analyser pour détecter les vulnérabilités logicielles et les risques d'exposition involontaire au réseau.

Standalone account environment

La procédure suivante décrit comment activer Amazon Inspector dans la console pour un compte membre. Pour activer Amazon Inspector par programme, inspector2-. enablement-with-cli

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 pour un compte autonome, tous les types de scan sont activés par défaut. Pour plus d'informations sur les comptes membres, consultez Comprendre le compte d'administrateur délégué et les comptes de membre dans Amazon Inspector.

Multi-account environment

La procédure suivante décrit comment activer Amazon Inspector dans la console pour un compte d'administrateur délégué. Pour activer Amazon Inspector par programme pour plusieurs comptes, utilisez le script Amazon enablement-with-cliInspector2-shell.

> **Note**
>
> Vous devez utiliser le compte AWS Organizations de gestion pour effectuer cette procédure. Seul le compte AWS Organizations de gestion peut désigner un administrateur délégué. Des autorisations peuvent être nécessaires pour désigner un administrateur délégué. Pour de plus amples informations, veuillez consulter Autorisations requises pour désigner un administrateur délégué.

Lorsque vous activez Amazon Inspector pour la première fois, Amazon Inspector crée le rôle lié au service `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 désigner un administrateur délégué pour Amazon Inspector

1. Connectez-vous au compte de AWS Organizations gestion, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Choisissez Démarrer.
3. Sous Administrateur délégué, entrez l'identifiant à 12 chiffres de celui que Compte AWS vous souhaitez désigner comme administrateur délégué.
4. Choisissez Déléguer, puis sélectionnez à nouveau Déléguer.
5. (Facultatif) Si vous souhaitez activer Amazon Inspector pour le compte AWS Organizations de gestion, choisissez Activer Amazon Inspector sous Autorisations de service.

Lorsque vous désignez un administrateur délégué, tous les types de scan sont activés par défaut pour le compte. Pour plus d'informations sur le compte d'administrateur délégué, consultez

Comprendre le compte d'administrateur délégué et les comptes de membre dans Amazon Inspector.

# Types de scan automatisés dans Amazon Inspector

Amazon Inspector utilise un moteur d'analyse spécialement conçu pour surveiller vos ressources afin de détecter les vulnérabilités logicielles et toute exposition involontaire au réseau. Lorsqu'Amazon Inspector détecte une vulnérabilité logicielle ou une exposition involontaire au réseau, il crée une constatation. Lorsque vous activez Amazon Inspector pour la première fois, votre compte est automatiquement inscrit à tous les types de scan, notamment le scan Amazon Amazon, le EC2 scan Amazon ECR et le scan standard Lambda.

> **Note**
>
> Le scan de code Lambda est une couche optionnelle de numérisation des fonctions Lambda que vous pouvez activer à tout moment.

Rubriques



# Présentation des types de scan Amazon Inspector

Amazon Inspector propose différents types de scan qui se concentrent sur des types de ressources spécifiques de votre AWS environnement.

EC2 Numérisation Amazon

Lorsque vous activez le EC2 scan Amazon, Amazon Inspector analyse vos EC2 instances pour détecter les éléments suivants :

- Vulnérabilités et expositions courantes
- Vulnérabilités des packages du système d'exploitation et du langage de programmation

- Accessibilité du réseau
- 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, consultezNumérisation d' EC2 instances Amazon avec Amazon Inspector.

> **Note**
>
> Par défaut, lorsque vous activez le EC2 scan Amazon, vous activez automatiquement le mode de numérisation hybride. Pour plus d'informations, consultez la section Numérisation sans agent.

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 filtres de numérisation. Toutes les images envoyées au cours des 14 derniers jours ou extraites au cours des 14 derniers jours sont initialement numérisées. Amazon Inspector continue de surveiller les images pendant 14 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 Elastic Container Registry 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 () CVEs 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 la section Analyse du code Lambda par Amazon Inspector.

## Activation d'un type de scan

Vous pouvez activer les types de scan Amazon Inspector à tout moment. Lorsque vous activez un type de scan, Amazon Inspector commence immédiatement à scanner les ressources éligibles pour ce type de scan. Voici une brève description de chaque type de scan :

### EC2 Numérisation Amazon

Ce type de scan extrait les métadonnées de votre EC2 instance avant de les comparer aux règles collectées à partir des avis de sécurité. Lorsque vous activez ce type de scan, Amazon Inspector analyse toutes les instances éligibles de votre compte pour détecter les vulnérabilités des packages et les problèmes d'accessibilité au réseau.

### Numérisation Amazon ECR

Ce type de scan scanne les images des conteneurs dans Amazon ECR. Lorsque vous activez ce type de numérisation, vous modifiez le paramètre de configuration de numérisation de votre registre privé en passant d'une analyse de base à une analyse améliorée.

### Numérisation standard Lambda

Le scan Lambda standard est le type de scan Lambda par défaut. Lorsque vous activez le scan standard Lambda, toutes les fonctions Lambda de votre compte sont analysées pour détecter les vulnérabilités de code, à condition qu'elles aient été invoquées ou mises à jour au cours des 90 derniers jours.

### Numérisation de code Lambda

Le scan de code Lambda scanne le code d'application personnalisé dans une fonction Lambda. Lorsque vous activez le scan de code Lambda, toutes les fonctions Lambda de votre compte sont analysées pour détecter les vulnérabilités du code, à condition qu'elles aient été invoquées ou mises à jour au cours des 90 derniers jours.

> **Note**
>
> Vous pouvez activer le scan standard Lambda ou le scan standard Lambda avec le scan de code Lambda.

Pour une présentation plus complète des types de scan disponibles, consultez Analyse automatisée des ressources avec Amazon Inspector. Cette section explique comment activer un type de scan dans Amazon Inspector.

## 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 le compte pour IDs lequel vous activez les scans, le jeton d'idempotencie, et un ou plusieurs des`EC2`, `ECR`LAMBDA, ou `LAMBDA_CODE` `resourceTypes` pour activer les scans de ce type.

# Numérisation d' EC2 instances Amazon avec Amazon Inspector

Amazon Inspector Le EC2 scan par Amazon extrait les métadonnées de votre EC2 instance avant de les comparer aux règles collectées à partir des avis de sécurité. Amazon Inspector analyse les instances pour détecter les vulnérabilités des packages et les problèmes d'accessibilité au réseau afin de produire des résultats. Amazon Inspector effectue des analyses d'accessibilité au réseau toutes les 24 heures et des analyses de vulnérabilité des packages à une cadence variable qui dépend de la méthode d'analyse associée à l'instance. EC2

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 deux méthodes d'analyse déterminent comment et quand Amazon Inspector collecte l'inventaire logiciel d'une EC2 instance pour les analyses de vulnérabilité des packages. L'analyse basée sur un agent collecte l'inventaire des logiciels à l'aide de l'agent SSM, tandis que l'analyse sans agent collecte l'inventaire des logiciels à l'aide de snapshots Amazon EBS.

Amazon Inspector utilise les méthodes de scan que vous activez pour votre compte. Lorsque vous activez Amazon Inspector pour la première fois, votre compte est automatiquement inscrit au scan hybride, qui utilise les deux méthodes de scan. Toutefois, vous pouvez modifier ce paramètre à tout moment. Pour plus d'informations sur l'activation d'un type de scan, voir Activation d'un type de scan. Cette section fournit des informations sur le EC2 scan Amazon.

> **Note**
>
> Amazon EC2 Scanning n'analyse pas les répertoires du système de fichiers liés à l'environnement virtuel, même s'ils sont approvisionnés par le biais d'une inspection approfondie. Par exemple, le chemin n'`/var/lib/docker/`est pas scanné car il est couramment utilisé pour les durées d'exécution des conteneurs.

# 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 Amazon basées sur Linux 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.

> **Note**
>
> Pour le scan basé sur un agent, l' EC2 instance Amazon doit être gérée par SSM dans le même environnement. Compte AWS

## Instances éligibles

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

- L'instance dispose d'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 : Amazon EC2 Scanning”
- L'instance n'est pas exclue des scans par les balises d' EC2 exclusion Amazon Inspector.

- 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 des EC2 instances dans les situations suivantes :

- Lorsque vous lancez une nouvelle EC2 instance.
- Lorsque vous installez un nouveau logiciel sur une EC2 instance 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 EC2 instance (Linux et Mac).

Amazon Inspector met à jour le champ Dernière analyse pour une EC2 instance 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 EC2 instance 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 EC2 instance Amazon 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 EC2 instances créées à partir de certaines Amazon Machine Images (AMIs). 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 EC2 instance Amazon 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 la EC2 numérisation par Amazon Inspector.

> **Note**
>
> Vous pouvez également automatiser la gestion SSM de toutes vos EC2 instances, 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 a besoin d'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` si elle n'existe pas déjà. 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.

### Ressources SSM créées pour la numérisation

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

**Note**

Si l'une de ces ressources SSM est supprimée alors qu'Amazon Inspector est activé pour le EC2 scan Amazon de 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 EC2 instances Amazon. 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 EC2 instances Amazon 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 plug-in 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 le EC2 scan Amazon ou l'inspection approfondie d'Amazon Inspector, la ressource SSM n'`InvokeInspectorLinuxSsmPlugin-do-not-delete`est plus invoquée.

# Numérisation sans agent

Amazon Inspector utilise la méthode d'analyse sans agent sur les instances éligibles lorsque votre compte est en mode de numérisation hybride. Le mode de numérisation hybride inclut des scans avec ou sans agent et est automatiquement activé lorsque vous activez le scan Amazon. EC2

Pour les scans sans agent, Amazon Inspector utilise des instantanés EBS pour collecter un inventaire logiciel à partir de vos instances. L'analyse sans agent analyse les instances pour détecter les vulnérabilités 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 Amazon basées sur Linux 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 d'EBS direct APIs 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 dispose d'un système d'exploitation compatible. Pour plus d'informations, consultez la colonne >Support du scan basé sur un agent de. the section called "Systèmes d'exploitation pris en charge : Amazon EC2 Scanning"
- Le statut de l'instance est `Unmanaged EC2 instance`Stale `inventory`, ou`No inventory`.
- L'instance est soutenue par Amazon EBS et possède l'un des formats de système de fichiers suivants :
  - `ext3`
  - `ext4`
  - `xfs`
- L'instance n'est pas exclue des scans via les balises EC2 d'exclusion Amazon.
- Le nombre de volumes attachés à l'instance est inférieur à 8 et leur taille combinée est inférieure ou égale à 1 200 Go.

### 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 EC2 instance Amazon chaque fois qu'il analyse des instantanés extraits d'une instance après un scan sans agent.

Vous pouvez vérifier la date à laquelle une EC2 instance 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 EC2 scan détermine les méthodes de scan qu'Amazon Inspector utilisera pour effectuer des EC2 scans sur votre compte. Vous pouvez consulter le mode de numérisation de votre compte EC2 sur la page des paramètres de numérisation 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 EC2 instances 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 EC2 numérisation.
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 exclure Linux des Windows instances des scans Amazon Inspector en les étiquetant avec la `InspectorEc2Exclusion` clé. L'inclusion d'une valeur de balise est facultative. Pour plus d'informations sur l'ajout de balises, consultez la section Marquer vos EC2 ressources Amazon.

Lorsque vous balisez une instance pour qu'elle soit exclue des scans Amazon Inspector, Amazon Inspector marque l'instance comme exclue et ne crée pas de résultats pour elle. Cependant, le plug-in Amazon Inspector SSM continuera d'être invoqué. Pour empêcher le plugin d'être invoqué, vous devez autoriser l'accès aux balises dans les métadonnées de l'instance.

> **Note**
>
> Les instances exclues ne vous sont pas facturées.

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 EC2 instances 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 Amazon basées sur Linux 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, consultezValeurs de statut des EC2 instances Amazon.

## Inspection approfondie d'Amazon Inspector pour les instances Amazon basées sur Linux EC2

Amazon Inspector étend la couverture EC2 d'Amazon en y incluant 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. Cependant, vous pouvez configurer des chemins personnalisés en plus des chemins analysés par défaut par Amazon Inspector.

> **Note**
>
> Vous pouvez utiliser une inspection approfondie avec le paramètre de configuration de gestion d'hôte par défaut. Toutefois, vous devez créer ou utiliser un rôle configuré avec les `ssm:GetParameter` autorisations `ssm:PutInventory` et.

Pour effectuer des analyses d'inspection approfondies pour vos instances Amazon basées sur Linux, EC2 Amazon Inspector utilise les données collectées avec le plugin Amazon Inspector SSM. Pour gérer le plug-in Amazon Inspector SSM et effectuer une inspection approfondie pour Linux, Amazon Inspector crée automatiquement l'association SSM `InvokeInspectorLinuxSsmPlugin-do-not-delete` dans votre compte. Amazon Inspector collecte l'inventaire des applications mis à jour à partir de vos instances EC2 Amazon basées sur Linux toutes les 6 heures.

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

Cette section explique comment gérer l'inspection approfondie d'Amazon Inspector pour les EC2 instances Amazon, notamment comment définir des chemins personnalisés à scanner par Amazon Inspector.

Rubriques



## Accès ou désactivation de l'inspection approfondie

> **Note**
>
> Pour les comptes qui activent Amazon Inspector après le 17 avril 2023, l'inspection approfondie est automatiquement activée dans le cadre du EC2 scan Amazon.

Pour gérer une inspection approfondie

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home
2. Dans le volet de navigation, choisissez Paramètres généraux, puis sélectionnez Paramètres de EC2 numérisation Amazon.

3. Dans le cadre de l'inspection approfondie de l' EC2 instance Amazon, vous pouvez définir des chemins personnalisés pour votre organisation ou pour votre propre compte.

Vous pouvez vérifier le statut d'activation par programmation pour un seul compte grâce à l'API GetEc2. DeepInspectionConfiguration Vous pouvez vérifier l'état d'activation de plusieurs comptes par programmation à l'aide de 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 activer une inspection approfondie pour vous-même et pour vos comptes membres.

Vous pouvez désactiver l'inspection approfondie via l'UpdateEc2DeepInspectionConfigurationAPI. Les comptes des 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.

## Chemins personnalisés pour l'inspection approfondie d'Amazon Inspector

Vous pouvez définir des chemins personnalisés à scanner par Amazon Inspector lors d'une inspection approfondie de vos EC2 instances Amazon Linux. Lorsque vous définissez un chemin personnalisé, Amazon Inspector analyse les packages de ce répertoire et tous les sous-répertoires qu'il contient.

Tous les comptes peuvent définir jusqu'à 5 chemins personnalisés. L'administrateur délégué d'une organisation peut définir 10 chemins personnalisés.

Amazon Inspector analyse tous les chemins personnalisés en plus des chemins par défaut suivants, qu'Amazon Inspector analyse 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 du système de fichiers réseau ou les montages du système de fichiers Amazon S3.

Formatage de chemins personnalisés

Un chemin personnalisé ne peut pas comporter plus de 256 caractères. Voici un exemple de ce à quoi peut ressembler un chemin personnalisé :

Exemple de chemin

```
/home/usr1/project01
```

> **Note**
>
> La limite de packages par instance est de 5 000. La durée maximale de collecte de l'inventaire des colis est de 15 minutes. Amazon Inspector vous recommande de choisir des chemins personnalisés pour éviter ces limites.

Définition d'un chemin personnalisé dans la console Amazon Inspector et avec l'API Amazon Inspector

Les procédures suivantes décrivent comment définir un chemin personnalisé pour l'inspection approfondie d'Amazon Inspector dans la console Amazon Inspector et avec l'API Amazon Inspector. Une fois que vous avez défini un chemin personnalisé, Amazon Inspector inclut ce chemin dans l'inspection approfondie suivante.

Console

1. Connectez-vous en AWS Management Console tant qu'administrateur délégué et ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home
2. Utilisez le Région AWS sélecteur pour choisir la région dans laquelle vous souhaitez activer le scan standard Lambda.
3. Dans le volet de navigation, choisissez Paramètres généraux, puis sélectionnez Paramètres de EC2 numérisation.

4. Sous Chemins personnalisés pour votre propre compte, choisissez Modifier.
5. Dans les zones de texte des chemins, entrez vos chemins personnalisés.
6. Choisissez Enregistrer.

API

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

## Programmes personnalisés pour l'inspection approfondie d'Amazon Inspector

Par défaut, Amazon Inspector collecte un inventaire des applications auprès des EC2 instances Amazon toutes les 6 heures. Toutefois, vous pouvez exécuter les commandes suivantes pour contrôler la fréquence à laquelle Amazon Inspector effectue ces opérations.

Exemple de commande 1 : Répertorier les associations pour afficher l'ID d'association et l'intervalle actuel

La commande suivante indique l'identifiant de l'association`InvokeInspectorLinuxSsmPlugin-do-not-delete`.

```
aws ssm list-associations \
--association-filter-list "key=AssociationName,value=InvokeInspectorLinuxSsmPlugin-do-not-delete" \
--region your-Region
```

Exemple de commande 2 : Mettre à jour l'association pour inclure un nouvel intervalle

La commande suivante utilise l'identifiant de l'association`InvokeInspectorLinuxSsmPlugin-do-not-delete`. Vous pouvez définir le taux pour une période comprise `schedule-expression` entre 6 heures et un nouvel intervalle, par exemple 12 heures.

```
aws ssm update-association \
--association-id "your-association-ID" \
--association-name "InvokeInspectorLinuxSsmPlugin-do-not-delete" \
--schedule-expression "rate(6 hours)" \
--region your-Region
```

> **Note**
>
> Selon votre cas d'utilisation, si vous définissez le taux `schedule-expression` entre 6 heures et un intervalle de 30 minutes, vous pouvez dépasser la limite d'inventaire SSM quotidienne. Cela retarde les résultats et vous risquez de rencontrer des EC2 instances Amazon présentant des statuts d'erreur partiels.

### Langages de programmation pris en charge

Pour les instances Linux, l'inspection approfondie d'Amazon Inspector peut produire des résultats pour les packages de langage de programmation d'applications et les packages de système d'exploitation.

Pour les instances Mac et Windows, l'inspection approfondie d'Amazon Inspector peut produire des résultats uniquement pour les packages de systèmes d'exploitation.

Pour plus d'informations sur les langages de programmation pris en charge, consultez Langages de programmation pris en charge : Amazon EC2 Deep Inspection.

## Numérisation Windows EC2 d'instances avec Amazon Inspector

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, consultez Systèmes d'exploitation et langages de programmation pris en charge par Amazon Inspector. Amazon Inspector exécute Windows des scans à intervalles réguliers. Windowsles instances sont scannées lors de leur découverte, puis toutes les 6 heures. Vous pouvez toutefois ajuster l'intervalle de numérisation par défaut après le premier scan.

Lorsque Amazon EC2 Scanning est activé, Amazon Inspector crée les associations SSM suivantes pour vos Windows ressources : `InspectorDistributor-do-not-deleteInspectorInventoryCollection-do-not-delete`, et`InvokeInspectorSsmPlugin-do-not-delete`. Pour installer le plug-in Amazon Inspector SSM sur vos Windows instances, l'association `InspectorDistributor-do-not-delete` SSM utilise le document SSM et le `AWS-ConfigureAWSPackageAmazonInspector2-InspectorSsmPlugin` package SSM Distributor. Pour plus d'informations, consultez le plug-in Amazon Inspector SSM pour Windows. Pour collecter les données d'instance et générer les résultats d'Amazon Inspector, l'association `InvokeInspectorSsmPlugin-do-not-delete` SSM exécute

le plug-in Amazon Inspector SSM toutes les 6 heures. Vous pouvez toutefois personnaliser ce paramètre à l'aide d'une expression cron ou rate.

> **Note**
>
> Amazon Inspector place les fichiers de définition OVAL (Open Vulnerability and Assessment Language) mis à jour dans le compartiment S3`inspector2-oval-prod-`*`your-AWS-Region`*. Le compartiment Amazon S3 contient les définitions OVAL utilisées dans les scans. Ces définitions OVAL ne doivent pas être modifiées. Dans le cas contraire, Amazon Inspector ne recherchera pas de nouveaux CVEs produits lors de leur sortie.

## 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, consultezValeurs de statut des EC2 instances Amazon.
- 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`*.

## Définition de plannings personnalisés pour les scans Windows par exemple

Vous pouvez personnaliser le délai entre les scans de votre EC2 instance Windows Amazon 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 Elastic Container Registry avec Amazon Inspector

Amazon Inspector analyse les images des conteneurs stockées dans Amazon Elastic Container Registry pour détecter les vulnérabilités logicielles afin de générer des informations sur les vulnérabilités des packages. Lorsque vous activez le scan Amazon ECR, vous définissez Amazon Inspector comme service de numérisation préféré pour votre registre privé.

> **Note**
>
> Amazon ECR utilise une politique de registre pour accorder des autorisations à un AWS mandant. Ce responsable dispose des autorisations requises pour appeler Amazon Inspector à APIs des fins de numérisation. Lorsque vous définissez le champ d'application de votre politique de registre, vous ne devez ni ajouter l'`ecr:*`action ni `PutRegistryScanningConfiguration` y ajouter`deny`. Cela entraîne des erreurs au niveau du registre lors de l'activation et de la désactivation de l'analyse pour Amazon ECR.

Avec l'analyse de base, vous pouvez configurer vos référentiels pour qu'ils effectuent une analyse push ou des analyses manuelles. Grâce à l'analyse améliorée, vous recherchez les vulnérabilités du système d'exploitation et des packages de langage de programmation au niveau du registre. Pour une side-by-side comparaison des différences entre la numérisation de base et la numérisation améliorée, consultez la FAQ Amazon Inspector.

> **Note**
>
> La numérisation de base est fournie et facturée via Amazon ECR. Pour plus d'informations, consultez la tarification d'Amazon Elastic Container Registry. La numérisation améliorée est

fournie et facturée via Amazon Inspector. Pour plus d'informations, consultez la Tarification d'Amazon Inspector.

Pour plus d'informations sur la façon d'activer le scan Amazon ECR, consultezActivation d'un type de scan. Pour plus d'informations sur la façon de consulter vos résultats, consultezGestion des résultats dans Amazon Inspector. Pour savoir comment afficher vos résultats au niveau de l'image, consultez la section Numérisation d'images dans le guide de l'utilisateur d'Amazon Elastic Container Registry. Vous pouvez également gérer les résultats Services AWS non disponibles pour la numérisation de base, comme AWS Security Hub Amazon EventBridge.

Cette section fournit des informations sur le scan Amazon ECR et décrit comment configurer le scan amélioré pour les référentiels Amazon ECR.

## 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 plus d'informations, consultez Configuration de la durée de nouvelle analyse d'Amazon 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.

## Associer des images de conteneurs à des conteneurs en cours d'exécution

Amazon Inspector fournit une gestion complète de la sécurité des conteneurs en mappant les images des conteneurs aux conteneurs en cours d'exécution sur Amazon Elastic Container Service (Amazon ECS) et Amazon Elastic Kubernetes Service (Amazon EKS). Ces mappages fournissent des informations sur les vulnérabilités des images présentes sur des conteneurs en cours d'exécution.

Grâce à cette fonctionnalité, vous pouvez hiérarchiser les efforts de correction en fonction des risques opérationnels et maintenir une couverture de sécurité dans l'ensemble de l'écosystème de conteneurs. Vous pouvez surveiller les images de conteneur actuellement utilisées et la date à laquelle les images de conteneur ont été utilisées pour la dernière fois sur un cluster Amazon ECS ou Amazon EKS au cours des dernières 24 heures. Ces informations seront disponibles dans vos résultats via la console Amazon Inspector sur l'écran de détails des résultats relatifs aux images de votre conteneur et via l'API Amazon Inspector via les `ecrImageLastInUseAt` filtres `ecrImageInUseCount` et.

> **Note**
>
> Ces données sont automatiquement envoyées aux résultats d'Amazon ECR lorsque vous activez le scan Amazon ECR et que vous configurez votre référentiel pour un scan continu. L'analyse continue doit être configurée au niveau du référentiel Amazon ECR. Pour plus d'informations, consultez la section Analyse améliorée dans le guide de l'utilisateur d'Amazon Elastic Container Registry.

Vous pouvez également numériser à nouveau des images de conteneurs à partir de clusters en fonction de leur last-in-use date.

# 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 : numérisation Amazon ECR avec Amazon Inspector.

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

Manifeste d'images

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

Configuration de l'image

- `"application/vnd.docker.container.image.v1+json"`
- `"application/vnd.oci.image.config.v1+json"`

Couches d'images

- `"application/vnd.docker.image.rootfs.diff.tar"`
- `"application/vnd.docker.image.rootfs.diff.tar.gzip"`
- `"application/vnd.docker.image.rootfs.foreign.diff.tar.gzip"`
- `"application/vnd.oci.image.layer.v1.tar"`
- `"application/vnd.oci.image.layer.v1.tar+gzip"`
- `"application/vnd.oci.image.layer.v1.tar+zstd"`
- `"application/vnd.oci.image.layer.nondistributable.v1.tar"`
- `"application/vnd.oci.image.layer.nondistributable.v1.tar+gzip"`

> **Note**
>
> Amazon Inspector ne prend pas en charge le type de `"application/vnd.docker.distribution.manifest.list.v2+json"` support pour l'analyse des référentiels Amazon ECR.

# Configuration de la durée de nouvelle analyse d'Amazon ECR

Le paramètre de durée de nouvelle analyse Amazon ECR détermine la durée pendant laquelle Amazon Inspector surveille en permanence les images des conteneurs dans les référentiels. Vous configurez la durée de nouvelle numérisation pour la date de dernière utilisation, la date de dernière extraction et la date de publication de l'image. Il est recommandé de configurer la durée de la nouvelle analyse en fonction de votre environnement.

Si vous créez souvent des images, choisissez une durée de numérisation plus courte. Pour les images utilisées sur de longues périodes, choisissez une durée de numérisation plus longue. La durée d'analyse par défaut pour les nouveaux comptes, y compris les nouveaux comptes ajoutés à une organisation, est de 30 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. Il en va de même pour les images dont la last-in-use date est configurée. Si une image n'a pas été envoyée ou extraite dans les délais d'envoi et d'extraction configurés, Amazon Inspector arrête de la surveiller. Il en va de même pour les images non utilisées à la last-in-use date configurée. 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`. Amazon Inspector planifie ensuite la fermeture de toutes les images trouvées.

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.

> **Note**
>
> 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. Si le compte d'administrateur délégué n'active pas le scan Amazon ECR, il ne peut pas afficher les clusters pour une image d'API.

### Durée de la nouvelle numérisation de l'image

La durée de numérisation des images détermine la durée pendant laquelle Amazon Inspector surveillera les images. La durée de numérisation de l'image comprend deux modes : date de

dernière utilisation ou date de dernière extraction. Choisissez Date de dernière utilisation si vous souhaitez utiliser la date de dernière utilisation de votre activité de cluster Amazon ECS/Amazon EKS. Choisissez Dernière date d'extraction si vous souhaitez utiliser la dernière date d'extraction de vos images Amazon ECR pour numériser à nouveau des images. Les options suivantes sont disponibles sous forme de durées de nouvelle numérisation :

- 14 jours (par défaut)

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 surveillera en permanence les images après leur transfert vers des référentiels. Les options suivantes sont disponibles sous forme de durées de nouvelle numérisation :

- 14 jours (par défaut)

Pour configurer la durée de nouvelle analyse d'Amazon ECR

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Sélectionnez l' Région AWS endroit où vous souhaitez configurer la durée de nouvelle analyse d'Amazon ECR.
3. Dans le volet de navigation, choisissez Paramètres généraux, puis sélectionnez Paramètres de numérisation ECR.
4. Sous Durée de nouvelle numérisation ECR, choisissez le mode de numérisation de l'image, puis choisissez la durée correspondante.
5. Sous Date de diffusion de l'image, choisissez la date de diffusion de l'image.
6. Choisissez Enregistrer.

# AWS Lambda Fonctions de numérisation avec Amazon Inspector

Le support d'Amazon Inspector pour AWS Lambda les fonctions et les couches fournit des évaluations automatisées continues des vulnérabilités de sécurité. Amazon Inspector propose deux types de numérisation par fonction Lambda :

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 des couches pour détecter les vulnérabilités des packages.

Numérisation du code Lambda d'Amazon Inspector

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

Lorsque vous activez le scan des fonctions Lambda, Amazon Inspector crée les canaux AWS CloudTrail liés aux services suivants dans votre compte : et. `cloudtrail:CreateServiceLinkedChannel` `cloudtrail:DeleteServiceLinkedChannel` Amazon Inspector gère ces canaux et les utilise pour surveiller vos CloudTrail événements à des fins d'analyse. Ces canaux vous permettent de suivre CloudTrail les événements sur votre compte comme si vous y étiez connecté CloudTrail. Nous vous recommandons de créer votre propre trail in CloudTrail pour gérer les événements de votre compte.

Pour plus d'informations sur la façon d'activer le scan par fonction Lambda, voir Activation d'un type de scan. Cette section fournit des informations sur le scan des fonctions Lambda.

## 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 ajouter des balises aux fonctions Lambda afin de les exclure des scans standard Lambda d'Amazon Inspector. Le fait d'exclure des fonctions des scans peut éviter des alertes inexploitables. Lorsque vous balisez une fonction pour l'exclure, la balise doit comporter la paire clé-valeur suivante.

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

Cette rubrique décrit comment baliser une fonction pour l'exclure des scans. Pour plus d'informations sur l'ajout de balises dans Lambda, consultez la section Utilisation de balises dans les fonctions Lambda.

Pour exclure une fonction des scans

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Lambda à l'adresse. https://console.aws.amazon.com/lambda/
2. Dans le volet de navigation, sélectionnez Functions.
3. Choisissez le nom de la fonction que vous souhaitez exclure des scans standard Amazon Inspector Lambda.
4. Sélectionnez Configuration, puis Tags (Balises).
5. Choisissez Gérer les balises, puis Ajouter une nouvelle balise.
   a. Pour Key (Clé), saisissez `InspectorExclusion`.
   b. Pour le champ Value (Valeur), saisissez `LambdaStandardScanning`.
6. Choisissez Save (Enregistrer).

## Numérisation du code Lambda d'Amazon Inspector

> **Important**
>
> Cette fonctionnalité capture des extraits de fonctions Lambda pour mettre en évidence les vulnérabilités détectées. Ces extraits peuvent afficher des informations d'identification codées en dur et d'autres informations sensibles.

Grâce à cette fonctionnalité, Amazon Inspector analyse le code de l'application dans une fonction Lambda pour détecter les vulnérabilités du code en se basant sur les meilleures pratiques de AWS sécurité afin de détecter les fuites de données, les défauts d'injection, les défauts de chiffrement et les faiblesses du chiffrement. Amazon Inspector utilise le raisonnement automatique et l'apprentissage automatique pour évaluer le code d'application de votre fonction Lambda. Il utilise également des détecteurs internes développés en collaboration avec Amazon CodeGuru pour identifier les violations des politiques et les vulnérabilités. Pour plus d'informations, consultez la bibliothèque CodeGuru de détecteurs.

Amazon Inspector génère une vulnérabilité de code lorsqu'il détecte une vulnérabilité dans le code de votre application de fonction Lambda. Ce type de recherche inclut un extrait de code indiquant le problème et indiquant où vous pouvez le trouver dans votre code. Il suggère également comment remédier au problème. La suggestion inclut des blocs de plug-and-play code que vous pouvez utiliser

pour remplacer des lignes de code vulnérables. Ces corrections de code sont fournies en plus des conseils généraux de correction du code pour ce type de recherche.

Les suggestions de correction du code s'appuient sur des services de raisonnement automatique et d'intelligence artificielle générative. Certaines suggestions de correction du code peuvent 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 les modifier pour vous assurer que votre code fonctionne comme prévu. Pour plus d'informations, consultez la politique en matière d'IA responsable.

Le scan de code Lambda peut être activé seul ou conjointement avec le scan standard Lambda. Pour plus d'informations, consultez la section Activation d'un type de scan. Pour plus d'informations sur les Régions AWS appareils compatibles avec cette fonctionnalité, consultezDisponibilité des fonctionnalités propres à la région.

## Chiffrer votre code lors des découvertes de vulnérabilités

CodeGuru stocke les extraits de code détectés comme étant liés à la détection d'une vulnérabilité de code à l'aide de l'analyse de code Lambda. Par défaut, CodeGuru contrôle la clé AWS détenue utilisée pour chiffrer votre code. Cependant, 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.

## Exclusion de fonctions du scan de code Lambda

Vous pouvez ajouter des balises aux fonctions Lambda afin de les exclure des scans de code Lambda d'Amazon Inspector. Le fait d'exclure des fonctions des scans peut éviter des alertes inexploitables. Lorsque vous balisez une fonction pour l'exclure, la balise doit comporter la paire clé-valeur suivante.

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

Cette rubrique explique comment étiqueter une fonction pour l'exclure des analyses de code. Pour plus d'informations sur l'ajout de balises dans Lambda, consultez la section Utilisation de balises dans les fonctions Lambda.

Pour exclure une fonction des analyses de code

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Lambda à l'adresse. https://console.aws.amazon.com/lambda/
2. Dans le volet de navigation, sélectionnez Functions.
3. Choisissez le nom de la fonction que vous souhaitez exclure des scans de code Lambda d'Amazon Inspector.
4. Sélectionnez Configuration, puis Tags (Balises).
5. Choisissez Gérer les balises, puis Ajouter une nouvelle balise.
   a. Pour Key (Clé), saisissez `InspectorCodeExclusion`.
   b. Pour le champ Value (Valeur), saisissez `LambdaCodeScanning`.
6. Choisissez Save (Enregistrer).

# Désactivation d'un type de scan dans Amazon Inspector

Cette section décrit comment désactiver un type de scan. Lorsque vous désactivez un type de scan, vous perdez l'accès aux résultats produits par ce type de scan. Si vous réactivez le type de scan, Amazon Inspector analyse toutes les ressources éligibles pour générer de nouvelles découvertes.

> **Tip**
>
> Si vous souhaitez conserver une trace de vos résultats, vous pouvez les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) sous forme de rapport de résultats. Pour de plus amples informations, veuillez consulter Exportation des rapports de résultats d'Amazon Inspector.

Lorsque vous désactivez un type de scan, vous pouvez rencontrer les modifications suivantes dans le AWS compte sur lequel vous avez désactivé le type de scan :

EC2 Numérisation Amazon

Lorsque vous désactivez le EC2 scan Amazon d'Amazon Inspector pour un compte, les associations SSM suivantes 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 Windows EC2 Instance de numérisation.

Numérisation Amazon ECR

Lorsque vous désactivez le scan Amazon ECR pour un compte, le compte de type de scan Amazon ECR passe du scan amélioré avec Amazon Inspector au scan de base avec Amazon ECR.

Numérisation standard Lambda

Lorsque vous désactivez le scan standard Lambda pour un compte, vous désactivez le scan du code Lambda si le type de scan était activé. Vous supprimez également le canal CloudTrail lié au service créé par Amazon Inspector lorsque vous avez activé le scan standard Lambda.

## 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 le compte pour lequel IDs vous désactivez les scans, et pour `resourceTypes` fournir un ou plusieurs scans `EC2` `ECR`LAMBDA, ou `LAMBDA_CODE` pour désactiver les scans.

# Le Center for Internet Security (CIS) analyse les systèmes d'exploitation des EC2 instances Amazon

Les scans CIS (scans CIS) d'Amazon Inspector évaluent les systèmes d'exploitation de vos EC2 instances Amazon pour s'assurer que vous les avez configurés conformément aux recommandations des meilleures pratiques établies par le Center for Internet Security. CIS Security Benchmarks fournit des bases de configuration conformes aux normes du secteur et les meilleures pratiques pour configurer un système en toute sécurité. Vous pouvez effectuer ou planifier des scans CIS après avoir activé le EC2 scan Amazon Inspector pour un compte. Pour plus d'informations sur la façon d'activer le EC2 scan Amazon, consultez Activation d'un type de scan.

> **Note**
>
> Les normes CIS sont destinées aux systèmes d'exploitation x86_64. Certaines vérifications peuvent ne pas être évaluées ou renvoyer des instructions de correction non valides sur les ressources basées sur ARM.

Amazon Inspector effectue des analyses CIS sur les EC2 instances Amazon cibles en fonction des balises d'instance et du calendrier d'analyse que vous avez défini. Amazon Inspector effectue une série de vérifications d'instance sur chaque instance ciblée. Chaque contrôle permet d'évaluer si la configuration de votre système répond aux recommandations spécifiques du CIS Benchmark. Chaque contrôle possède un identifiant et un titre de contrôle CIS, qui correspondent à une recommandation CIS Benchmark pour cette plate-forme. Lorsqu'une analyse CIS est terminée, vous pouvez consulter les résultats pour voir quelles vérifications d'instance ont été réussies, ignorées ou ont échoué pour ce système.

> **Note**
>
> Pour effectuer ou planifier des scans CIS, vous devez disposer d'une connexion Internet sécurisée. Toutefois, si vous souhaitez exécuter des scans CIS sur des instances privées, vous devez utiliser un point de terminaison VPC.

Rubriques

- Exigences relatives aux EC2 instances Amazon pour les scans Amazon Inspector CIS

- Exécution de scans CIS
- Considérations relatives à la gestion des scans Amazon Inspector CIS avec AWS Organizations
- Compartiments Amazon S3 appartenant à Amazon Inspector et utilisés pour les scans CIS par Amazon Inspector
- Création d'une configuration de scan CIS
- Affichage des résultats du scan CIS
- Modification d'une configuration de scan CIS
- Téléchargement des résultats d'un scan CIS

# Exigences relatives aux EC2 instances Amazon pour les scans Amazon Inspector CIS

Pour exécuter un scan CIS sur votre EC2 EC2 instance Amazon, celle-ci doit répondre 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 plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge par Amazon Inspector.
- L'instance est une instance Amazon EC2 Systems Manager. Pour plus d'informations, consultez la section Utilisation de l'agent SSM dans le guide de l'AWS Systems Manager utilisateur.
- Le plug-in Amazon Inspector SSM est installé sur l'instance. Amazon Inspector installe automatiquement ce plugin sur les instances gérées.
- L'instance possède un profil d'instance qui autorise SSM à gérer l'instance et Amazon Inspector à exécuter des scans CIS pour cette instance. Pour accorder ces autorisations, associez les ManagedCisPolicy politiques Amazon SSMManaged InstanceCore et AmazonInspector2 à un rôle IAM. Attachez ensuite le rôle IAM 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 les rôles IAM dans le guide de EC2 l'utilisateur Amazon.

> **Note**
>
> Vous n'êtes pas obligé d'activer l'inspection approfondie d'Amazon Inspector avant d'exécuter un scan CIS sur votre EC2 instance Amazon. Si vous désactivez l'inspection approfondie d'Amazon Inspector, Amazon Inspector installe automatiquement l'agent SSM, mais celui-

ci ne sera plus invoqué pour exécuter une inspection approfondie. Cependant, de ce fait, l'`InspectorLinuxDistributor-do-not-delete`association est présente dans votre compte.

## Exigences relatives aux terminaux Amazon Virtual Private Cloud pour exécuter des scans CIS sur des EC2 instances Amazon privées

Vous pouvez exécuter des scans CIS sur EC2 des instances Amazon via un réseau Amazon. Toutefois, si vous souhaitez exécuter des scans CIS sur des EC2 instances Amazon privées, vous devez créer des points de terminaison Amazon VPC. Les points de terminaison suivants sont requis lorsque vous créez des points de terminaison Amazon VPC pour Systems Manager :

- `com.amazonaws.`*`region`*`.ec2messages`
- `com.amazonaws.`*`region`*`.inspector2`
- `com.amazonaws.`*`region`*`.s3`
- `com.amazonaws.`*`region`*`.ssm`
- `com.amazonaws.`*`region`*`.ssmmessages`

Pour plus d'informations, consultez la section Création de points de terminaison Amazon VPC pour Systems Manager dans le guide de l'AWS Systems Manager utilisateur.

> **Note**
>
> Actuellement, certains Régions AWS ne prennent pas en charge le `amazonaws.com.`*`region`*`.inspector2` point de terminaison.

# 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.

# Considérations relatives à la gestion des scans Amazon Inspector CIS avec AWS Organizations

Lorsque vous exécutez des scans CIS dans une organisation, les administrateurs délégués et les comptes membres d'Amazon Inspector interagissent différemment avec les configurations de scan CIS et les résultats des scans.

Comment les administrateurs délégués d'Amazon Inspector peuvent interagir avec les configurations de scan CIS et les résultats des scans

Lorsque l'administrateur délégué crée une configuration de numérisation, que ce soit pour tous les comptes ou pour un compte de membre spécifique, l'organisation est propriétaire de la configuration. Les configurations de scan détenues par une organisation possèdent un ARN spécifiant l'ID de l'organisation en tant que propriétaire :

`arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId`*

L'administrateur délégué peut gérer les configurations de scan détenues par une organisation, même si elles ont été créées par un autre compte.

L'administrateur délégué peut consulter les résultats du scan pour n'importe quel compte de son organisation.

Si l'administrateur délégué crée une configuration de scan et indique `SELF` qu'il s'agit du compte cible, il est propriétaire de la configuration de scan, même s'il quitte l'organisation. Toutefois, l'administrateur délégué ne peut pas modifier la cible d'une configuration de scan `SELF` en la désignant comme cible.

> **Note**
>
> L'administrateur délégué ne peut pas ajouter de balises aux configurations de scan CIS détenues par l'organisation.

Comment les comptes membres d'Amazon Inspector peuvent interagir avec les configurations de scan CIS et les résultats des scans

Lorsqu'un compte membre crée une configuration de scan CIS, il en est propriétaire. Toutefois, l'administrateur délégué peut consulter la configuration. Si un compte membre quitte l'organisation, l'administrateur délégué ne pourra pas consulter la configuration.

> **Note**
>
> L'administrateur délégué ne peut pas modifier une configuration de scan créée par le compte membre.

Les comptes membres, les administrateurs délégués SELF ayant pour cible et les comptes autonomes possèdent tous leurs propres configurations de scan qu'ils créent. Ces configurations de scan ont un ARN qui indique l'ID du compte en tant que propriétaire :

`arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`111122223333`*`/cis-configuration/`*`scanId`*

Un compte membre peut consulter les résultats des scans sur son compte, y compris les résultats des scans CIS planifiés par l'administrateur délégué.

## Compartiments Amazon S3 appartenant à Amazon Inspector et utilisés pour les scans CIS par Amazon Inspector

L'Open Vulnerability and Assessment Language (OVAL) est un effort de sécurité de l'information qui normalise la manière d'évaluer et de signaler l'état des machines des systèmes informatiques. Le tableau suivant répertorie tous les compartiments Amazon S3 appartenant à Amazon Inspector dotés de définitions OVAL utilisés pour les scans CIS. Amazon Inspector prépare les fichiers de définition OVAL requis pour les scans CIS. Les compartiments Amazon S3 appartenant à Amazon Inspector doivent être autorisés VPCs si nécessaire.

> **Note**
>
> Les détails de chacun des compartiments Amazon S3 suivants appartenant à Amazon Inspector ne sont pas sujets à modification. Cependant, le tableau peut être mis à jour pour refléter les nouvelles fonctionnalités prises en charge Régions AWS. Vous ne pouvez pas utiliser les compartiments Amazon S3 appartenant à Amazon Inspector pour d'autres opérations Amazon S3 ou dans vos propres compartiments Amazon S3.

| seau CIS | Région AWS |
|---|---|
| `cis-datasets-prod-arn-5908f6f` | Europe (Stockholm) |
| `cis-datasets-prod-bah-8f88801` | Moyen-Orient (Bahreïn) |
| `cis-datasets-prod-bjs-0f40506` | Chine (Beijing) |
| `cis-datasets-prod-bom-435a167` | Asie-Pacifique (Mumbai) |

| seau CIS | Région AWS |
|---|---|
| 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) |
| 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) |

| seau CIS | Région AWS |
| --- | --- |
| `cis-datasets-prod-yul-5e0c95e` | Canada (Centre) |
| `cis-datasets-prod-zhy-5a8eacb` | Chine (Ningxia) |
| `cis-datasets-prod-zrh-67e0e3d` | Europe (Zurich) |

# Création d'une configuration de scan CIS

Cette rubrique décrit comment créer une configuration de scan CIS.

Pour exécuter un scan CIS

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le Région AWS menu déroulant pour sélectionner l' Région AWS endroit où vous souhaitez exécuter une analyse CIS.
3. Dans le volet de navigation, choisissez Analyses à la demande, puis sélectionnez Analyses CIS.
4. Choisissez Créer un nouveau scan.
5. Pour Nom de configuration de numérisation, entrez un nom de configuration de numérisation.
6. Pour les balises de ressource cible, entrez une clé et la valeur correspondante pour les instances que vous souhaitez scanner. Vous pouvez spécifier jusqu'à cinq valeurs différentes pour chaque clé et un total de 25 balises à inclure dans le scan.
7. Pour le niveau CIS Benchmark, vous pouvez sélectionner le niveau 1 pour les configurations de sécurité de base ou le niveau 2 pour les configurations de sécurité avancées.
8. Pour les comptes Target, spécifiez les comptes à inclure dans le scan CIS. Pour de plus amples informations, veuillez consulter Considérations relatives à la gestion des scans Amazon Inspector CIS avec AWS Organizations.

   Si votre compte est le compte d'administrateur délégué, vous pouvez sélectionner Tous les comptes ou Spécifier les comptes. L'option Tous les comptes cible tous les comptes de votre organisation. L'option Spécifier les comptes cible uniquement les comptes individuels de votre organisation. Si vous choisissez cette option, vous pouvez spécifier plusieurs comptes en séparant les numéros de compte par une virgule. Vous pouvez également saisir, à la `SELF` place d'un identifiant de compte, une configuration de numérisation pour votre compte.

Si votre compte est un compte autonome ou un compte membre d'une organisation, vous pouvez sélectionner Self pour créer une configuration de numérisation pour votre compte.

9. Pour Planifier, choisissez Scan unique, qui s'exécute dès que vous avez fini de créer votre configuration de scan, ou Scans récurrents, qui s'exécutent à l'heure que vous spécifiez.
10. Confirmez vos choix, puis choisissez Créer.

# Affichage des résultats du scan CIS

Amazon Inspector crée une tâche de scan pour chaque configuration de scan qui s'exécute et collecte les résultats d'un scan avec un identifiant de scan unique. Les résultats du scan CIS sont disponibles pendant 90 jours. Vous pouvez afficher les résultats de l'analyse CIS à l'aide de ses contrôles ou de ses ressources numérisées :

- Résultats du scan agrégés par contrôles : regroupe les résultats d'un scan pour chaque contrôle individuel effectué pendant le scan. Pour chaque vérification, vous obtenez un rapport indiquant le nombre de ressources qui ont échoué, qui ont été ignorées ou qui ont été utilisées.
- Résultats de numérisation agrégés par ressources numérisées : regroupe les résultats d'une analyse par ressource numérisée ciblée pendant l'analyse. Pour chaque ressource, vous obtenez un rapport indiquant le nombre de vérifications auxquelles une ressource a échoué, a été ignorée ou a réussi.

Cette rubrique décrit comment afficher les résultats d'une analyse CIS.

Pour afficher les résultats du scan

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le Région AWS menu déroulant pour sélectionner l' Région AWS endroit où vous avez créé votre configuration de scan CIS.
3. Dans le volet de navigation, choisissez Analyses à la demande, puis sélectionnez Analyses CIS.
4. Choisissez l'onglet Résultats du scan.
5. Dans la colonne Planifié par, choisissez l'ID du calendrier de numérisation que vous souhaitez afficher. Vous pouvez également sélectionner la ligne contenant l'ID du calendrier de numérisation que vous souhaitez afficher, puis choisissez Afficher les détails.

6. Choisissez Contrôles pour afficher chaque contrôle effectué ou Ressources numérisées pour afficher chaque ressource numérisée ciblée lors de l'analyse.

Vous pouvez également consulter les détails des scans CIS planifiés.

Pour afficher les détails des scans CIS planifiés

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le Région AWS menu déroulant pour sélectionner l' Région AWS endroit où vous avez créé votre configuration de scan CIS.
3. Dans le volet de navigation, choisissez Analyses à la demande, puis sélectionnez Analyses CIS.
4. Choisissez l'onglet Planifié.
5. Dans la colonne Nom de la configuration de numérisation, choisissez le nom de la configuration de numérisation que vous souhaitez consulter. Vous pouvez également sélectionner la ligne contenant la configuration de numérisation que vous souhaitez afficher, puis choisissez Afficher les détails.

# Modification d'une configuration de scan CIS

Cette rubrique décrit comment modifier une configuration de scan CIS.

Pour modifier une configuration de scan CIS

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le Région AWS menu déroulant pour sélectionner l' Région AWS endroit où vous avez créé votre configuration de scan CIS.
3. Dans le volet de navigation, choisissez Analyses à la demande, puis sélectionnez Analyses CIS.
4. Choisissez l'onglet Planifié.
5. Sélectionnez la ligne contenant la configuration de numérisation que vous souhaitez modifier, puis choisissez Modifier.

# Téléchargement des résultats d'un scan CIS

Vous pouvez télécharger un PDF ou un CSV d'un scan CIS à l'aide de la console ou de l'API Amazon Inspector.

> **Note**
>
> Vous ne pouvez télécharger un fichier CSV contenant les résultats de votre scan CIS que pour les scans CIS collectés après le 05/03/2024.

Cette rubrique explique comment télécharger un scan CIS à l'aide de la console Amazon Inspector.

Pour télécharger les résultats du scan CIS depuis la console

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le Région AWS menu déroulant pour sélectionner l' Région AWS endroit où vous avez créé votre configuration de scan CIS.
3. Dans le volet de navigation, choisissez Analyses à la demande, puis sélectionnez Analyses CIS.
4. Choisissez l'onglet Résultats du scan.
5. Dans la colonne Planifié par, choisissez l'ID du calendrier de numérisation que vous souhaitez afficher. Vous pouvez également sélectionner la ligne contenant l'ID du calendrier de numérisation que vous souhaitez afficher, puis choisissez Afficher les détails.
6. Choisissez Télécharger, puis choisissez PDF ou CSV. Si votre compte est le compte d'administrateur délégué, vous pouvez choisir Sélectionner un compte pour télécharger les résultats d'un compte de membre spécifique.

# Comprendre les résultats d'Amazon Inspector

Amazon Inspector génère un résultat lorsqu'il détecte une vulnérabilité dans une EC2 instance Amazon, une image de conteneur dans Amazon ECR ou une AWS Lambda fonction. Une constatation est un rapport détaillé sur une vulnérabilité affectant l'une de vos AWS ressources.

Les résultats sont nommés d'après des vulnérabilités et fournissent des évaluations de gravité, des informations sur les AWS ressources touchées et des détails décrivant comment remédier aux vulnérabilités détectées. Amazon Inspector stocke tous vos résultats actifs jusqu'à ce que vous les corrigiez.

Lorsqu'une ressource est supprimée ou résiliée, Amazon Inspector ferme automatiquement les résultats associés à la ressource, puis les supprime au bout de sept jours. Si les résultats sont fermés pour une autre raison, ils sont supprimés au bout de 30 jours.

> **Note**
>
> Amazon Inspector rouvrira une découverte corrigée dans les sept jours suivant sa fermeture si le problème à l'origine de la vulnérabilité se reproduit.

Si vous désactivez Amazon Inspector, les résultats sont supprimés au bout de 24 heures. Si une ressource est supprimée, toute constatation liée à la ressource est supprimée au bout de sept jours. En cas de AWS suspension de votre compte, les résultats sont supprimés au bout de 90 jours. Les résultats relatifs aux instances arrêtées restent actifs.

Les résultats indiquent

Amazon Inspector classe les résultats dans les états suivants.

Actif

Amazon Inspector classe un résultat qui n'a pas été corrigé comme actif.

Supprimé

Amazon Inspector classe une découverte soumise à une ou plusieurs règles de suppression dans la catégorie Supprimée.

Fermées

Lorsqu'un résultat a été corrigé, Amazon Inspector le classe dans la catégorie Fermé.

Rubriques



# Types de recherche Amazon Inspector

Cette section décrit les différents types de recherche dans Amazon Inspector.

Rubriques



## 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 risques courants (CVEs). 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/.

Amazon Inspector peut générer des informations sur les vulnérabilités des packages pour les EC2 instances, 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 activez le scan du code Lambda par Amazon Inspector.

Les extraits de code détectés en lien avec une vulnérabilité de code sont stockés par le CodeGuru service. 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 de plus amples informations, veuillez consulter 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 EC2 instances Amazon 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 12 heures une fois Amazon Inspector activé.

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

- EC2 Instances Amazon
- 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

## Afficher les résultats de votre Amazon Inspector

Vous pouvez consulter vos résultats Amazon Inspector dans la console Amazon Inspector et à l'aide de l'`ListFindings`API Amazon Inspector. Dans la console Amazon Inspector, vous pouvez consulter vos résultats dans le tableau de bord Amazon Inspector et sur l'écran Résultats. Vous pouvez également consulter vos résultats dans AWS Security Hub Amazon Elastic Container Registry (Amazon ECR). Par défaut, le tableau de bord et l'écran Findings d'Amazon Inspector affichent vos résultats actifs. Vous pouvez également consulter vos résultats par catégorie. Les procédures décrites dans cette section décrivent comment consulter vos résultats dans la console Amazon Inspector et à l'aide de l'API Amazon Inspector.

Console

Pour consulter les résultats d'Amazon Inspector

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.

2. (Facultatif) Dans le volet de navigation, choisissez Dashboard. Le tableau de bord présente une vue d'ensemble de la couverture de votre environnement et uniquement vos résultats critiques.
3. (Facultatif) Dans le volet de navigation, choisissez Findings. L'écran Résultats affiche tous vos résultats actifs dans un tableau dans lequel vous pouvez filtrer vos résultats par statut et par critère de filtrage. Vous pouvez également créer des règles de suppression pour exclure les résultats de l'affichage. Vous pouvez consulter les détails d'une recherche en choisissant le nom de la recherche.
4. (Facultatif) Dans le volet de navigation, choisissez l'une des options suivantes pour afficher vos résultats par catégorie :

   - Par vulnérabilité : affiche vos vulnérabilités les plus critiques.
   - Par compte : affiche tous vos comptes, la couverture du scan et le nombre total de résultats avec des notes de gravité critique et élevée.

     > **Note**
     >
     > Cette catégorie est réservée aux administrateurs délégués.

   - Par instance : affiche vos instances Amazon EC2 les plus vulnérables.

     > **Note**
     >
     > Les résultats regroupés dans cette catégorie n'incluent pas d'informations sur la disponibilité du réseau.

   - Par image de conteneur — Affiche les images de vos conteneurs Amazon ECR les plus vulnérables.
   - Par référentiel de conteneurs : affiche vos référentiels les plus vulnérables.
   - Par fonction Lambda — Affiche vos fonctions Lambda les plus vulnérables.

API

Pour consulter les résultats d'Amazon Inspector

- Exécutez l'opération ListFindingsAPI. Dans la demande, spécifiez FilterCriteria pour renvoyer des résultats spécifiques.

# Afficher les informations relatives aux résultats de vos recherches sur Amazon Inspector

La procédure décrite dans cette section explique comment consulter les informations relatives aux résultats d'Amazon Inspector.

Pour consulter les détails d'une recherche

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 de votre 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, voirComprendre les niveaux de gravité des conclusions de votre 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 EC2 instances, les images de conteneurs ECR et les fonctions Lambda. Pour plus d'informations, consultez Vulnérabilité du package.

Les résultats de vulnérabilité des packages incluent également[Consulter le score d'Amazon Inspector et comprendre les informations détaillées 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 des EC2 instances scannées à l'aide de[Numérisation sans agent](#).
- 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 le Common Vulnerabilities and Exposures (CVEs) 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, voirComprendre les niveaux de gravité des conclusions de votre Amazon Inspector. Les scores suivants sont inclus, y compris les vecteurs de notation pour chacun :
  - Score du système EPSS (Exploit Prediction Scoring System)
  - 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 versions plus anciennes) CVEs
- Vulnérabilités associées — Spécifie les autres vulnérabilités liées à la découverte. Il s'agit généralement d'autres CVEs éléments qui ont un impact sur la même version du package, ou d'autres CVEs appartenant au même groupe que le CVE trouvé, tel que 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 mêmeYES.
- 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 : IDs du Common Weakness Enumeration (CWE) associé 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 EC2 instances. Pour plus d'informations, consultez Accessibilité du réseau. Ce type de recherche comporte les détails suivants :

- Plage de ports ouverts : plage de ports par laquelle l' EC2 instance est accessible.
- Chemins réseau ouverts : indique le chemin d'accès libre à l' EC2 instance. Sélectionnez un élément sur le chemin pour plus d'informations.
- Correction : recommande une méthode pour fermer le chemin réseau ouvert.

# Consulter le score d'Amazon Inspector et comprendre les informations détaillées sur les vulnérabilités

Amazon Inspector crée un score pour les résultats des instances Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez consulter le score Amazon Inspector et les informations relatives aux vulnérabilités dans la console Amazon Inspector. Le score Amazon Inspector vous fournit des informations que vous pouvez comparer aux indicateurs du Common Vulnerability Scoring System. Ces informations ne sont disponibles que pour les découvertes relatives à la vulnérabilité des packages. Cette section explique comment interpréter le score d'Amazon Inspector et comprendre les informations détaillées sur les vulnérabilités.

## Note d'Amazon Inspector

Le score Amazon Inspector est un score contextualisé créé par Amazon Inspector pour chaque recherche d' EC2 instance. 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 forme « Source de vulnérabilité » (ou packageVulnerabilityDetails.source dans le résultat (JSON)

> **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 par first.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 CVEs.

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

AT&CK

Cette section présente les tactiques, techniques et procédures MITRE (TTPs) associées au CVE. Les informations associées TTPs sont affichées, s'il y en a plus de deux applicables, TTPs 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.

# Comprendre les niveaux de gravité des conclusions de votre Amazon Inspector

Lorsqu'Amazon Inspector génère une constatation, il lui attribue une note de gravité. Les indices de gravité vous aident à évaluer et à hiérarchiser vos résultats. L'indice de gravité d'une constatation correspond à un score et à un niveau numériques : informationnel, faible, moyen, élevé et critique. Amazon Inspector détermine le niveau de gravité d'une constatation en fonction du type de constatation. Cette section décrit comment Amazon Inspector détermine une note de gravité pour chaque type de constatation.

## Gravité de la vulnérabilité des progiciels

Amazon Inspector utilise le NVD/CVSS score as the basis of severity scoring for software package vulnerabilities. The NVD/CVSS score is the vulnerability severity score published by the NVD and defined by the CVSS. The NVD/CVSS score comme 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 | Notation |
| --- | --- |
| 0 | Informationnel |
| 0,1 à 3,9 | Faible |
| 4,0—6,9 | Moyen |
| 7,0—8,9 | Élevé |
| 9,0—10,0 | Critique |

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 la référence du résultat URLs pour étudier cette vulnérabilité et 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 réseaux pairs et AWS Direct Connect de VPCs réseaux. 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 | Moyen | Informationnel |
| Elasticsearch | 9300, 9200 | NA | Moyen | Informationnel |
| FTP | 21 | 21 | Élevé | Moyen |
| Catalogue global LDAP | 3268 | NA | Moyen | Informationnel |
| Catalogue global LDAP via TLS | 3269 | NA | Moyen | Informationnel |
| HTTP | 80 | 80 | Faible | Informationnel |
| HTTPS | 443 | 443 | Faible | Informationnel |
| Kerberos | 88, 464, 543, 544, 749, 751 | 88, 464, 749, 750, 751, 752 | Moyen | Informationnel |
| LDAP | 389 | 389 | Moyen | Informationnel |
| LDAP via TLS | 636 | NA | Moyen | Informationnel |
| MongoDB | 27017, 27018, 27019, 28017 | NA | Moyen | Informationnel |
| MySQL | 3306 | NA | Moyen | Informationnel |
| NetBIOS | 137, 139 | 137, 138 | Moyen | Informationnel |
| NFS | 111, 2049, 4045, 1110 | 111, 2049, 4045, 1110 | Moyen | Informationnel |
| Oracle | 1521, 1630 | NA | Moyen | Informationnel |
| PostgreSQL | 5432 | NA | Moyen | Informationnel |
| Services d'impression | 515 | NA | Élevé | Moyen |
| RDP | 3389 | 3389 | Moyen | Faible |

| | | | | |
|---|---|---|---|---|
| RPC | 111, 135, 530 | 111, 135, 530 | Moyen | Informationnel |
| SMB | 445 | 445 | Moyen | Informationnel |
| SSH | 22 | 22 | Moyen | Faible |
| SQL Server | 1433 | 1434 | Moyen | Informationnel |
| Syslog | 601 | 514 | Moyen | Informationnel |
| Telnet | 23 | 23 | Élevé | Moyen |
| WINS | 1512, 42 | 1512, 42 | Moyen | Informationnel |

# Gestion des résultats dans Amazon Inspector

Avec Amazon Inspector, vous pouvez gérer vos résultats de différentes manières. Vous pouvez filtrer vos résultats en fonction de leur statut. Vous pouvez rechercher vos résultats en fonction de critères de filtrage. Vous pouvez créer des règles de suppression pour exclure les résultats de votre liste de résultats. Vous pouvez également exporter les résultats vers AWS Security Hub Amazon EventBridge et Amazon Simple Storage Service (Amazon S3).

Rubriques



# Filtrer les résultats de votre Amazon Inspector

Vous pouvez filtrer les résultats de votre Amazon Inspector à l'aide de critères de filtrage. Si un résultat ne correspond pas à vos critères de filtre, Amazon Inspector l'exclut de la vue. Cette section explique comment filtrer les résultats de votre Amazon Inspector à l'aide de critères de filtrage.

## 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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.

# Supprimer les résultats d'Amazon Inspector

Vous pouvez créer des règles de suppression pour masquer les résultats correspondant aux critères. Par exemple, vous pouvez créer une règle de suppression pour masquer les résultats en fonction de leur niveau de gravité. Si Amazon Inspector génère un résultat qui correspond à votre règle de suppression, Amazon Inspector supprime le résultat et le masque. Amazon Inspector conserve les résultats supprimés jusqu'à ce qu'ils soient corrigés. Une fois qu'un résultat supprimé est corrigé, Amazon Inspector ferme le résultat. Vous pouvez consulter les résultats supprimés dans la console.

Vous créez des règles de suppression pour hiérarchiser vos découvertes les plus importantes. Les règles de suppression n'ont aucun impact sur vos résultats, car elles ne font que masquer les résultats. Vous ne pouvez pas créer de règle de suppression qui ferme ou corrige les résultats. Vous pouvez également supprimer les résultats indésirables à l' AWS Security Hub aide d'une EventBridge règle Amazon. Les procédures décrites dans cette section décrivent comment créer, afficher, modifier et supprimer une règle de suppression.

> **Note**
>
> Seul l'administrateur délégué d'une organisation peut créer et gérer des 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 d'une règle de suppression

Vous pouvez modifier les règles de suppression à tout moment.

Pour modifier les règles de suppression

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Règles de suppression.
3. Choisissez le nom de la règle de suppression que vous souhaitez modifier, puis choisissez Modifier.
4. Apportez les modifications souhaitées, puis choisissez Enregistrer.

## Supprimer une règle 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 des rapports de résultats d'Amazon Inspector

Un rapport de résultats est un fichier CSV ou JSON qui fournit un aperçu détaillé de vos résultats. Vous pouvez exporter un rapport de résultats vers AWS Security Hub Amazon EventBridge et Amazon Simple Storage Service (Amazon S3). Lorsque vous configurez un rapport de résultats, vous spécifiez les résultats à inclure dans celui-ci. Par défaut, votre rapport de résultats inclut des données pour tous vos résultats actifs. Si vous êtes l'administrateur délégué d'une organisation, votre rapport de résultats inclut les données de tous les comptes membres de l'organisation. Pour personnaliser un rapport de résultats, créez et appliquez-lui un filtre.

Lorsque vous exportez un rapport de résultats, Amazon Inspector chiffre les données de vos résultats à l'aide d'un rapport AWS KMS key que vous spécifiez. Une fois qu'Amazon Inspector a chiffré les données de vos résultats, il stocke votre rapport de recherche dans un compartiment Amazon S3 que vous spécifiez. Votre AWS KMS clé doit être utilisée au même endroit Région AWS que votre compartiment Amazon S3. Votre politique AWS KMS clé doit autoriser Amazon Inspector à l'utiliser, et votre politique de compartiment Amazon S3 doit autoriser Amazon Inspector à y ajouter des objets. Après avoir exporté votre rapport de résultats, vous pouvez le télécharger depuis votre compartiment Amazon S3 ou le transférer vers un nouvel emplacement. Vous pouvez également utiliser votre compartiment Amazon S3 comme référentiel pour d'autres rapports de résultats exportés.

Cette section explique comment exporter un rapport de résultats dans la console Amazon Inspector. Les tâches suivantes nécessitent que vous vérifiiez vos autorisations, que vous configuriez un compartiment Amazon S3, que vous configuriez un AWS KMS key compartiment et que vous configuriez et exportiez un rapport de résultats.

> **Note**
>
> Si vous exportez un rapport de résultats avec l'CreateFindingsReportAPI Amazon Inspector, vous ne pouvez consulter que vos résultats actifs. Si vous souhaitez consulter vos résultats

supprimés ou fermés, vous devez spécifier les critères de filtrage `SUPPRESSED` ou `CLOSED` en faire partie.

Tâches

- Étape 1 : Vérifier vos autorisations
- Étape 2 : Configuration d'un compartiment S3
- Étape 3 : Configuration d'un AWS KMS key
- Étape 4 : Configuration et exportation d'un rapport de résultats
- Résoudre les erreurs d'exportation

## Étape 1 : Vérifier vos autorisations

> **Note**
>
> Après avoir exporté un rapport de résultats pour la première fois, les étapes 1 à 3 sont facultatives. Pour suivre ces étapes, vous devez déterminer si vous souhaitez utiliser le même compartiment Amazon S3 et AWS KMS key pour d'autres rapports de résultats exportés. Si vous souhaitez exporter un rapport de résultats par programmation après avoir effectué les étapes 1 à 3, utilisez le CreateFindingsReportfonctionnement de l'API Amazon Inspector.

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 examiner 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

Pour AWS 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. Connectez-vous à l'aide de vos informations d'identification, puis 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. Sélectionnez l'onglet 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:::amzn-s3-demo-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 :

   - *amzn-s3-demo-bucket*est le nom du compartiment.
   - *111122223333*est l'identifiant de compte de votre Compte AWS.
   - *Region*est celui Région AWS dans lequel 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 manuellement Région 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 `me-south-1` code de région est indiqué, `inspector2.amazonaws.com` remplacez-le `inspector2.me-south-1.amazonaws.com` par 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 Amazon Resource Names (ARNs) 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 l'Amazon Resource Name (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

> **Note**
>
> La procédure suivante permet de mettre à jour une clé existante afin de permettre à Amazon Inspector de l'utiliser. Si vous n'avez pas de clé existante, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.

Pour mettre à jour la politique clé

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
2. Dans le volet de navigation, sélectionnez Clés gérées par le client.
3. Choisissez la clé KMS que vous souhaitez utiliser pour chiffrer le rapport. La clé doit être une clé de chiffrement symétrique (SYMMETRIC_DEFAULT).
4. 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.
5. 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/*"
        }
    }
}
```

6. 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.

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

   - *111122223333*est l'identifiant de compte de votre Compte AWS.
   - *Region*est celui Région AWS dans lequel 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 manuellement Région 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), `inspector2.amazonaws.com` remplacez 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 AWS effectuer 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 cette condition ARNs pour chaque compte supplémentaire. 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 avec AWS KMS. Bien que cela ne soit pas recommandé, vous pouvez supprimer ces conditions de la déclaration.

8. 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

> **Note**
>
> Vous ne pouvez exporter qu'un seul rapport de résultats à la fois. Si une exportation est en cours, vous devez attendre qu'elle soit terminée avant d'exporter un autre 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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.

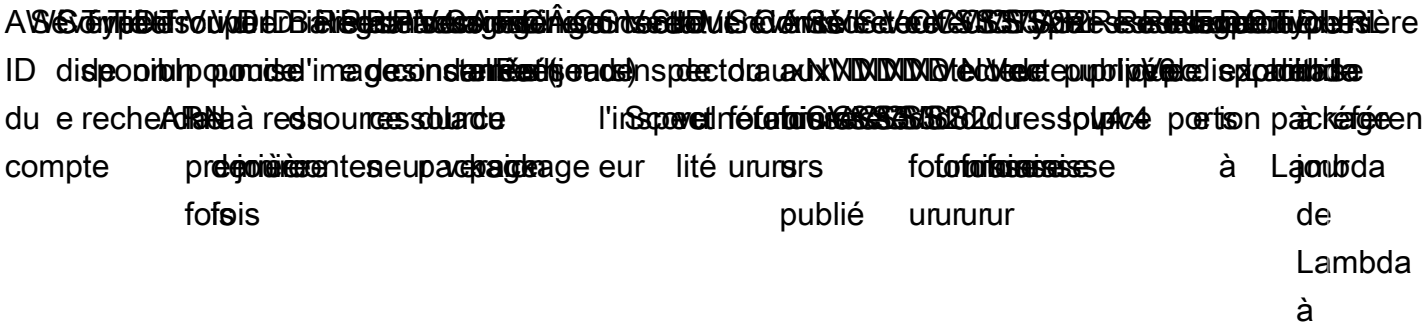
4. Choisissez Exporter les résultats.
5. Dans la section Paramètres d'exportation, pour Type de fichier d'exportation, spécifiez un format de fichier pour le rapport :

   - 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 de la notation et URLs les références 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. Cliquez sur 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 essayez 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 conclusions d'Amazon Inspector avec Amazon EventBridge

Amazon Inspector crée un événement dans Amazon EventBridge pour les résultats nouvellement générés et les résultats agrégés. Amazon Inspector crée également un événement pour toute modification de l'état d'un résultat. Cela signifie qu'Amazon Inspector crée un nouvel événement pour une recherche lorsque vous effectuez des actions telles que le redémarrage d'une ressource ou la modification des balises associées à une ressource. Lorsqu'Amazon Inspector crée un nouvel événement pour un résultat mis à jour, le résultat `id` reste le même.

> **Note**
>
> Si votre compte est un compte d'administrateur délégué Amazon Inspector, il EventBridge publie les événements sur votre compte et sur le compte du membre d'où proviennent les événements.

Lorsque vous utilisez EventBridge des événements avec Amazon Inspector, vous pouvez automatiser les tâches pour vous aider à résoudre les problèmes de sécurité révélés par vos résultats. Pour recevoir des notifications concernant les résultats d'Amazon Inspector basés sur EventBridge des événements, vous devez créer une EventBridge règle et spécifier un objectif pour Amazon Inspector. La EventBridge règle permet d' EventBridge envoyer des notifications pour les résultats d'Amazon Inspector, et la cible indique où envoyer les notifications.

Amazon Inspector émet des événements vers le bus d'événements par défaut dans Région AWS lequel vous utilisez actuellement Amazon Inspector. Cela signifie que vous devez configurer des règles d'événements pour chaque Région AWS endroit où vous avez activé Amazon Inspector et configuré Amazon Inspector pour recevoir des EventBridge événements. Amazon Inspector émet des événements dans la mesure du possible.

Cette section fournit un exemple de schéma d'événement et décrit comment créer une EventBridge règle.

## Schéma d'événement

Voici un exemple du format d'événement Amazon Inspector pour un événement de EC2 recherche. Par exemple, le schéma des autres types de recherche et types 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 augmenter 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' EventBridge événement.

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

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

Cette procédure définit l'endroit où vous souhaitez envoyer les données des résultats d'Amazon Inspector. La rubrique SNS peut être ajoutée à une règle d' EventBridge événement pendant ou après la création de la règle d'événement.

Email setup

Création d'une rubrique SNS

1. Connectez-vous à la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/
2. Dans le volet de navigation, sélectionnez Sujets, puis sélectionnez Créer un sujet.
3. Dans la section Créer un sujet, sélectionnez Standard. Entrez ensuite un nom de rubrique, tel que**`Inspector_to_Email`**. D'autres détails sont facultatifs.
4. Choisissez Créer la rubrique. Cela ouvre un nouveau panneau contenant les détails de 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, entrez l'adresse e-mail à laquelle vous souhaitez recevoir des notifications.

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

c. Choisissez Créer un abonnement.

7. Recherchez un message d'abonnement dans votre boîte de réception et choisissez Confirmer l'abonnement.

Slack setup

Création d'une rubrique SNS

1. Connectez-vous à la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/
2. Dans le volet de navigation, sélectionnez Sujets, puis sélectionnez Créer un sujet.
3. Dans la section Créer un sujet, sélectionnez Standard. Entrez ensuite un nom de rubrique, tel que**`Inspector_to_Slack`**. D'autres détails sont facultatifs. Choisissez Créer un sujet pour terminer la création du point de terminaison.

Configuration d'un développeur Amazon Q dans un client d'applications de chat

1. Accédez au développeur Amazon Q dans la console des applications de chat à l'adressehttps://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 accordées à Amazon Q Developer dans les applications de chat pour accéder 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 le canal.

b. Pour la chaîne Slack, choisissez la chaîne que vous souhaitez 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 Management Console fenêtre Amazon Q Developer dans les applications de chat, collez l'identifiant de chaîne que vous avez copié depuis Slack dans le champ ID de chaîne privée.

e. Dans Autorisations, choisissez de créer un rôle IAM à l'aide d'un modèle si vous n'en avez pas déjà un.

f. Pour les modèles de politique, choisissez Autorisations de notification. Il s'agit du modèle de politique IAM pour Amazon Q Developer dans les applications de chat. 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 du canal, 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 à la chaîne Slack.

5. Sélectionnez Configure (Configurer).

## Amazon Chime setup

### Création d'une rubrique SNS

1. Connectez-vous à la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/
2. Sélectionnez Sujets dans le volet de navigation, puis sélectionnez Créer un sujet.
3. Dans la section Créer un sujet, sélectionnez Standard. Entrez ensuite un nom de rubrique, tel que**`Inspector_to_Chime`**. D'autres détails sont facultatifs. Choisissez Créer un sujet pour terminer.

Configuration d'un développeur Amazon Q dans un client d'applications de chat

1. Accédez au développeur Amazon Q dans la console des applications de chat à l'adressehttps://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, saisissez le nom du canal.
5. Dans Amazon Chime, ouvrez le salon de discussion souhaité.
    a. Choisissez l'icône d'engrenage dans le coin supérieur droit, puis sélectionnez Manage webhooks (Gérer les webhooks) .
    b. Sélectionnez Copier l'URL pour copier l'URL du webhook dans votre presse-papiers.
6. Dans la AWS Management Console fenêtre Amazon Q Developer dans les applications de chat, 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 n'en avez pas déjà un.
8. Pour les modèles de politique, choisissez Autorisations de notification. Il s'agit du modèle de politique IAM pour Amazon Q Developer dans les applications de chat. 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. Connectez-vous à l'aide de vos informations d'identification.
2. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
3. Sélectionnez Règles dans le volet de navigation, puis sélectionnez Créer une règle.
4. Entrez un nom et une description facultative pour votre règle.
5. Sélectionnez Règle avec un modèle d'événement, puis Suivant.
6. Dans le volet Event Pattern, sélectionnez Custom patterns (éditeur JSON).
7. Collez le code 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 résultat actif `CRITICAL` ou de `HIGH` gravité détecté par Amazon Inspector.

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

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

## EventBridge pour les environnements multi-comptes Amazon Inspector

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

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

# Utilisation du tableau de bord dans Amazon Inspector

Le tableau de bord fournit un aperçu des statistiques agrégées relatives aux ressources analysées par Amazon Inspector. Utilisez le tableau de bord pour en savoir plus sur la couverture de votre environnement et sur les résultats critiques.

> **Note**
>
> Si votre compte est le compte d'administrateur délégué d'une organisation, le tableau de bord affiche les informations relatives à votre compte et à tous les autres comptes de l'organisation.

Cette section explique comment afficher le tableau de bord et comprendre les composants qui le composent.

Rubriques



## 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 consulter le tableau de bord :

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, choisissez Dashboard.
    a. Le tableau de bord actualise les données automatiquement toutes les cinq minutes. Vous pouvez actualiser les données manuellement en sélectionnant l'icône d'actualisation dans le coin supérieur droit de la page.
    b. Vous pouvez consulter les données justificatives d'un article en le sélectionnant.

c. Si votre compte est le compte administrateur délégué d'une organisation, vous pouvez consulter les statistiques agrégées d'un compte membre en saisissant l'identifiant du compte membre dans le champ Compte.

# Comprendre les composants du tableau de bord et interpréter les données

Chaque section du tableau de bord fournit un aperçu des indicateurs clés et des données de résultats, afin que vous puissiez comprendre le niveau de vulnérabilité de vos AWS ressources par rapport à votre situation actuelle Région AWS.

Couverture environnementale

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' EC2 instances Amazon, d'images Amazon ECR et de AWS Lambda fonctions numérisées par Amazon Inspector. Si vous gérez plusieurs comptes AWS Organizations en tant qu'administrateur délégué d'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 obtenu 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 entreprise 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 du groupe que vous sélectionnez. La page de gestion des comptes indique en détail quels comptes, EC2 instances Amazon 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

Constatations critiques

La section Résultats critiques fournit un décompte des vulnérabilités critiques de votre environnement et un décompte total de toutes les découvertes dans votre environnement. Dans cette section, les chiffres sont présentés par ressource et par type d'évaluation. Pour plus d'informations sur les résultats critiques et sur la manière dont Amazon Inspector détermine le caractère critique, consultezComprendre les résultats d'Amazon Inspector.

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

Les groupes de constatations critiques suivants sont disponibles :

- Constatations relatives aux images des conteneurs ECR
- EC2 Conclusions d'Amazon
- Résultats relatifs à l'accessibilité du réseau
- AWS Lambda résultats relatifs aux fonctions

Remédiations basées sur les risques

La section Corrections basées sur les risques présente les cinq principaux progiciels présentant des vulnérabilités critiques qui affectent le plus de ressources de votre environnement. La correction de ces packages peut réduire considérablement le nombre de risques critiques pour votre environnement. Choisissez le nom du package logiciel pour voir les détails de la vulnérabilité associée et les ressources concernées.

Comptes présentant les résultats les plus critiques

La section Comptes présentant les résultats les plus critiques indique les cinq AWS comptes de votre environnement présentant les résultats les plus critiques, ainsi que le nombre total de résultats pour ce compte. Cette section est uniquement visible depuis le compte d'administrateur délégué lorsque Amazon Inspector est configuré pour le scan multi-comptes avec. AWS Organizations Cette vue permet aux administrateurs délégués de comprendre quels sont les comptes les plus exposés au sein de l'organisation.

Choisissez le numéro de compte pour obtenir 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) contenant les résultats les plus critiques présente les cinq principaux référentiels Amazon ECR de votre environnement présentant les résultats les plus critiques en matière d'images de conteneurs. La vue indique 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 les plus exposés.

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

Images de conteneurs contenant les résultats les plus critiques

La section Images de conteneurs présentant les résultats les plus critiques présente les cinq principales images de conteneur de votre environnement présentant les résultats les plus critiques. 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 doivent 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 présente les cinq EC2 instances Amazon présentant les résultats les plus critiques. La vue indique 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 de l'infrastructure à identifier les instances susceptibles de nécessiter des correctifs.

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

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

La section Amazon Machine Images (AMIs) présentant les résultats les plus critiques présente AMIs les cinq résultats les plus critiques de votre environnement. La vue indique l'identifiant de l'AMI, l'identifiant du AWS compte, le nombre d' EC2 instances 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 celles qui AMIs peuvent nécessiter une reconstruction.

Choisissez Instances affectées pour obtenir plus d'informations sur les instances lancées depuis l'AMI affectée.

AWS Lambda fonctions présentant les résultats les plus critiques

La section AWS Lambda Fonctions présentant les résultats les plus critiques présente les cinq principales fonctions Lambda de votre environnement présentant les résultats les plus critiques. La vue indique le nom de la fonction Lambda, l'identifiant du AWS compte, l'environnement d'exécution, le nombre de vulnérabilités critiques, le nombre de vulnérabilités graves et le nombre total de vulnérabilités. Cette vue aide les propriétaires de l'infrastructure à identifier les fonctions Lambda susceptibles de nécessiter des mesures correctives.

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

# Recherche dans la base de données des vulnérabilités d'Amazon Inspector

Vous pouvez effectuer une recherche dans la base de données des vulnérabilités d'Amazon Inspector pour trouver les vulnérabilités et expositions courantes (CVE). Amazon Inspector utilise les informations de la base de données de vulnérabilités pour produire des informations relatives à un identifiant CVE. Vous pouvez consulter ces informations sur l'écran des détails du CVE. Amazon Inspector suit et détecte les vulnérabilités logicielles dans la base de données de vulnérabilités. Amazon Inspector est uniquement compatible CVEs avec les plateformes répertoriées dans la section Plateformes de détection de l'écran de détails du CVE. Cette section explique comment effectuer une recherche dans la base de données des vulnérabilités d'Amazon Inspector à l'aide d'un identifiant CVE.

> **Note**
>
> 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home
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.

# Exporter SBOMs avec Amazon Inspector

Une nomenclature logicielle (SBOM) est un inventaire imbriqué de tous les composants logiciels open source et tiers de votre base de code. Amazon Inspector fournit SBOMs des ressources individuelles dans votre environnement. Vous pouvez utiliser la console Amazon Inspector ou l'API Amazon Inspector SBOMs pour générer des ressources. Vous pouvez exporter toutes SBOMs les ressources prises en charge et surveillées par Amazon Inspector. Les données exportées SBOMs fournissent des informations sur votre fournisseur de logiciels. Vous pouvez vérifier l'état de vos ressources en évaluant la couverture de votre AWS environnement. Cette section décrit comment configurer et exporter SBOMs.

> **Note**
>
> Actuellement, Amazon Inspector ne prend pas en charge l'exportation SBOMs pour les EC2 instances Amazon Windows.

## Formats Amazon Inspector

Amazon Inspector prend en charge l'exportation SBOMs dans les formats compatibles avec CyclonedX 1.4 et SPDX 2.3. Amazon Inspector exporte SBOMs 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 SBOMs

Lorsque vous exportez, SBOMs vous pouvez inclure des filtres pour créer des rapports pour des sous-ensembles de ressources spécifiques. Si vous ne fournissez pas de filtre, toutes SBOMs 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 SBOMs exporter toutes les ressources associées à un ID de compte spécifique.
- EC2 balise d'instance — Ce filtre peut être utilisé SBOMs pour exporter des EC2 instances dotées de balises spécifiques.
- Nom de la fonction — Ce filtre peut être utilisé SBOMs pour exporter des fonctions Lambda spécifiques.

- Balise d'image — Ce filtre peut être utilisé SBOMs pour exporter des images de conteneur avec des balises spécifiques.
- Balise de fonction Lambda — Ce filtre peut être utilisé pour exporter des fonctions SBOMs 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 SBOMs pour générer des images de conteneur dans des référentiels spécifiques.

## Configuration et exportation SBOMs

Pour exporter SBOMs, 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 SBOMs pour exporter des sous-ensembles spécifiques de vos ressources. Pour effectuer une exportation SBOMs 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 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 SBOMs.
4. (Facultatif) Sur la SBOMs page Exporter, utilisez le menu Ajouter un filtre pour sélectionner un sous-ensemble de ressources pour lesquelles 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 KMS clé configurée pour qu'Amazon Inspector puisse utiliser pour chiffrer vos rapports.

API

- SBOMs Pour exporter 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

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

```
aws inspector2 create-sbom-export --report-format
FORMAT --s3-destination bucketName=amzn-s3-demo-
bucket1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
```

Dans votre demande, remplacez-le *FORMAT* par le format de votre choix, CYCLONEDX_1_4 ouSPDX_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.

# Schéma EventBridge d'événements Amazon pour les événements Amazon Inspector

Amazon EventBridge fournit un flux de données en temps réel provenant d'applications et d'autres sources Services AWS à des cibles, telles que des AWS Lambda fonctions, des rubriques Amazon Simple Notification Service et des flux de données dans Amazon Kinesis Data Streams. Pour faciliter l'intégration avec d'autres applications, services et systèmes, Amazon Inspector publie automatiquement les résultats EventBridge sous forme d'événements. Vous pouvez utiliser Amazon Inspector pour publier des événements relatifs aux résultats, à la couverture et aux scans. Cette section fournit des exemples de schémas d' EventBridge événements.

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 selon le 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 conclusions d'Amazon Inspector avec Amazon EventBridge.

Les champs suivants identifient un événement de recherche :

- `detail-type`est réglé sur`Inspector2 Finding`.
- `detail`décrit le résultat.
- `detail.resources.tags`est l'endroit où les données clé-valeur sont stockées.

Vous pouvez filtrer les onglets pour voir les schémas d'événements de recherche correspondant à différentes ressources et types de recherche.

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "4d621919-f1f4-4201-a0e2-37e4e330ff51",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T17:00:36Z",
    "region": "eu-central-1",
    "resources": [
        "i-12345678901234567"
    ],
    "detail": {
        "awsAccountId": "123456789012",
        "description": "In snapd versions prior to 2.62, snapd failed to properly
 check the destination of symbolic links when extracting a snap. The snap format
 is a squashfs file-system image and so can contain symbolic links and other file
```

```
 types. Various file entries within the snap squashfs image (such as icons and
 desktop files etc) are directly read by snapd when it is extracted. An attacker who
 could convince a user to install a malicious snap which contained symbolic links
 at these paths could then cause snapd to write out the contents of the symbolic
 link destination into a world-readable directory. This in-turn could allow an
 unprivileged user to gain access to privileged information.",
        "epss": {
            "score": 0.00043
        },
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:59:44.356 UTC 2024",
        "fixAvailable": "YES",
        "inspectorScore": 4.8,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "UBUNTU_CVE",
                "score": 4.8,
                "scoreSource": "UBUNTU_CVE",
                "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Wed Sep 04 16:59:44.476 UTC 2024",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 4.8,
                    "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L",
                    "source": "UBUNTU_CVE",
                    "version": "3.1"
                },
                {
                    "baseScore": 7.3,
                    "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://www.cve.org/CVERecord?id=CVE-2024-29069",
                "https://ubuntu.com/security/notices/USN-6940-1"
```

```
            ],
            "relatedVulnerabilities": [
                "USN-6940-1"
            ],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2024/
CVE-2024-29069.html",
            "vendorCreatedAt": "Thu Jul 25 20:15:00.000 UTC 2024",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2024-29069",
            "vulnerablePackages": [
                {
                    "arch": "ALL",
                    "epoch": 0,
                    "fixedInVersion": "0:2.63+22.04ubuntu0.1",
                    "name": "snapd",
                    "packageManager": "OS",
                    "remediation": "apt-get update && apt-get upgrade",
                    "version": "2.63"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsEc2Instance": {
                        "iamInstanceProfileArn":
 "arn:aws:iam::123456789012:instance-profile/AmazonSSMRoleForInstancesQuickSetup",
                        "imageId": "ami-02ff980600c693b38",
                        "ipV4Addresses": [
                            "1.23.456.789",
                            "123.45.67.890"
                        ],
                        "ipV6Addresses": [],
                        "launchedAt": "Wed Sep 04 16:57:40.000 UTC 2024",
                        "platform": "UBUNTU_22_04",
                        "subnetId": "subnet-12345678",
                        "type": "t2.small",
                        "vpcId": "vpc-12345678"
```

```
                    }
                },
                "id": "i-12345678901234567",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_EC2_INSTANCE"
            }
        ],
        "severity": "MEDIUM",
        "status": "CLOSED",
        "title": "CVE-2024-29069 - snapd",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 17:00:36.951 UTC 2024"
    }
}
```

## Amazon EC2 network reachability finding

```
{
    "version": "0",
    "id": "9eb1603b-4263-19ec-8be2-33184694cb92",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-05T13:06:56Z",
    "region": "eu-central-1",
    "resources": ["i-12345678901234567"],
    "detail": {
        "awsAccountId": "123456789012",
        "description": "On the instance i-12345678901234567, the port range
 22-22 is reachable from the InternetGateway igw-261bab4d from an attached ENI
 eni-094ad651219472857.",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Thu Sep 05 13:06:56.334 UTC 2024",
        "lastObservedAt": "Thu Sep 05 13:06:56.334 UTC 2024",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-261bab4d",
                    "componentType": "AWS::EC2::InternetGateway"
```

```
                }, {
                    "componentId": "acl-171b527d",
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0d34debf87410f2d9",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-094ad651219472857",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-12345678901234567",
                    "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::123456789012:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-02ff980600c693b38",
                    "ipV4Addresses": ["1.23.456.789", "123.45.67.890"],
                    "ipV6Addresses": [],
                    "launchedAt": "Wed Sep 04 17:41:24.000 UTC 2024",
                    "platform": "UBUNTU_22_04",
                    "subnetId": "subnet-12345678",
                    "type": "t2.small",
                    "vpcId": "vpc-12345678"
                }
            },
            "id": "i-12345678901234567",
            "partition": "aws",
            "region": "eu-central-1",
```

```
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway - TCP",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Thu Sep 05 13:06:56.334 UTC 2024"
    }
}
```

## Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5325facf-a1aa-7d97-6bce-25fde6f6d2fc",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T16:55:38Z",
    "region": "eu-central-1",
    "resources": [
        "arn:aws:ecr:eu-central-1:123456789012:repository/inspector2/
sha256:84f507df33c6864d49c296fb734192696e4cb6f78166ac51ac8b9b118181085d"
    ],
    "detail.resources.tags.testkey": "allow",
    "detail": {
        "awsAccountId": "123456789012",
        "description": "Possible denial of service in X.509 name checks",
        "epss": {
            "score": 0.00045
        },
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:55:38.411 UTC 2024",
        "fixAvailable": "YES",
        "lastObservedAt": "Wed Sep 04 16:55:38.411 UTC 2024",
        "packageVulnerabilityDetails": {
            "cvss": [],
            "referenceUrls": [
                "https://www.cve.org/CVERecord?id=CVE-2024-6119",
```

```
                "https://ubuntu.com/security/notices/USN-6986-1"
            ],
            "relatedVulnerabilities": [
                "USN-6986-1"
            ],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2024/
CVE-2024-6119.html",
            "vendorCreatedAt": "Tue Sep 03 00:00:00.000 UTC 2024",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2024-6119",
            "vulnerablePackages": [
                {
                    "arch": "ARM64",
                    "epoch": 0,
                    "fixedInVersion": "0:3.0.13-0ubuntu3.4",
                    "name": "libssl3t64",
                    "packageManager": "OS",
                    "release": "0ubuntu3.2",
                    "remediation": "apt-get update && apt-get upgrade",
                    "sourceLayerHash":
 "sha256:1567e7ea90b67fc95ccdeeec39bdc3045098dee7e0c604975b957a9f8c0e9616",
                    "version": "3.0.13"
                },
                {
                    "arch": "ARM64",
                    "epoch": 0,
                    "fixedInVersion": "0:3.0.13-0ubuntu3.4",
                    "name": "openssl",
                    "packageManager": "OS",
                    "release": "0ubuntu3.2",
                    "remediation": "apt-get update && apt-get upgrade",
                    "sourceLayerHash":
 "sha256:1567e7ea90b67fc95ccdeeec39bdc3045098dee7e0c604975b957a9f8c0e9616",
                    "version": "3.0.13"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
```

```
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "arm64",
                        "imageHash":
 "sha256:84f507df33c6864d49c296fb734192696e4cb6f78166ac51ac8b9b118181085d",
                        "imageTags": [
                            "ubuntu_latest"
                        ],
                        "platform": "UBUNTU_24_04",
                        "pushedAt": "Wed Sep 04 16:55:28.000 UTC 2024",
                        "registry": "123456789012",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:eu-central-1:123456789012:repository/inspector2/
sha256:84f507df33c6864d49c296fb734192696e4cb6f78166ac51ac8b9b118181085d",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2024-6119 - libssl3t64, openssl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 16:55:38.411 UTC 2024"
    }
}
```

## Lambda package vulnerability finding

```
{
    "version": "0",
    "id": "9eadd71a-e49c-9864-6ba9-2a5d3f83c88f",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T16:50:37Z",
    "region": "eu-central-1",
    "resources": [
```

```
        "arn:aws:lambda:eu-central-1:123456789012:function:VulnerableFunction:
$LATEST"
    ],
    "detail": {
        "awsAccountId": "123456789012",
        "description": "Flask is a lightweight WSGI web application framework. When
 all of the following conditions are met, a response containing data intended for
 one client may be cached and subsequently sent by the proxy to other clients. If
 the proxy also caches `Set-Cookie` headers, it may send one client's `session`
 cookie to other clients. The severity depends on the application's use of the
 session and the proxy's behavior regarding cookies. The risk depends on all these
 conditions being met.\n\n1. The application must be hosted behind a caching proxy
 that does not strip cookies or ignore responses with cookies. 2. The application
 sets `session.permanent = True` 3. The application does not access or modify the
 session at any point during a request. 4. `SESSION_REFRESH_EACH_REQUEST` enabled
 (the default). 5. The application does not set a `Cache-Control` header to indicate
 that a page is private or should not be cached.\n\nThis happens because vulnerable
 versions of Flask only set the `Vary: Cookie` header when the session is ac",
        "epss": {
            "score": 0.00208
        },
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Sat Aug 31 00:04:50.000 UTC 2024"
        },
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:50:37.627 UTC 2024",
        "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:H/I:N/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Wed Sep 04 16:50:37.627 UTC 2024",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
```

```
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://www.debian.org/security/2023/dsa-5442",
                "https://lists.debian.org/debian-lts-announce/2023/08/msg00024.html"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2023-30861",
            "vendorCreatedAt": "Tue May 02 18:15:52.000 UTC 2023",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Sun Aug 20 21:15:09.000 UTC 2023",
            "vulnerabilityId": "CVE-2023-30861",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "requirements.txt",
                    "fixedInVersion": "2.3.2",
                    "name": "flask",
                    "packageManager": "PIP",
                    "version": "2.0.0"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "O7jkFEmfPB+CK3Y6Pby5zW9gjG
+zusAaqRRMGS8B27c=",
                        "executionRoleArn": "arn:aws:iam::123456789012:role/service-
role/VulnerableFunction-role-f9vs5mq8",
                        "functionName": "VulnerableFunction",
```

```
                        "lastModifiedAt": "Wed Sep 04 16:50:20.000 UTC 2024",
                        "packageType": "ZIP",
                        "runtime": "PYTHON_3_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:eu-
central-1:123456789012:function:VulnerableFunction:$LATEST",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2023-30861 - flask",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 16:50:37.627 UTC 2024"
    }
}
```

## Lambda code vulnerability finding

```
{
    "version": "0",
    "id": "e764f7be-f931-ff1b-204b-8cab2d91724b",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T16:51:01Z",
    "region": "eu-central-1",
    "resources": [
        "arn:aws:lambda:eu-central-1:123456789012:function:VulnerableFunction:
$LATEST"
    ],
    "detail": {
        "awsAccountId": "123456789012",
        "codeVulnerabilityDetails": {
            "cwes": [
                "CWE-798"
            ],
```

```
            "detectorId": "python/hardcoded-credentials@v1.0",
            "detectorName": "Hardcoded credentials",
            "detectorTags": [
                "secrets",
                "security",
                "owasp-top10",
                "top25-cwes",
                "cwe-798",
                "Python"
            ],
            "filePath": {
                "endLine": 6,
                "fileName": "lambda_function.py",
                "filePath": "lambda_function.py",
                "startLine": 6
            },
            "ruleId": "python-detect-hardcoded-aws-credentials"
        },
        "description": "Access credentials, such as passwords and access keys,
 should not be hardcoded in source code. Hardcoding credentials may cause leaks even
 after removing them. This is because version control systems might retain older
 versions of the code. Credentials should be stored securely and obtained from the
 runtime environment.",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:51:01.869 UTC 2024",
        "lastObservedAt": "Wed Sep 04 16:51:01.869 UTC 2024",
        "remediation": {
            "recommendation": {
                "text": "Your code uses hardcoded AWS credentials which might
 allow unauthorized users access to your AWS account. These attacks can occur
 a long time after the credentials are removed from the code. We recommend that
 you set AWS credentials with environment variables or an AWS profile instead.
 You should consider deleting the affected account or rotating the secret key
 and then monitoring Amazon CloudWatch for unexpected activity.\n[https://
boto3.amazonaws.com/v1/documentation/api/latest/guide/credentials.html](https://
boto3.amazonaws.com/v1/documentation/api/latest/guide/credentials.html)"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
```

```
                            "X86_64"
                        ],
                        "codeSha256": "O7jkFEmfPB+CK3Y6Pby5zW9gjG
+zusAaqRRMGS8B27c=",
                        "executionRoleArn": "arn:aws:iam::123456789012:role/service-
role/VulnerableFunction-role-f9vs5mq8",
                        "functionName": "VulnerableFunction",
                        "lastModifiedAt": "Wed Sep 04 16:50:20.000 UTC 2024",
                        "packageType": "ZIP",
                        "runtime": "PYTHON_3_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:eu-
central-1:123456789012:function:VulnerableFunction:$LATEST",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "CRITICAL",
        "status": "ACTIVE",
        "title": "CWE-798 - Hardcoded credentials",
        "type": "CODE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 16:51:01.869 UTC 2024"
    }
}
```


> **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"
    }
}
```

# Exemple de schéma d'activation automatique d'Amazon Inspector

L'événement d'activation automatique est envoyé à l'administrateur délégué lorsqu'Amazon Inspector n'est pas en mesure de prendre en charge le nombre de membres d'une organisation. Les champs suivants identifient un événement d'activation automatique :

- Le champ `detail-type` est défini sur `Inspector2 AutoEnable`.
- L'`detail`objet décrit pourquoi l'événement d'activation automatique a échoué.

```
{
    "version": "0",
    "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
    "detail-type": "Inspector2 AutoEnable",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-08-21T02:36:48Z",
    "region": "us-east-1",
    "detail": {
        “version”: “1.0.0”,
        “AutoEnableStatus”: “Failed”,
        “Reason”: "The number of member accounts enabled with AWS Inspector has reached
 the maximum limit of 10,000"
```

```
        }
}
```

# Le plug-in Amazon Inspector SSM pour Linux and Windows

Cette rubrique décrit le plug-in Amazon Inspector SSM pour Linux and Windows instances.

## Le plug-in Amazon Inspector SSM pour Linux

Amazon Inspector utilise le plug-in Amazon Inspector SSM pour effectuer des analyses d'inspection approfondies sur les instances Linux. Le plug-in Amazon Inspector SSM est automatiquement installé sur les instances Linux du `/opt/aws/inspector/bin` répertoire. Le nom de l'exécutable est`inspectorssmplugin`.

Amazon Inspector utilise Systems Manager Distributor pour déployer le plugin sur votre instance. Pour effectuer des analyses d'inspection approfondies, Systems Manager Distributor et Amazon Inspector doivent prendre en charge le système d'exploitation de votre EC2 instance Amazon. Pour plus d'informations sur les systèmes d'exploitation pris en charge par Systems Manager Distributor, consultez la section Plateformes et architectures de packages prises en charge dans le Guide de AWS Systems Manager l'utilisateur.

Amazon Inspector crée des répertoires de fichiers pour gérer les données collectées à des fins d'inspection approfondie par le plugin Amazon Inspector SSM. Ces répertoires de fichiers incluent `/opt/aws/inspector/var/input` et`/opt/aws/inspector/var/output`.

Le `packages.txt` fichier contient `/opt/aws/inspector/var/output` les chemins complets vers les packages découverts par une inspection approfondie. Si Amazon Inspector détecte le même package plusieurs fois sur votre instance, le `packages.txt` 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 SSM `InspectorLinuxDistributor-do-not-delete` essaiera de le réinstaller au prochain `inspectorssmplugin` intervalle d'analyse.

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

# Le plug-in Amazon Inspector SSM pour Windows

Le plug-in Amazon Inspector SSM est nécessaire pour qu'Amazon Inspector puisse scanner votre Windows instances. Le plug-in Amazon Inspector SSM est automatiquement installé sur votre 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.

> **Note**
>
> Vous pouvez utiliser … Windows instances avec le paramètre de configuration de gestion d'hôte par défaut. Toutefois, vous devez créer ou utiliser un rôle configuré avec les `ssm:GetParameter` autorisations `ssm:PutInventory` et.

## Désinstaller le plug-in Amazon Inspector SSM

Si le `InspectorSsmPlugin.exe` fichier est supprimé par inadvertance, l'`InspectorDistributor-do-not-delete`association le réinstallera à la `InspectorSsmPlugin.exe` prochaine Windows intervalle de numérisation. Si vous souhaitez désinstaller le plug-in Amazon Inspector SSM, vous pouvez utiliser l'action Désinstaller du `AmazonInspector2-ConfigureInspectorSsmPlugin` document. Cependant, le plug-in Amazon Inspector SSM sera automatiquement désinstallé de tous Windows hébergeurs si vous désactivez le EC2 scan Amazon.

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

# Générateur de SBOM Amazon Inspector

Une nomenclature logicielle (SBOM) est une liste officiellement structurée de composants, de bibliothèques et de modules nécessaires à la création d'un logiciel. Le générateur Amazon Inspector SBOM (Sbomgen) est un outil qui produit un SBOM pour les archives, les images de conteneurs, les répertoires, les systèmes locaux, les compilés et les fichiers binaires. Go Rust Sbomgenrecherche les fichiers contenant des informations sur les packages installés. Lorsqu'il Sbomgen trouve un fichier pertinent, il extrait les noms de package, les versions et les autres métadonnées. Sbomgentransforme ensuite les métadonnées du package en CycloneDX SBOM. Vous pouvez l'utiliser Sbomgen pour générer le CycloneDX SBOM sous forme de fichier ou dans STDOUT et l'envoyer à Amazon SBOMs Inspector pour détecter les vulnérabilités. Vous pouvez également l'utiliser dans le Sbomgen cadre de l'intégration CI/CD, qui scanne automatiquement les images des conteneurs dans le cadre de votre pipeline de déploiement.

## Types de packages pris en charge

Sbomgencollecte l'inventaire des types de colis suivants :

- Alpine APK
- Debian/Ubuntu DPKG
- Red Hat RPM
- C#
- Go
- Java
- Node.js
- PHP
- Python
- Ruby
- Rust

# Contrôles de configuration d'image de conteneur pris en charge

Sbomgenpeut scanner des fichiers Dockerfiles autonomes et créer un historique à partir d'images existantes pour des problèmes de sécurité. Pour plus d'informations, consultez Amazon Inspector Dockerfile checks.

# Installation deSbomgen

Sbomgenest uniquement disponible pour les systèmes d'exploitation Linux.

Vous devez l'avoir Docker installé si vous Sbomgen souhaitez analyser des images mises en cache localement. Dockern'est pas nécessaire pour analyser les images exportées sous forme de `.tar` fichiers ou d'images hébergées dans des registres de conteneurs distants.

Amazon Inspector vous recommande de l'exécuter Sbomgen à partir d'un système présentant au moins les caractéristiques matérielles suivantes :

- Processeur 4 cœurs
- 8 Go de RAM

Pour installer Sbomgen

1. Téléchargez le dernier 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

   Vous pouvez également télécharger les versions précédentes du fichier zip Amazon Inspector SBOM Generator.
2. Décompressez le téléchargement à l'aide de la commande suivante :

   ```
   unzip inspector-sbomgen.zip
   ```
3. Vérifiez la présence des fichiers suivants dans le répertoire extrait :

   - `inspector-sbomgen`— Il s'agit de l'outil que vous allez exécuter pour générer SBOMs.
   - `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 de l'Sbomgenoutil.
- `sbom.json`— Il s'agit d'un CycloneDX SBOM pour l'Sbomgenoutil.
- `WhatsNew.txt`— Ce fichier contient un journal des modifications résumé, qui vous permet de visualiser rapidement les principales modifications et améliorations entre Sbomgen les versions.

4. (Facultatif) Vérifiez l'authenticité et l'intégrité de l'outil 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 à l'outil 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

Cette section décrit les différentes méthodes que vous pouvez utiliserSbomgen. Pour en savoir plus sur l'utilisation, consultez Sbomgen des exemples intégrés. Pour visualiser ces exemples, exécutez la `list-examples` commande :

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

## Génère un SBOM pour une image de conteneur et affiche le résultat

Vous pouvez l'utiliser Sbomgen pour générer des images SBOMs pour le conteneur et générer le résultat dans un fichier. Cette fonctionnalité peut être activée à l'aide de la `container` sous-commande.

Exemple de commande

Dans l'extrait suivant, vous pouvez remplacer par *image:tag* l'ID de votre image et par le chemin *output_path.json* d'accès à la sortie que vous souhaitez enregistrer.

```
# generate SBOM for container image
./inspector-sbomgen container --image image:tag -o output_path.json
```

> **Note**
>
> La durée et les performances de numérisation dépendent de la taille de l'image et du petit nombre de couches. Les images plus petites améliorent non seulement Sbomgen les performances, mais réduisent également la surface d'attaque potentielle. Les images plus petites améliorent également les temps de création, de téléchargement et de chargement des images.

Lors de l'utilisation Sbomgen avec `ScanSbom`, l'API Amazon Inspector Scan ne traite pas les colis SBOMs contenant plus de 5 000 colis. Dans ce scénario, l'API Amazon Inspector Scan renvoie une réponse HTTP 400.

Si une image inclut des fichiers ou des répertoires multimédias en masse, pensez à les exclure de Sbomgen l'utilisation de l'`--skip-files`argument.

Exemple : cas d'erreur courants

La numérisation des images du conteneur peut échouer en raison des erreurs suivantes :

- `InvalidImageFormat`— Se produit lors de l'analyse d'images de conteneurs malformées contenant des en-têtes TAR, des fichiers manifestes ou des fichiers de configuration corrompus.
- `ImageValidationFailure`— Se produit lorsque la validation de la somme de contrôle ou de la longueur du contenu échoue pour les composants de l'image du conteneur, tels que des en-têtes de contenu incompatibles, des résumés de manifeste incorrects ou un échec de la vérification de la somme de contrôle. SHA256
- `ErrUnsupportedMediaType`— Se produit lorsque les composants de l'image incluent des types de média non pris en charge. Pour plus d'informations sur les types de supports pris en charge, voir Systèmes d'exploitation et types de supports pris en charge.

Amazon Inspector ne prend pas en charge ce type de `application/vnd.docker.distribution.manifest.list.v2+json` média. Amazon Inspector prend toutefois en charge les listes de manifestes. Lorsque vous scannez des images utilisant des listes de manifestes, vous pouvez spécifier explicitement la plate-forme à utiliser avec l'`--platform`argument. Si l'`--platform`argument n'est pas spécifié, le générateur Amazon Inspector SBOM sélectionne automatiquement le manifeste en fonction de la plate-forme sur laquelle il s'exécute.

## Générer un SBOM à partir de répertoires et d'archives

Vous pouvez l'utiliser Sbomgen pour générer à SBOMs partir de répertoires et d'archives. Cette fonctionnalité peut être activée à l'aide des `archive` sous-commandes `directory` ou. Amazon Inspector recommande d'utiliser cette fonctionnalité lorsque vous souhaitez générer une SBOM à partir d'un dossier de projet, tel qu'un dépôt git téléchargé.

Exemple de commande 1

L'extrait suivant montre une sous-commande qui génère une SBOM à partir d'un fichier de répertoire.

```
# generate SBOM from directory
./inspector-sbomgen directory --path /path/to/dir -o /tmp/sbom.json
```

Exemple de commande 2

L'extrait suivant montre une sous-commande qui génère une SBOM à partir d'un fichier d'archive. Les seuls formats d'archive pris en charge sont `.zip.tar`, et`.tar.gz`.

```
# generate SBOM from archive file (tar, tar.gz, and zip formats only)
./inspector-sbomgen archive --path testData.zip -o /tmp/sbom.json
```

## Génération d'un SBOM à partir de fichiers binaires Go compilés Rust

Vous pouvez l'utiliser Sbomgen pour générer à SBOMs partir de fichiers compilés Go et Rust binaires. Vous pouvez activer cette fonctionnalité via la sous-commande : `binary`

```
./inspector-sbomgen binary --path /path/to/your/binary
```

# Envoyez un SBOM à Amazon Inspector pour identifier les vulnérabilités

Outre la génération d'une SBOM, vous pouvez envoyer une SBOM à scanner à l'aide d'une seule commande depuis l'API Amazon Inspector Scan. Amazon Inspector évalue le contenu de la SBOM pour détecter les vulnérabilités avant de renvoyer les résultats à. Sbomgen En fonction de votre saisie, les résultats peuvent être affichés ou écrits dans un fichier.

> **Note**
>
> Pour utiliser cette fonctionnalité, vous devez disposer `InspectorScan-ScanSbom` d'une autorisation de lecture active Compte AWS .

Pour activer cette fonctionnalité, vous devez transmettre l'`--scan-sbom`argument à la Sbomgen CLI. Vous pouvez également transmettre l'`--scan-sbom`argument à l'une des Sbomgen sous-commandes suivantes :`archive`,`binary`, `containerdirectory`,`localhost`.

> **Note**
>
> L'API Amazon Inspector Scan ne SBOMs traite pas plus de 2 000 packages. Dans ce scénario, l'API Amazon Inspector Scan renvoie une réponse HTTP 400.

Vous pouvez vous authentifier auprès d'Amazon Inspector via un AWS profil ou un rôle IAM avec les arguments suivants : AWS CLI

```
--aws-profile profile
--aws-region region
--aws-iam-role-arn role_arn
```

Vous pouvez également vous authentifier auprès d'Amazon Inspector en fournissant les variables d'environnement suivantes àSbomgen.

```
AWS_ACCESS_KEY_ID=$access_key \
AWS_SECRET_ACCESS_KEY=$secret_key \
```

```
AWS_DEFAULT_REGION=$region \
./inspector-sbomgen arguments
```

Pour spécifier le format de réponse, utilisez l'`--scan-sbom-output-format cyclonedx`argument ou l'`--scan-sbom-output-format inspector`argument.

Exemple de commande 1

Cette commande crée une SBOM pour la dernière Alpine Linux version, analyse la SBOM et écrit les résultats de la vulnérabilité dans un fichier JSON.

```
./inspector-sbomgen container --image alpine:latest \
                          --scan-sbom \
                          --aws-profile your_profile \
                          --aws-region your_region \
                          --scan-sbom-output-format cyclonedx \
                          --outfile /tmp/inspector_scan.json
```

Exemple de commande 2

Cette commande s'authentifie auprès d'Amazon Inspector en utilisant les AWS informations d'identification comme variables d'environnement.

```
AWS_ACCESS_KEY_ID=$your_access_key \
AWS_SECRET_ACCESS_KEY=$your_secret_key \
AWS_DEFAULT_REGION=$your_region \
./inspector-sbomgen container --image alpine:latest \
                          -o /tmp/sbom.json \
                          --scan-sbom \
                          --scan-sbom-output-format inspector
```

Exemple de commande 3

Cette commande s'authentifie auprès d'Amazon Inspector à l'aide de l'ARN d'un rôle IAM.

```
./inspector-sbomgen container --image alpine:latest \
                          --scan-sbom \
                          --aws-profile your_profile \
                          --aws-region your_region \
                          --outfile /tmp/inspector_scan.json
```

```
                        --aws-iam-role-arn arn:aws:iam::123456789012:role/your_role
```

## Utiliser des scanners supplémentaires pour améliorer les capacités de détection

Le générateur Amazon Inspector SBOM applique des scanners prédéfinis en fonction de la commande utilisée.

Groupes de scanners par défaut

Chaque sous-commande Amazon Inspector SBOM Generator applique automatiquement les groupes de scanners par défaut suivants.

- Pour la `directory` sous-commande : binary programming-language-packages, dockerfile scanner groups
- Pour la `localhost` sous-commande : os programming-language-packages, extra-ecosystems scanner groups
- Pour la `container` sous-commande : os, extra-ecosystems programming-language-packages, dockerfile, groupes de scanners binaires

Scanners spéciaux

Pour inclure des scanners autres que les groupes de scanners par défaut, utilisez l'`--additional-scanners`option suivie du nom du scanner à ajouter. Voici un exemple de commande qui montre comment procéder.

```
# Add WordPress installation scanner to directory scan
./inspector-sbomgen directory --path /path/to/directory/ --additional-scanners
 wordpress-installation -o output.jso
```

Voici un exemple de commande qui montre comment ajouter plusieurs scanners avec une liste séparée par des virgules.

```
./inspector-sbomgen container --image image:tag --additional-scanners scanner1,scanner2
 -o output.json
```

## Personnalisez les scans pour exclure des fichiers spécifiques

Lors de l'analyse et du traitement d'une image de conteneur, Sbomgen scanne la taille de tous les fichiers de cette image de conteneur. Vous pouvez personnaliser les analyses pour exclure des fichiers spécifiques ou cibler des packages spécifiques.

Pour réduire la consommation de disque, la consommation de RAM, le temps d'exécution écoulé et ignorer les fichiers qui dépassent le seuil indiqué, utilisez l'`--max-file-size`argument associé à la sous-commande : `container`

```
./inspector-sbomgen container --image alpine:latest \
--outfile /tmp/sbom.json \
--max-file-size 300000000
```

## Désactiver l'indicateur de progression

Sbomgenaffiche un indicateur de progression de rotation qui peut entraîner l'apparition de barres obliques excessives dans les environnements CI/CD.

```
INFO[2024-02-01 14:58:46]coreV1.go:53: analyzing artifact
|
\
/
|
\
/
INFO[2024-02-01 14:58:46]coreV1.go:62: executing post-processors
```

Vous pouvez désactiver l'indicateur de progression à l'aide de l'`--disable-progress-bar`argument :

```
./inspector-sbomgen container --image alpine:latest \
--outfile /tmp/sbom.json \
--disable-progress-bar
```

# Authentification auprès de registres privés avec Sbomgen

En fournissant les informations d'authentification de votre registre privé, vous pouvez générer des données SBOMs à partir de conteneurs hébergés dans des registres privés. Vous pouvez fournir ces informations d'identification par les méthodes suivantes :

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

Pour cette méthode, vous devez vous authentifier auprès de votre registre de conteneurs. Par exemple, si vous utilisezDocker, vous pouvez vous authentifier auprès de votre registre de conteneurs à l'aide de la commande de Docker journalisation :. `docker login`

1. Authentifiez-vous 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 :
2. Après vous être authentifié auprès de votre registre de conteneurs, utilisez-le Sbomgen sur une image de conteneur qui se trouve dans le registre. Pour utiliser l'exemple suivant, remplacez-le *`image:tag`* par le nom de l'image à numériser :

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

## Authentifiez-vous à l'aide de la méthode interactive

Pour cette méthode, entrez votre nom d'utilisateur comme 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 que vous souhaitez numériser et *`your_username`* par un nom d'utilisateur ayant accès à l'image :

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

## Authentifier à l'aide de la méthode non interactive

Pour cette méthode, enregistrez votre mot de passe ou votre jeton de registre dans un `.txt` fichier.

> **Note**
>
> L'utilisateur actuel ne devrait pouvoir lire que ce fichier. Le fichier doit également contenir 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, *password.txt* par le `.txt` fichier contenant votre mot de passe ou votre jeton sur une seule ligne et *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"
        }
      ]
    }
  ]
}
```


# Versions précédentes du générateur Amazon Inspector SBOM

Cette rubrique fournit des liens vers les versions les plus récentes et précédentes d'Amazon Inspector SBOM Generator. Pour plus d'informations sur l'installation de Sbomgen, consultez Installation de Sbomgen.

Dernière version

- https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip
- https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip

Sbomgen1.7.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.3

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.3/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.3/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.2

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.2/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.2/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.1

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.1/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.5

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.5/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.5/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.4

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.4/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.4/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.3

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.3/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.3/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.2

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.2/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.2/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.1

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.1/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.4.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.4.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.4.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.3.2

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.2/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.2/linux/arm64/inspector-sbomgen.zip

Sbomgen1.3.1

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.1/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.3.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.2.1

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.1/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.2.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.1.1

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.1/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.1/linux/arm64/inspector-sbomgen.zip

Sbomgen 1.1.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.0.0

- Linux AMD64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.0.0/linux/amd64/inspector-sbomgen.zip
- Linux ARM64 : https://amazon-inspector-sbomgen.s3.amazonaws.com/1.0.0/linux/arm64/inspector-sbomgen.zip

# Collection complète de systèmes d'exploitation Amazon Inspector SBOM Generator

Le générateur Amazon Inspector SBOM analyse différents systèmes d'exploitation pour garantir une analyse robuste et détaillée des composants du système. La génération d'une SBOM vous aide à comprendre la composition de votre système d'exploitation, afin d'identifier les vulnérabilités des packages gérés par le système. Cette rubrique décrit les principales fonctionnalités des différentes collections de packages de systèmes d'exploitation prises en charge par Amazon Inspector SBOM Generator. Pour plus d'informations sur les systèmes d'exploitation pris en charge par Amazon Inspector, consultez Systèmes d'exploitation et langages de programmation pris en charge par Amazon Inspector.

## Artefacts du système d'exploitation supportés

Le générateur Amazon Inspector SBOM prend en charge les artefacts du système d'exploitation suivants :

| Plateforme | Binaire | Source | Flux |
|---|---|---|---|
| Alma Linux | N/A | Oui | Oui |
| Alpine Linux | Oui | Oui | N/A |
| Amazon Linux | N/A | Oui | N/A |
| CentOS | N/A | Oui | N/A |
| Chainguard | Oui | Oui | N/A |
| Debian | Oui | Oui | N/A |
| Distroless | Oui | Oui | N/A |
| Fedora | N/A | Oui | N/A |
| OpenSUSE | N/A | Oui | N/A |
| Oracle Linux | N/A | Oui | N/A |

| Plateforme | Binaire | Source | Flux |
|---|---|---|---|
| Photon OS | N/A | Oui | N/A |
| RHEL | N/A | Oui | Oui |
| Rocky Linux | N/A | Oui | Oui |
| SLES | N/A | Oui | N/A |
| Ubuntu | Oui | Oui | N/A |

## Collection de packages de systèmes d'exploitation basés sur APK

Cette section inclut les plateformes prises en charge et les principales fonctionnalités de la collection de packages de systèmes APK d'exploitation basés sur le système d'exploitation. Pour plus d'informations, consultez Alpine Package Keeper sur le Alpine Linux site Web.

### Plateformes prises en charge

Les plateformes suivantes sont prises en charge.

- Alpine Linux

> **Note**
>
> Pour les systèmes APK basés, le générateur Amazon Inspector SBOM collecte les métadonnées du package à partir du `/lib/apk/db/`fichier.

### Fonctions principales

- Collection de noms de packages : extrait le nom de chaque package installé
- Collection de versions — Extrait la version de chaque package installé
- Identification du package source — Identifie le package source pour chaque package installé

### exemple

L'extrait suivant est un exemple de fichier de APK base de données.

```
C:Q1JlboSJkrN4qkDcokr4zenpcWEXQ=
P:zlib
V:1.2.13-r1
A:x86_64
S:54253
I:110592
T:A compression/decompression Library
U:https://zlib.net/
L:Zlib
o:zlib
```

## Collection de packages de systèmes d'exploitation basés sur DPKG

Cette section inclut les plateformes prises en charge et les principales fonctionnalités de la collection de packages de systèmes DPKG d'exploitation basés sur le système d'exploitation. Pour plus d'informations, consultez le Package Debian sur le Debian site Web.

### Plateformes prises en charge

Les plateformes suivantes sont prises en charge.

- Debian
- Ubuntu

> **Note**
>
> Pour les systèmes DPKG basés, le générateur Amazon Inspector SBOM collecte les métadonnées du package à partir du `/var/lib/dpkg/status`fichier.

### Fonctions principales

Les principales fonctionnalités des packages de systèmes d'exploitation DPKG basés sur les systèmes d'exploitation sont les suivantes.

- Collection de noms de packages : extrait le nom de chaque package installé
- Collection de versions — Extrait la version de chaque package installé
- Identification du package source — Identifie le package source pour chaque package installé

### exemple

L'extrait de code suivant est un exemple de fichier. `/var/lib/dpkg/`

```
Package: zlib1g
Status: install ok installed
Priority: optional
Section: libs
Installed-Size: 168
Maintainer: Mark Brown <broonie@debian.org>
Architecture: amd64
Multi-Arch: same
Source: zlib
Version: 1:1.2.13.dfsg-1
Provides: libz1
Depends: libc6 (>= 2.14)
Breaks: libxml2 (<< 2.7.6.dfsg-2), texlive-binaries (<< 2009-12)
Conflicts: zlib1 (<= 1:1.0.4-7)
Description: compression library - runtime
 zlib is a library implementing the deflate compression method found
 in gzip and PKZIP.  This package includes the shared library.
Homepage: http://zlib.net/
```

## Collection de packages de systèmes d'exploitation basés sur le RPM

Cette section inclut les plateformes prises en charge et les principales fonctionnalités de la collection de packages de systèmes RPM d'exploitation basés sur le système d'exploitation. Pour plus d'informations, consultez la section RPM Package Manager sur le RPM site Web.

### Plateformes prises en charge

Les plateformes suivantes sont prises en charge.

- Alma Linux

- Amazon Linux
- CentOS
- Fedora
- OpenSUSE
- Oracle Linux
- PhotonOS
- RedHat Enterprise Linux
- Rocky Linux
- SUSE Linux Enterprise Server

> **Note**
>
> Pour les systèmes RPM basés, le générateur Amazon Inspector SBOM collecte les métadonnées du package à partir du `/var/lib/rpm`fichier.

## Fonctions principales

Les principales fonctionnalités des collections de packages de systèmes d'exploitation RPM basés sur les systèmes d'exploitation sont les suivantes.

- Collection de noms de packages : extrait le nom de chaque package installé
- Collection de versions — Extrait la version de chaque package installé
- Identification du package source — Identifie le package source pour chaque package installé
- Support des flux : extrait les métadonnées des flux de chaque package installé

## exemple

Voici un exemple d'extrait de fichier de RPM base de données.

```
/usr/lib/sysimage/rpm/rpmdb.sqlite
/usr/lib/sysimage/rpm/Packages
/usr/lib/sysimage/rpm/Packages.db
/var/lib/rpm/rpmdb.sqlite
```

```
/var/lib/rpm/Packages
/var/lib/rpm/Packages.db
```

## Collection de packages d'images Chainguard

Cette section inclut les plateformes prises en charge et les fonctionnalités clés pour la collecte de packages Chainguard d'images. Pour plus d'informations, voir Images sur le Chainguard site Web.

### Plateformes prises en charge

Les plateformes suivantes sont prises en charge

- Wolfi Linux

> **Note**
>
> Pour les Chainguard images, le générateur Amazon Inspector SBOM collecte les métadonnées du package à partir du `/lib/apk/db/installed` fichier.

### Fonctions principales

Les principales fonctionnalités sont les suivantes.

- Collection de noms de packages : extrait le nom de chaque package installé
- Collection de versions — Extrait la version de chaque package installé
- Identification du package source — Identifie le package source pour chaque package installé

### exemple

L'extrait suivant est un exemple de fichier Chainguard image.

```
P:wolfi-keys
V:1-r8
A:x86_64
L:MIT
```

```
T:Wolfi signing keyring
o:wolfi-keys
```

## Collection de packages d'images sans distribution

Distrolessles conteneurs sont des images de conteneurs qui excluent les gestionnaires de packages, les shells et les autres utilitaires des Linux distributions. Distrolessles conteneurs incluent uniquement les dépendances essentielles requises pour exécuter l'application et améliorer les performances et la sécurité.

> **Note**
>
> Pour les Distrolessimages, le générateur Amazon Inspector SBOM collecte les métadonnées du package à partir du `/var/lib/dpkg/status.d` fichier. Seules Debian les distributions Ubuntu basées sur et basées sont prises en charge. Ils peuvent être identifiés par le `NAME` champ du système de `/etc/os-release` fichiers, qui indique « Debian » ou « »Ubuntu.

### Fonctions principales

- Collection de noms de packages : extrait le nom de chaque package installé
- Collection de versions — Extrait la version de chaque package installé

### exemple

Voici un exemple de fichier Distroless image.

```
Package: tzdata
Version: 2021a-1+deb11u10
Architecture: all
Maintainer: GNU Libc Maintainers <debian-glibc@lists.debian.org>
Installed-Size: 3413
Depends: debconf (>= 0.5) | debconf-2.0
Provides: tzdata-bullseye
Section: localization
Priority: required
Multi-Arch: foreign
Homepage: https://www.iana.org/time-zones
```

```
Description: time zone and daylight-saving time data
 This package contains data required for the implementation of
 standard local time for many representative locations around the
 globe. It is updated periodically to reflect changes made by
 political bodies to time zone boundaries, UTC offsets, and
 daylight-saving rules.
```

# Collection de dépendances des langages de programmation

Le générateur Amazon Inspector SBOM prend en charge différents langages de programmation et frameworks, qui constituent un ensemble robuste et détaillé de dépendances. La génération d'une SBOM vous aide à comprendre la composition de votre logiciel, afin d'identifier les vulnérabilités et de garantir la conformité aux normes de sécurité. Le générateur SBOM d'Amazon Inspector prend en charge les langages de programmation et formats de fichiers suivants.

## Analyser les dépendances

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| Go | Go | `go.mod` | N/A | N/A | N/A | N/A | Oui |
| | | `go.sum` | N/A | N/A | N/A | N/A | Oui |
| | | Go Binaries | Oui | N/A | N/A | N/A | Oui |
| | | `GOMODCACHE` | N/A | N/A | N/A | N/A | Non |

### go.mod/go.sum

Utilisez `go.mod` des `go.sum` fichiers et pour définir et verrouiller les dépendances dans les Go projets. Le générateur Amazon Inspector SBOM gère ces fichiers différemment en fonction de la version de la chaîne Go d'outils.

Fonctions principales

- Collecte les dépendances depuis `go.mod` (si la version de la Go chaîne d'outils est 1.17 ou supérieure)
- Collecte les dépendances depuis `go.sum` (si la version de la Go chaîne d'outils est 1.17 ou inférieure)
- Analyses `go.mod` pour identifier toutes les dépendances déclarées et les versions de dépendance

Exemple de fichier **`go.mod`**

Voici un exemple de `go.mod` fichier.

```
module example.com/project

go 1.17

require (
github.com/gin-gonic/gin v1.7.2
golang.org/x/crypto v0.0.0-20210616213533-5cf6c0f8e123
)
```

Exemple de fichier **`go.sum`**

Voici un exemple de `go.sum` fichier.

```
github.com/gin-gonic/gin v1.7.2 h1:VZ7DdRl0sghbA6lVGSkX+UXO2+J0aH7RbsNugG+FA8Q=
github.com/gin-gonic/gin v1.7.2/go.mod h1:ILZ1Ngh2f1pL1ASUj7gGk8lGFeNC8cRTaN2ZhsBNbXU=
golang.org/x/crypto v0.0.0-20210616213533-5cf6c0f8e123 h1:b6rCu+qHze
+BUsmC3CZzH8aNu8LzPZTVsNTo64OypSc=
golang.org/x/crypto v0.0.0-20210616213533-5cf6c0f8e123/go.mod h1:K5Dkpb0Q4ewZW/
EzWlQphgJcUMBCzoWrLfDOVzpTGVQ=
```

> **Note**
>
> Chacun de ces fichiers produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une

nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Binaires Go

Le générateur Amazon Inspector SBOM extrait les dépendances Go des fichiers binaires compilés pour garantir le code utilisé.

> **Note**
>
> Le générateur Amazon Inspector SBOM permet de capturer et d'évaluer les versions de la chaîne d'outils à partir de Go fichiers binaires créés à l'aide du compilateur officiel. Go Pour plus d'informations, consultez la section Téléchargement et installation sur le Go site Web. Si vous utilisez la Go chaîne d'outils d'un autre fournisseur, par exempleRed Hat, l'évaluation peut ne pas être précise en raison de différences potentielles dans la distribution et la disponibilité des métadonnées.

### Fonctions principales

- Extrait les informations de dépendance directement à partir des Go fichiers binaires
- Collecte les dépendances intégrées dans le binaire
- Détecte et extrait la version de la Go chaîne d'outils utilisée pour compiler le binaire.

## GOMODCACHE

Le générateur Amazon Inspector SBOM analyse le cache du Go module pour collecter des informations sur les dépendances installées. Ce cache stocke les modules téléchargés pour s'assurer que les mêmes versions sont utilisées dans les différentes versions.

### Fonctions principales

- Analyse le `GOMODCACHE` répertoire pour identifier les modules mis en cache
- Extrait les métadonnées détaillées, y compris les noms des modules, les versions et les sources URLs

### Exemple de structure

Voici un exemple de `GOMODCACHE` structure.

```
~/go/pkg/mod/
### github.com/gin-gonic/gin@v1.7.2
### golang.org/x/crypto@v0.0.0-20210616213533-5cf6c0f8e123
```

> **Note**
>
> Cette structure produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Analyse des dépendances Java

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| `Java` | `Maven` | JavaApplications compilées (.jar/.war/.ear)<br><br>`pom.xml` | N/A<br><br>N/A | N/A<br><br>N/A | Oui<br><br>Oui | N/A<br><br>N/A | Oui<br><br>Oui |

Le générateur Amazon Inspector SBOM effectue une analyse des Java dépendances en analysant les Java applications et `pom.xml` les fichiers compilés. Lors de l'analyse d'applications compilées, le scanner génère des hachages SHA-1 pour vérifier l'intégrité, extrait `pom.properties` les fichiers intégrés et analyse les fichiers imbriqués. `pom.xml`

## collection de hachage SHA-1 (pour les fichiers .jar, .war, .ear compilés)

Le générateur Amazon Inspector SBOM essaie de collecter les hachages SHA-1 pour tous `.ear.jar`, ainsi que les `.war` fichiers d'un projet afin de garantir l'intégrité et la traçabilité des artefacts compilés. Java

### Fonctions principales

- Génère des hachages SHA-1 pour tous les artefacts compilés Java

### Exemple d'artefact

Voici un exemple d'artefact SHA-1.

```
{
  "bom-ref": "comp-52",
  "type": "library",
  "name": "jul-to-slf4j",
  "version": "2.0.6",
  "hashes": [
    {
      "alg": "SHA-1",
      "content": ""
    }
  ],
  "purl": "pkg:maven/jul-to-slf4j@2.0.6",
  "properties": [
    {
      "name": "amazon:inspector:sbom_generator:source_path",
      "value": "test-0.0.1-SNAPSHOT.jar/BOOT-INF/lib/jul-to-slf4j-2.0.6.jar"
    }
  ]
}
```

> **Note**
>
> Cet artefact produit une sortie contenant l'URL d'un package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature

logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## pom.properties

Le `pom.properties` fichier est utilisé dans les Maven projets pour stocker les métadonnées du projet, notamment les noms et les versions des packages. Le générateur Amazon Inspector SBOM analyse ce fichier pour collecter des informations sur le projet.

Fonctions principales

- Analyse et extrait les artefacts, les groupes de packages et les versions des packages

### Exemple de fichier **`pom.properties`**

Voici un exemple de fichier `pom.properties`.

```
#Generated by Maven
#Tue Mar 16 15:44:02 UTC 2021

version=1.6.0
groupId=net.datafaker
artifactId=datafaker
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

### À l'exclusion de l'analyse imbriquée **`pom.xml`**

Si vous souhaitez exclure l'analyse `pom.xml` syntaxique lors de l'analyse d'Javaapplications compilées, utilisez l'`--skip-nested-pomxml`argument.

## pom.xml

Le `pom.xml` fichier est le fichier de configuration de base pour les Maven projets. Il contient des informations sur les projets et leurs dépendances. Le générateur Amazon Inspector SBOM analyse les pom.xml fichiers pour collecter les dépendances, en analysant les fichiers autonomes dans les référentiels et les fichiers contenus dans les fichiers compilés. .jar

### Fonctions principales

- Analyse et extrait les artefacts de packages, les groupes de packages et les versions de packages à partir de `pom.xml` fichiers.

### Étendue et Maven tags pris en charge

Les dépendances sont collectées avec les Maven étendues suivantes :

- compile
- fourni
- environnement d'exécution
- test
- system
- importation

Les dépendances sont collectées avec la Maven balise suivante :`<optional>true</optional>`.

### Exemple de **`pom.xml`** fichier avec une portée

Voici un exemple de `pom.xml` fichier doté d'une portée.

```
<dependency>
<groupId>jakarta.servlet</groupId>
<artifactId>jakarta.servlet-api</artifactId>
</version>6.0.0</version>
<scope>provided</scope>
</dependency>
<dependency>
<groupId>mysql</groupId>
```

```
<artifactId>mysql-connector-java</artifactId>
<version>8.0.28</version>
<scope>runtime</scope>
</dependency>
```

### Exemple **pom.xml** de fichier sans portée

Voici un exemple de `pom.xml` fichier sans portée.

```
<dependency>
<groupId>com.fasterxml.jackson.core</groupId>
<artifactId>jackson-databind</artifactId>
<version>2.17.1</version>
</dependency>

<dependency>
<groupId>org.jenkins-ci.plugins</groupId>
<artifactId>plain-credentials</artifactId>
<version>183.va_de8f1dd5a_2b_</version>
</dependency>

<dependency>
<groupId>org.jenkins-ci.plugins</groupId>
<artifactId>jackson2-api</artifactId>
<version>2.15.2-350.v0c2f3f8fc595</version>
</dependency>
```

> **Note**
>
> Chacun de ces fichiers produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

# JavaScript analyse des dépendances

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| `Javascript` | `Node Modules` | `node_modules/*/package.json` | N/A | N/A | Oui | Oui | Oui |
| | `NPM` | | N/A | Oui | N/A | N/A | Non |
| | `PNPM` | | N/A | Oui | N/A | N/A | Non |
| | `YARN` | | N/A | Oui | N/A | N/A | Non |
| | | `package-lock.json (v1, v2, and v3) / npm-shrinkwrap.json` | | | | | |
| | | `pnpm-lock.yaml` | | | | | |
| | | `yarn.lock` | | | | | |

## package.json

Le `package.json` fichier est un élément essentiel des Node.js projets. Il contient des métadonnées sur les packages installés. Le générateur SBOM d'Amazon Inspector analyse ce fichier pour identifier les noms et les versions des packages.

Fonctions principales

- Analyse la structure du fichier JSON pour extraire les noms et les versions des packages
- Identifie les packages privés avec des valeurs privées

### Exemple de fichier **`package.json`**

Voici un exemple de fichier `package.json`.

```
{
"name": "arrify",
"private": true,
"version": "2.0.1",
"description": "Convert a value to an array",
"license": "MIT",
"repository": "sindresorhus/arrify"
}
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## package-lock.json

Le `package-lock.json` fichier est automatiquement généré par npm pour verrouiller les versions exactes des dépendances installées pour un projet. Il garantit la cohérence des environnements en stockant les versions exactes de toutes les dépendances et de leurs sous-dépendances. Ce fichier permet de faire la distinction entre les dépendances classiques et les dépendances de développement.

Fonctions principales

- Analyse la structure du fichier JSON pour extraire les noms et les versions des packages
- Supporte la détection des dépendances des développeurs

### Exemple de fichier **`package-lock.json`**

Voici un exemple de fichier `package-lock.json`.

```
"verror": {
"version": "1.10.0",
"resolved": "https://registry.npmjs.org/verror/-/verror-1.10.0.tgz",
"integrity": "sha1-OhBcoXBTr1XW4nDB+CiGguGNpAA=",
"requires": {
    "assert-plus": "^1.0.0",
    "core-util-is": "1.0.2",
    "extsprintf": "^1.2.0"
}
},
"wrappy": {
"version": "1.0.2",
"resolved": "https://registry.npmjs.org/wrappy/-/wrappy-1.0.2.tgz",
"integrity": "sha1-tSQ9jz7BqjXxNkYFvA0QNuMKtp8=",
"dev": true
},
"yallist": {
"version": "3.0.2",
"resolved": "https://registry.npmjs.org/yallist/-/yallist-3.0.2.tgz",
"integrity": "sha1-hFK0u36Dx8GI2AQcGoN8dz1ti7k="
}
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## npm-shrinkwrap.json

npmgénère automatiquement `package-lock.json` des `npm-shrinkwrap.json` fichiers pour verrouiller les versions exactes des dépendances installées pour un projet. Cela garantit la cohérence des environnements en stockant les versions exactes de toutes les dépendances et sous-

dépendances. Les fichiers font la distinction entre les dépendances classiques et les dépendances de développement.

Fonctions principales

- Analyser `package-lock` les versions 1, 2 et 3 de la structure du JSON fichier pour extraire le nom et la version du package
- La détection des dépendances des développeurs est prise en charge (`package-lock.json`oncapture les dépendances de production et de développement, permettant aux outils d'identifier les packages utilisés dans les environnements de développement)
- Le `npm-shrinkwrap.json` fichier est prioritaire par rapport au `package-lock.json` fichier

exemple

Voici un exemple de fichier `package-lock.json`.

```
"verror": {
            "version": "1.10.0",
            "resolved": "https://registry.npmjs.org/verror/-/verror-1.10.0.tgz",
            "integrity": "sha1-OhBcoXBTr1XW4nDB+CiGguGNpAA=",
            "requires": {
                "assert-plus": "^1.0.0",
                "core-util-is": "1.0.2",
                "extsprintf": "^1.2.0"
            }
        },
        "wrappy": {
            "version": "1.0.2",
            "resolved": "https://registry.npmjs.org/wrappy/-/wrappy-1.0.2.tgz",
            "integrity": "sha1-tSQ9jz7BqjXxNkYFvA0QNuMKtp8=",
            "dev": true
        },
        "yallist": {
            "version": "3.0.2",
            "resolved": "https://registry.npmjs.org/yallist/-/yallist-3.0.2.tgz",
            "integrity": "sha1-hFK0u36Dx8GI2AQcGoN8dz1ti7k="
}
```

## pnpm-yaml.lock

Le `pnpm-lock.yaml` fichier est généré par pnpm pour conserver un enregistrement des versions de dépendance installées. Il suit également les dépendances de développement séparément.

### Fonctions principales

- Analyse la structure du fichier YAML pour extraire les noms et les versions des packages
- Supporte la détection des dépendances des développeurs

### exemple

Voici un exemple de fichier `pnpm-lock.yaml`.

```
lockfileVersion: 5.3
importers:
my-project:
dependencies:
  lodash: 4.17.21
devDependencies:
  jest: 26.6.3
specifiers:
  lodash: ^4.17.21
  jest: ^26.6.3
packages:
/lodash/4.17.21:
resolution:
  integrity: sha512-xyz
engines:
  node: '>=6'
dev: false
/jest/26.6.3:
resolution:
  integrity: sha512-xyz
dev: true
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## yarn.lock

Le générateur Amazon Inspector SBOM essaie de collecter les hachages SHA-1 pour `.ear.jar`, et les `.war` fichiers d'un projet afin de garantir l'intégrité et la traçabilité des artefacts compilés. Java

### Fonctions principales

- Génère des hachages SHA-1 pour tous les artefacts compilés Java

### Exemple d'artefact SHA-1

Voici un exemple d'artefact SHA-1.

```
"@ampproject/remapping@npm:^2.2.0":
version: 2.2.0
resolution: "@ampproject/remapping@npm:2.2.0"
dependencies:
"@jridgewell/gen-mapping": ^0.1.0
"@jridgewell/trace-mapping": ^0.3.9
checksum:
 d74d170d06468913921d72430259424b7e4c826b5a7d39ff839a29d547efb97dc577caa8ba3fb5cf023624e9af9d09
languageName: node
linkType: hard

"@babel/code-frame@npm:^7.0.0, @babel/code-frame@npm:^7.12.13, @babel/code-
frame@npm:^7.18.6, @babel/code-frame@npm:^7.21.4":
version: 7.21.4
resolution: "@babel/code-frame@npm:7.21.4"
dependencies:
"@babel/highlight": ^7.18.6
checksum:
 e5390e6ec1ac58dcef01d4f18eaf1fd2f1325528661ff6d4a5de8979588b9f5a8e852a54a91b923846f7a5c681b217
```

```
languageName: node
linkType: hard
```

> **Note**
>
> Cet artefact produit une sortie contenant l'URL d'un package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Analyse des dépendances .NET

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| `.NET` | `.NET Core` | `*.deps.json` | N/A | N/A | N/A | N/A | Oui |
| | `Nuget` | `Packages.config` | N/A | N/A | N/A | N/A | Oui |
| | `Nuget` | `packages.lock.json` | N/A | N/A | Oui | N/A | Oui |
| | `.NET` | `.csproj` | N/A | N/A | N/A | N/A | Oui |

### Packages.config

Le `Packages.config` fichier est un fichier XML utilisé par une ancienne version de Nuget pour gérer les dépendances du projet. Il répertorie tous les packages référencés par le projet, y compris les versions spécifiques.

Fonctions principales

- Analyse la structure XML pour extraire le package IDs et les versions

exemple

Voici un exemple de fichier `Packages.config`.

```
<?xml version="1.0" encoding="utf-8"? >
<packages>
<package id="FluentAssertions" version="5.4.1" targetFramework="net461" />
<package id="Newtonsoft.Json" version="11.0.2" targetFramework="net461" />
<package id="SpecFlow" version="2.4.0" targetFramework="net461" />
<package id="SpecRun.Runner" version="1.8.0" targetFramework="net461" />
<package id="SpecRun.SpecFlow" version="1.8.0" targetFramework="net461" />
<package id="SpecRun.SpecFlow.2-4-0" version="1.8.0" targetFramework="net461" />
<package id="System.ValueTuple" version="4.5.0" targetFramework="net461" />
</packages>
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## *.deps.json

Le `*.deps.json` fichier est généré par les .NET Core projets et contient des informations détaillées sur toutes les dépendances, notamment les chemins, les versions et les dépendances d'exécution. Ce fichier garantit que le moteur d'exécution dispose des informations nécessaires pour charger les versions correctes des dépendances.

Fonctions principales

- Analyse la structure JSON pour obtenir des détails complets sur les dépendances
- Extrait les noms et les versions des packages dans une `libraries` liste.

### Exemple de fichier **`.deps.json`**

Voici un exemple de fichier `.deps.json`.

```
{
"runtimeTarget": {
    "name": ".NETCoreApp,Version=v7.0",
    "signature": ""
},
"libraries": {
    "sample-Nuget/1.0.0": {
        "type": "project",
        "serviceable": false,
        "sha512": ""
    },
    "Microsoft.EntityFrameworkCore/7.0.5": {
        "type": "package",
        "serviceable": true,
        "sha512": "sha512-
RXbRLHHWP2Z3pq8qcL5nQ6LPeoOyp8hasM5bd0Te8PiQi3RjWQR4tcbdY5XMqQ+oTO9wA8/RLhZRn/
hnxlTDnQ==",
        "path": "microsoft.entityframeworkcore/7.0.5",
        "hashPath": "microsoft.entityframeworkcore.7.0.5.nupkg.sha512"
    },
}
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## packages.lock.json

Le `packages.lock.json` fichier est utilisé par les nouvelles versions de Nuget pour verrouiller les versions exactes des dépendances d'un .NET projet afin de garantir que les mêmes versions sont utilisées de manière cohérente dans différents environnements.

Fonctions principales

- Analyse la structure JSON pour répertorier les dépendances verrouillées
- Supporte les dépendances directes et transitives
- Extrait le nom du package et les versions résolues

### Exemple de fichier **`packages.lock.json`**

Voici un exemple de fichier `packages.lock.json`.

```
{
"version": 1,
"dependencies": {
"net7.0": {
  "Microsoft.EntityFrameworkCore": {
    "type": "Direct",
    "requested": "[7.0.5, )",
    "resolved": "7.0.5",
    "contentHash": "RXbRLHHWP2Z3pq8qcL5nQ6LPeoOyp8hasM5bd0Te8PiQi3RjWQR4tcbdY5XMqQ
+oTO9wA8/RLhZRn/hnxlTDnQ==",
    "dependencies": {
      "Microsoft.EntityFrameworkCore.Abstractions": "7.0.5",
      "Microsoft.EntityFrameworkCore.Analyzers": "7.0.5",
      "Microsoft.Extensions.Caching.Memory": "7.0.0",
      "Microsoft.Extensions.DependencyInjection": "7.0.0",
      "Microsoft.Extensions.Logging": "7.0.0"
    }
  },
  "Newtonsoft.Json": {
    "type": "Direct",
    "requested": "[13.0.3, )",
    "resolved": "13.0.3",
    "contentHash": "HrC5BXdl00IP9zeV+0Z848QWPAoCr9P3bDEZguI+gkLcBKAOxix/tLEAAHC
+UvDNPv4a2d18lOReHMOagPa+zQ=="
  },
  "Microsoft.Extensions.Primitives": {
    "type": "Transitive",
    "resolved": "7.0.0",
    "contentHash": "um1KU5kxcRp3CNuI8o/GrZtD4AIOXDk
+RLsytjZ9QPok3ttLUelLKpilVPuaFT3TFjOhSibUAso0odbOaCDj3Q=="
  }
```

```
}
}
}
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

### .csproj

Le `.csproj` fichier est écrit en XML et le fichier de projet pour les .NET projets. Il inclut des références aux Nuget packages, aux propriétés du projet et aux configurations de construction.

Fonctions principales

- Analyse le XML de la structure pour extraire les références des packages

#### Exemple de fichier **`.csproj`**

Voici un exemple de fichier `.csproj`.

```
<Project Sdk="Microsoft.NET.Sdk">
<PropertyGroup>
<TargetFramework>net7.0</TargetFramework>
<RootNamespace>sample_Nuget</RootNamespace>
<ImplicitUsings>enable</ImplicitUsings>
<Nullable>enable</Nullable>
<RestorePackagesWithLockFile>true</RestorePackagesWithLockFile>
</PropertyGroup>
<ItemGroup>
</ItemGroup>
<ItemGroup>
<PackageReference Include="Newtonsoft.Json" Version="13.0.3" />
<PackageReference Include="Microsoft.EntityFrameworkCore" Version="7.0.5" />
</ItemGroup>
```

```
</Project>
```

### Exemple de fichier `.csproj`

Voici un exemple de fichier `.csproj`.

```
<PackageReference Include="ExamplePackage" Version="6.*" />
<PackageReferencePackageReference Include="ExamplePackage" Version="(4.1.3,)" />
<PackageReference Include="ExamplePackage" Version="(,5.0)" />
<PackageReference Include="ExamplePackage" Version="[1,3)" />
<PackageReference Include="ExamplePackage" Version="[1.3.2,1.5)" />
```

> **Note**
>
> Chacun de ces fichiers produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Analyse des dépendances PHP

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| PHP | `Composer` | `composer.lock` | N/A | N/A | Oui | N/A | Oui |
| | | `/vendor/composer/i` | N/A | N/A | Oui | N/A | Oui |

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| | | `nstalled.json` | | | | | |

## composer.lock

Le `composer.lock` fichier est automatiquement généré lors de l'exécution des commandes d'installation ou de mise à jour du compositeur. Ce fichier garantit que les mêmes versions des dépendances sont installées dans tous les environnements. Cela fournit un processus de construction cohérent et fiable.

Fonctions principales

- Analyse le format JSON pour les données structurées
- Extrait les noms et les versions des dépendances

### Exemple de fichier **`composer.lock`**

Voici un exemple de fichier `composer.lock`.

```
{
"packages": [
    {
        "name": "nesbot/carbon",
        "version": "2.53.1",
        // TRUNCATED
    },
    {
        "name": "symfony/deprecation-contracts",
        "version": "v3.2.1",
        // TRUNCATED
    },
    {
        "name": "symfony/polyfill-mbstring",
        "version": "v1.27.0",
```

```
        // TRUNCATED
    }
]
// TRUNCATED
}
```

> **Note**
>
> Cela produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## /vendor/composer/installed.json

Le `/vendor/composer/installed.json` fichier se trouve dans le `vendor/composer` répertoire et fournit une liste complète de tous les packages installés et de toutes les versions de packages.

Fonctions principales

- Analyse le format JSON pour les données structurées
- Extrait les noms et les versions des dépendances

### Exemple de fichier **`/vendor/composer/installed.json`**

Voici un exemple de fichier `/vendor/composer/installed.json`.

```
{
"packages": [
    {
        "name": "nesbot/carbon",
        "version": "2.53.1",
        // TRUNCATED
    },
    {
        "name": "symfony/deprecation-contracts",
        "version": "v3.2.1",
        // TRUNCATED
```

```
    },
    {
        "name": "symfony/polyfill-mbstring",
        "version": "v1.27.0",
        // TRUNCATED
    }
]
// TRUNCATED
}
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Analyse des dépendances en Python

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| Python | pip | requirements.txt | N/A | N/A | N/A | N/A | Oui |
| | Poetry | Poetry.lock | N/A | N/A | N/A | N/A | Oui |
| | Pipenv | Pipfile.lock | N/A | N/A | N/A | N/A | Oui |
| | Egg/Wheel | .egg-info/PKG-INFO | N/A | N/A | N/A | N/A | Oui |

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| | | `.dist-info/METADATA` | | | | | |

## requirements.txt

Le `requirements.txt` fichier est un format largement utilisé dans les Python projets pour spécifier les dépendances des projets. Chaque ligne de ce fichier inclut un package avec ses contraintes de version. Le générateur Amazon Inspector SBOM analyse ce fichier pour identifier et cataloguer les dépendances avec précision.

Fonctions principales

- Supporte les spécificateurs de version (== et xRip=)
- Supporte les commentaires et les lignes de dépendance complexes

> **Note**
>
> Les spécificateurs de version <= et => ne sont pas pris en charge.

### Exemple de fichier **`requirements.txt`**

Voici un exemple de fichier `requirements.txt`.

```
flask==1.1.2
requests==2.24.0
numpy==1.18.5
foo~=1.2.0
# Comment about a dependency
scipy. # invalid
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Pipfile.lock

Pipenvest un outil qui offre le meilleur de tous les mondes de l'emballage (groupé, épinglé et non épinglé). Il `Pipfile.lock` verrouille les versions exactes des dépendances pour faciliter les constructions déterministes. Le générateur Amazon Inspector SBOM lit ce fichier pour répertorier les dépendances et leurs versions résolues.

Fonctions principales

- Analyse le format JSON pour la résolution des dépendances
- Supporte les dépendances par défaut et de développement

### Exemple de fichier **`Pipfile.lock`**

Voici un exemple de fichier `Pipfile.lock`.

```
{
"default": {
    "requests": {
        "version": "==2.24.0",
        "hashes": [
            "sha256:cc718bb187e53b8d"
        ]
    }
},
"develop": {
    "blinker": {
        "hashes": [
            "sha256:1779309f71bf239144b9399d06ae925637cf6634cf6bd131104184531bf67c01",
```

```
            "sha256:8f77b09d3bf7c795e969e9486f39c2c5e9c39d4ee07424be2bc594ece9642d83"
        ],
        "markers": "python_version >= '3.8'",
        "version": "==1.8.2"
    }
}
}
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Poetry.lock

Poetryest un outil de gestion des dépendances et d'empaquetage pour Python. Le `Poetry.lock` fichier verrouille les versions exactes des dépendances afin de garantir la cohérence des environnements. Le générateur Amazon Inspector SBOM extrait les informations de dépendance détaillées de ce fichier.

### Fonctions principales

- Analyse le format TOML pour les données structurées
- Extrait les noms et les versions des dépendances

### Exemple de fichier **`Poetry.lock`**

Voici un exemple de fichier `Poetry.lock`.

```
[[package]]
name = "flask"
version = "1.1.2"
description = "A simple framework for building complex web applications."
category = "main"
optional = false
```

```
python-versions = ">=3.5"
[[package]]
name = "requests"
version = "2.24.0"
description = "Python HTTP for Humans."
category = "main"
optional = false
python-versions = ">=3.5"
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Œuf/Roue

Pour les packages Python installés dans le monde entier, le générateur Amazon Inspector SBOM prend en charge l'analyse des fichiers de métadonnées trouvés dans les `.egg-info/PKG-INFO` répertoires et. `.dist-info/METADATA` Ces fichiers fournissent des métadonnées détaillées sur les packages installés.

Fonctions principales

- Extrait le nom et la version du package
- Supporte les formats « œuf » et « roue »

Exemple de fichier **`PKG-INFO/METADATA`**

Voici un exemple de fichier `PKG-INFO/METADATA`.

```
Metadata-Version: 1.2
Name: Flask
Version: 1.1.2
Summary: A simple framework for building complex web applications.
```

```
Home-page: https://palletsprojects.com/p/flask/
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Analyse des dépendances Ruby

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| Ruby | Bundler | Gemfile.lock | N/A | N/A | Oui | N/A | Oui |
| | | .gemspec | N/A | N/A | N/A | N/A | Oui |
| | | globall installed Gems | N/A | N/A | N/A | N/A | Oui |

### Gemfile.lock

Le `Gemfile.lock` fichier verrouille les versions exactes de toutes les dépendances afin de garantir que les mêmes versions sont utilisées dans tous les environnements.

Fonctions principales

- Analyse le `Gemfile.lock` fichier pour identifier les dépendances et les versions des dépendances
- Extrait les noms détaillés des packages et les versions des packages

### Exemple de fichier **`Gemfile.lock`**

Voici un exemple de fichier `Gemfile.lock`.

```
GEM
remote: https://rubygems.org/
specs:
ast (2.4.2)
awesome_print (1.9.2)
diff-lcs (1.5.0)
json (2.6.3)
parallel (1.22.1)
parser (3.2.2.0)
nokogiri (1.16.6-aarch64-linux)
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## .gemspec

Le `.gemspec` fichier est un RubyGem fichier contenant des métadonnées relatives à une gemme. Le générateur Amazon Inspector SBOM analyse ce fichier pour collecter des informations détaillées sur une gemme.

Fonctions principales

- Analyse et extrait le nom et la version de la gemme

> **Note**
>
> La spécification de référence n'est pas prise en charge.

### Exemple de fichier `.gemspec`

Voici un exemple de fichier `.gemspec`.

```
Gem::Specification.new do |s|
s.name        = "generategem"
s.version     = "2.0.0"
s.date        = "2020-06-12"
s.summary     = "generategem"
s.description = "A Gemspec Builder"
s.email       = "edersondeveloper@gmail.com"
s.files       = ["lib/generategem.rb"]
s.homepage    = "https://github.com/edersonferreira/generategem"
s.license     = "MIT"
s.executables = ["generategem"]
s.add_dependency('colorize', '~> 0.8.1')
end
```

```
# Not supported

Gem::Specification.new do |s|
s.name        = &class1
s.version     = &foo.bar.version
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Gemmes installées dans le monde entier

Le générateur Amazon Inspector SBOM prend en charge l'analyse des gemmes installées dans le monde entier, qui se trouvent dans des répertoires standard, tels que `/usr/local/lib/`

`ruby/gems/<ruby_version>/gems/` Amazon EC2 /Amazon ECR et Lambda. `ruby/gems/<ruby_version>/gems/` Cela garantit que toutes les dépendances installées dans le monde entier sont identifiées et cataloguées.

Fonctions principales

- Identifie et analyse toutes les gemmes installées dans le monde entier dans les répertoires standard
- Extrait les métadonnées et les informations de version pour chaque gem installée dans le monde entier

Exemple de structure de répertoire

Voici un exemple de structure de répertoire.

```
.
### /usr/local/lib/ruby/3.5.0/gems/
### actrivesupport-6.1.4
### concurrent-ruby-1.1.9
### i18n-1.8.10
```

> **Note**
>
> Cette structure produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

# Analyse des dépendances Rust

| Langage de programmation | Gestionnaire de packages | Artefacts supportés | Support de la chaîne d'outils | Dépendances de développement | Dépendances transitives | Drapeau privé | Récursivement |
|---|---|---|---|---|---|---|---|
| Rust | Cargo.toml | Cargo.toml | N/A | N/A | N/A | N/A | Oui |
| | | Cargo.lock | N/A | N/A | Oui | N/A | Oui |
| | | Rust binary (built with cargo-auditable) | Oui | N/A | N/A | N/A | Oui |

## Cargo en ml

Le `Cargo.toml` fichier est le fichier manifeste des Rust projets.

Fonctions principales

- Analyse et extrait le `Cargo.toml` fichier pour identifier le nom et la version du package du projet.

Exemple de fichier **`Cargo.toml`**

Voici un exemple de fichier `Cargo.toml`.

```
[package]
name = "wait-timeout"
version = "0.2.0"
```

```
description = "A crate to wait on a child process with a timeout specified across Unix
 and\nWindows platforms.\n"
homepage = "https://github.com/alexcrichton/wait-timeout"
documentation = "https://docs.rs/wait-timeout"
readme = "README.md"
categories = ["os"]
license = "MIT/Apache-2.0"
repository = "https://github.com/alexcrichton/wait-timeout"
[target."cfg(unix)".dependencies.libc]
version = "0.2"
[badges.appveyor]
repository = "alexcrichton/wait-timeout"
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Cargo.lock

Le `Cargo.lock` fichier verrouille les versions de dépendance pour s'assurer que les mêmes versions sont utilisées chaque fois qu'un projet est créé.

Fonctions principales

- Analyse le `Cargo.lock` fichier pour identifier toutes les dépendances et les versions de dépendance.

Exemple de fichier **`Cargo.lock`**

Voici un exemple de fichier `Cargo.lock`.

```
# This file is automatically @generated by Cargo.
# It is not intended for manual editing.
[[package]]
```

```
name = "adler32"
version = "1.0.3"
source = "registry+https://github.com/rust-lang/crates.io-index"

[[package]]
name = "aho-corasick"
version = "0.7.4"
source = "registry+https://github.com/rust-lang/crates.io-index"
```

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

## Binaires Rust avec cargo-auditable

Le générateur Amazon Inspector SBOM collecte les dépendances à partir des Rust fichiers binaires créés avec la bibliothèque. `cargo-auditable` Cela fournit des informations de dépendance supplémentaires en permettant l'extraction des dépendances à partir de fichiers binaires compilés.

### Fonctions principales

- Extrait les informations de dépendance directement à partir Rust des fichiers binaires créés avec la bibliothèque `cargo-auditable`
- Récupère les métadonnées et les informations de version pour les dépendances incluses dans les fichiers binaires

> **Note**
>
> Ce fichier produit une sortie contenant l'URL du package. Cette URL peut être utilisée pour spécifier des informations sur les progiciels lors de la génération d'une nomenclature logicielle et peut être incluse dans l'ScanSbomAPI. Pour plus d'informations, consultez package-url sur le GitHub site Web.

# Artefacts non pris en charge

Cette section décrit les artefacts non pris en charge.

## Java

Le générateur Amazon Inspector SBOM Generator prend uniquement en charge la détection des vulnérabilités pour les dépendances provenant du référentiel standard. Maven MavenLes référentiels privés ou personnalisés, tels que Red Hat Maven etJenkins, ne sont pas pris en charge. Pour une détection précise des vulnérabilités, assurez-vous que Java les dépendances sont extraites du Maven référentiel principal. Les dépendances provenant d'autres référentiels ne seront pas couvertes par les analyses de vulnérabilité.

## JavaScript

bundles esbuild

Pour les bundles esbuild minifiés, le générateur SBOM d'Amazon Inspector ne prend pas en charge l'analyse des dépendances pour les projets utilisant. esbuild Les cartes sources générées par esbuild n'incluent pas suffisamment de métadonnées (noms et versions des dépendances) requises pour une Sbomgen génération précise. Pour des résultats fiables, scannez les fichiers du projet d'origine, tels que le `node_modules/directory` et`package-lock.json`, avant le processus de regroupement.

package.json

Le générateur Amazon Inspector SBOM ne prend pas en charge l'analyse des informations de dépendance dans le fichier package.json situé au niveau racine. Ce fichier indique uniquement les noms de packages et les plages de versions, mais n'inclut pas les versions de packages entièrement résolues. Pour des résultats de numérisation précis, utilisez `package.json` ou d'autres fichiers de verrouillage, tels que `yarn.lock` et`pnpm.lock`, qui incluent des versions résolues.

## Dotnet

Lorsque vous utilisez des versions flottantes ou des plages de versions`PackageReference`, il devient plus difficile de déterminer la version exacte du package utilisée dans un projet sans effectuer de résolution de package. Les versions flottantes et les plages de versions permettent aux développeurs de spécifier une plage de versions de package acceptables plutôt qu'une version fixe.

### Binaires Go

Le générateur Amazon Inspector SBOM ne scanne pas Go les fichiers binaires créés avec des indicateurs de compilation configurés pour exclure l'ID de build. Ces indicateurs de construction Bomerman empêchent de mapper avec précision le binaire à sa source d'origine. GoLes fichiers binaires peu clairs ne sont pas pris en charge en raison de l'impossibilité d'extraire les informations du package. Pour une analyse précise des dépendances, assurez-vous que Go les fichiers binaires sont créés avec les paramètres par défaut, y compris l'ID de version.

### Binaires Rust

Le générateur Amazon Inspector SBOM analyse les Rust fichiers binaires uniquement s'ils sont créés à l'aide de la bibliothèque cargo-auditable. Rustles binaires n'utilisant pas cette bibliothèque ne disposent pas des métadonnées nécessaires pour une extraction précise des dépendances. Le générateur Amazon Inspector SBOM extrait la version compilée de la Rust chaîne d'outils à partir de la version Rust 1.7.3, mais uniquement pour les fichiers binaires d'un environnement. Linux Pour une analyse complète, créez des Rust fichiers binaires à l'Linuxaide de cargo-auditable.

> **Note**
>
> La détection des vulnérabilités pour la Rust chaîne d'outils elle-même n'est pas prise en charge, même si la version de la chaîne d'outils est extraite.

## Collection complète de l'écosystème Amazon Inspector SBOM Generator

Le générateur Amazon Inspector SBOM est un outil permettant de créer une nomenclature logicielle (SBOM) et d'effectuer une analyse des vulnérabilités pour les packages pris en charge par les systèmes d'exploitation et les langages de programmation. Il prend également en charge l'analyse de divers écosystèmes au-delà des systèmes d'exploitation principaux, garantissant ainsi une analyse robuste et détaillée des composants de l'infrastructure. En générant une SBOM, les utilisateurs peuvent comprendre la composition de leur infrastructure technologique moderne, identifier les vulnérabilités des composants de l'écosystème et gagner en visibilité sur les logiciels tiers.

# Écosystèmes soutenus

La collection de l'écosystème étend la génération de SBOM au-delà des packages installés via les gestionnaires de packages du système d'exploitation. Cela se fait par le biais de la collecte d'applications déployées selon des méthodes alternatives, telles que l'installation manuelle. Le générateur Amazon Inspector SBOM prend en charge l'analyse des écosystèmes suivants :

| Écosystèmes | Applications |
| --- | --- |
| Oracle Java | JDK<br>JRE<br>Amazon Corretto |
| Apache | httpd<br>tomcat |
| WordPress | principal<br>.<br>thème |
| Google | Chrome |
| Node.JS | nœud |

## Apachecollection de l'écosystème

Le générateur Amazon Inspector SBOM recherche les Apache installations qui se trouvent dans des chemins d'installation communs à toutes les plateformes :

- macOS: `/Library/`
- Linux: `/etc/`, `/usr/share`, `/usr/lib`, `/usr/local`, `/var`, `/opt`

Applications prises en charge

- httpd
- tomcat

Fonctions principales

- Apache httpd— Analyse le `/include/ap_release.h` fichier pour extraire les macros d'installation, qui contiennent les chaînes d'identification principales, les chaînes d'identification secondaires et les chaînes d'identification des correctifs.
- Apache tomcat— Décompresse le `catalina.jar` fichier pour extraire les macros d'installation à l'intérieur du fichier (`META-INF/MANIFEST.MF`), qui contient la chaîne de version.

Exemple de fichier **`ap_release.h`**

Voici un exemple du contenu du `ap_release.h` fichier.

```
//truncated

#define AP_SERVER_BASEVENDOR "Apache Software Foundation"
#define AP_SERVER_BASEPROJECT "Apache HTTP Server"
#define AP_SERVER_BASEPRODUCT "Apache"

#define AP_SERVER_MAJORVERSION_NUMBER 2
#define AP_SERVER_MINORVERSION_NUMBER 4
#define AP_SERVER_PATCHLEVEL_NUMBER   1
#define AP_SERVER_DEVBUILD_BOOLEAN    0

//truncated
```

Exemple de PURL

Voici un exemple d'URL de package pour une `Apache httpd` application.

```
Sample PURL: pkg:generic/apache/httpd@2.4.1
```

Exemple de fichier **`catalina.jar/META-INF/MANIFEST.MF`**

Voici un exemple du contenu du `catalina.jar/META-INF/MANIFEST.MF` fichier.

```
//truncated

Implementation-Title: Apache Tomcat
Implementation-Vendor: Apache Software Foundation
Implementation-Version: 10.1.31

//truncated
```

Exemple de PURL

Voici un exemple d'URL de package pour une `Apache Tomcat` application.

```
Sample PURL: pkg:generic/apache/tomcat@10.1.31
```

## Javacollection de l'écosystème

Applications prises en charge

- Oracle JDK
- Oracle JRE
- Amazon Corretto

Fonctions principales

- Extrait la chaîne de caractères de l'Javainstallation.
- Identifie le chemin du répertoire qui contient le Java runtime.
- Identifie le fournisseur en tant que Oracle JDKOracle JRE, etAmazon Corretto.

Le générateur Amazon Inspector SBOM analyse les Java installations sur les chemins d'installation et plateformes suivants :

- macOS: `/Library/Java/JavaVirtualMachines`
- Linux 32-bit: `/usr/lib/jvm`
- Linux 64-bit: `/usr/lib64/jvm`
- Linux (generic): `/usr/java and /opt/java`

Exemple d'informations sur Java la version

Voici un exemple de Oracle Java version.

```
// Amazon Corretto
IMPLEMENTOR="Amazon.com Inc."
IMPLEMENTOR_VERSION="Corretto-17.0.11.9.1"
JAVA_RUNTIME_VERSION="17.0.11+9-LTS"
JAVA_VERSION="17.0.11"
JAVA_VERSION_DATE="2024-04-16"
LIBC="default"
MODULES="java.base java.compiler java.datatransfer java.xml java.prefs java.desktop
 java.instrument java.logging java.management java.security.sasl java.naming
 java.rmi java.management.rmi java.net.http java.scripting java.security.jgss
 java.transaction.xa java.sql java.sql.rowset java.xml.crypto java.se java.smartcardio
 jdk.accessibility jdk.internal.jvmstat jdk.attach jdk.charsets jdk.compiler
 jdk.crypto.ec jdk.crypto.cryptoki jdk.dynalink jdk.internal.ed jdk.editpad
 jdk.hotspot.agent jdk.httpserver jdk.incubator.foreign jdk.incubator.vector
 jdk.internal.le jdk.internal.opt jdk.internal.vm.ci jdk.internal.vm.compiler
 jdk.internal.vm.compiler.management jdk.jartool jdk.javadoc jdk.jcmd jdk.management
 jdk.management.agent jdk.jconsole jdk.jdeps jdk.jdwp.agent jdk.jdi jdk.jfr jdk.jlink
 jdk.jpackage jdk.jshell jdk.jsobject jdk.jstatd jdk.localedata jdk.management.jfr
 jdk.naming.dns jdk.naming.rmi jdk.net jdk.nio.mapmode jdk.random jdk.sctp
 jdk.security.auth jdk.security.jgss jdk.unsupported jdk.unsupported.desktop
 jdk.xml.dom jdk.zipfs"
OS_ARCH="x86_64"
OS_NAME="Darwin"
SOURCE=".:git:7917f11551e8+"

// JDK
IMPLEMENTOR="Oracle Corporation"
JAVA_VERSION="19"
JAVA_VERSION_DATE="2022-09-20"
LIBC="default"
MODULES="java.base java.compiler java.datatransfer java.xml java.prefs java.desktop
 java.instrument java.logging java.management java.security.sasl java.naming
```

```
 java.rmi java.management.rmi java.net.http java.scripting java.security.jgss
 java.transaction.xa java.sql java.sql.rowset java.xml.crypto java.se java.smartcardio
 jdk.accessibility jdk.internal.jvmstat jdk.attach jdk.charsets jdk.zipfs jdk.compiler
 jdk.crypto.ec jdk.crypto.cryptoki jdk.dynalink jdk.internal.ed jdk.editpad
 jdk.hotspot.agent jdk.httpserver jdk.incubator.concurrent jdk.incubator.vector
 jdk.internal.le jdk.internal.opt jdk.internal.vm.ci jdk.internal.vm.compiler
 jdk.internal.vm.compiler.management jdk.jartool jdk.javadoc jdk.jcmd jdk.management
 jdk.management.agent jdk.jconsole jdk.jdeps jdk.jdwp.agent jdk.jdi jdk.jfr jdk.jlink
 jdk.jpackage jdk.jshell jdk.jsobject jdk.jstatd jdk.localedata jdk.management.jfr
 jdk.naming.dns jdk.naming.rmi jdk.net jdk.nio.mapmode jdk.random jdk.sctp
 jdk.security.auth jdk.security.jgss jdk.unsupported jdk.unsupported.desktop
 jdk.xml.dom"
OS_ARCH="x86_64"
OS_NAME="Darwin"
SOURCE=".:git:53b4a11304b0 open:git:967a28c3d85f"
```

Exemple de PURL

Voici un exemple d'URL de package pour une Oracle Java version.

```
Sample PURL:
# Amazon Corretto
pkg:generic/amazon/amazon-corretto@21.0.3
# Oracle JDK
pkg:generic/oracle/jdk@11.0.16
# Oracle JRE
pkg:generic/oracle/jre@20
```

## Googlecollection de l'écosystème

Application prise en charge

- Google Chrome

Artefacts supportés

Amazon Inspector collecte des Google Chrome informations auprès des sources suivantes :

- Le `chrome/VERSION` fichier (source de construction)

- Le `puppeteer` fichier (installation)

Le générateur Amazon Inspector SBOM analyse et collecte les versions correspondantes de chacun des artefacts pris en charge.

Exemple de fichier de **`chrome/VERSION`** version

Voici un exemple de fichier de `chrome/VERSION` version.

```
MAJOR=130
MINOR=0
BUILD=6723
PATCH=58
```

Exemple de PURL

Voici un exemple d'URL de package pour un fichier de `chrome/VERSION` version.

```
Sample PURL: pkg:generic/google/chrome@131.0.6778.87
```

Exemple de fichier de **`puppeteer`** version

Voici un exemple de fichier de `puppeteer` version.

```
{
"name": "puppeteer",
"version": "23.9.0",
"description": "A high-level API to control headless Chrome over the DevTools
 Protocol",
"keywords": [
  "puppeteer",
  "chrome",
  "headless",
  "automation"
]
}
```

Exemple de PURL

Voici un exemple d'URL de package pour un fichier de `puppeteer` version.

```
Sample PURL: pkg:generic/google/puppeteer@23.9.0
```

## WordPresscollection de l'écosystème

Composants pris en charge

- WordPress core
- WordPressplugins
- WordPressthèmes

Fonctions principales

- WordPresscore — analyse le `/wp-includes/version.php` fichier pour extraire la valeur de version de la variable $wp_version.
- WordPressplugins — analyse le `/wp-content/plugins/<WordPress Plugin>/readme.txt` fichier ou le `/wp-content/plugins/<WordPress Plugin>/readme.md` fichier pour extraire le `Stable` tag sous forme de chaîne de version.
- WordPressthèmes — analyse le `/wp-content/themes/<WordPress Theme>/style.css` fichier pour extraire la version à partir des métadonnées de version.

Exemple de fichier **`version.php`**

Voici un exemple de `version.php` fichier de WordPress base.

```
// truncated

/**
* The WordPress version string.
*
* Holds the current version number for WordPress core. Used to bust caches
* and to enable development mode for scripts when running from the /src directory.
```

```
*
* @global string $wp_version
*/
$wp_version = '6.5.5';

// truncated
```

Exemple de PURL

Voici un exemple d'URL de package pour le WordPress noyau.

```
Sample PURL: pkg:generic/wordpress/core/wordpress@6.5.5
```

Exemple de fichier **`readme.txt`**

Voici un exemple de `readme.txt` fichier de WordPress plugin.

```
=== Plugin Name ===
Contributors: (this should be a list of wordpress.org userid's)
Donate link: https://example.com/
Tags: tag1, tag2
Requires at least: 4.7
Tested up to: 5.4
Stable tag: 4.3
Requires PHP: 7.0
License: GPLv2 or later
License URI: https://www.gnu.org/licenses/gpl-2.0.html

// truncated
```

Exemple de PURL

Voici un exemple d'URL de package pour un WordPress plugin.

```
Sample PURL: pkg:generic/wordpress/plugin/exclusive-addons-for-elementor@1.0.0
```

### Exemple de fichier **`style.css`**

Voici un exemple de `style.css` fichier de WordPress thème.

```
/*
Author: the WordPress team
Author URI: https://wordpress.org
Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable
 to any website. Its collection of templates and patterns tailor to different needs,
 such as presenting a business, blogging and writing or showcasing work. A multitude
 of possibilities open up with just a few adjustments to color and typography. Twenty
 Twenty-Four comes with style variations and full page designs to help speed up the
 site building process, is fully compatible with the site editor, and takes advantage
 of new design tools introduced in WordPress 6.4.
Requires at least: 6.4
Tested up to: 6.5
Requires PHP: 7.0
Version: 1.2
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Text Domain: twentytwentyfour
Tags: one-column, custom-colors, custom-menu, custom-logo, editor-style, featured-
images, full-site-editing, block-patterns, rtl-language-support, sticky-post,
 threaded-comments, translation-ready, wide-blocks, block-styles, style-variations,
 accessibility-ready, blog, portfolio, news
*/
```

### Exemple de PURL

Voici un exemple d'URL de package pour un WordPress thème.

```
Sample PURL: pkg:generic/wordpress/theme/avada@1.0.0
```

## Node.JScollection d'exécution

### Applications prises en charge

- binaire d'exécution de nœuds pour Node.JS

Artefacts supportés

- MacOSet Linux — détection `node` binaire par le biais de détails binaires installés avec `asdf`,`fnm`,`nvm`, ou `volta`

> **Note**
>
> Dockerles images ou les images créées par l'node.jséditeur ne sont pas prises en charge. Ces images ne contiennent pas d'artefacts fiables. Vous pouvez consulter des exemples de ces images sur le Dockerhub et. GitHub

Exemple MacOS et Linux parcours

Voici un exemple de chemins pour MacOS etLinux.

```
NVM:   ~/.nvm/, /usr/local/nvm
FNM:   ~/.local/share/fnm/
ASDF:  ~/.asdf/
MISE:  ~/.local/share/mise/
VOLTA: ~/.volta/
```

Exemple de PURL

Voici un exemple d'URL de package pourNode.JS.

```
Sample PURL: pkg:generic/nodejs/node@20.18.0
```

# Collection de licences Amazon Inspector SBOM Generator

Le générateur Amazon Inspector SBOM permet de suivre les informations de licence figurant dans une nomenclature logicielle (SBOM). Il collecte des informations de licence à partir de packages pris en charge par différents systèmes d'exploitation et langages de programmation. Avec des expressions de licence standardisées dans votre SBOM générée, vous pouvez comprendre vos obligations en matière de licence.

## Collectez les informations de licence

Exemple de commande

L'exemple suivant montre comment collecter des informations de licence à partir d'un répertoire.

```
./inspector-sbomgen directory --path /path/to/your/directory/ --collect-licenses
```

Exemple de composant SBOM

L'exemple suivant montre une entrée de composant dans le SBOM généré.

```
"components": [
    {
      "bom-ref": "comp-2",
      "type": "application",
      "name": "sample-js-pkg",
      "version": "1.2.3",
      "licenses": [
        {
          "expression": "Apache-2.0 AND (MIT OR GPL-2.0-only)"
        }
      ],
      "purl": "pkg:npm/sample-js-pkg@1.2.3",
    }
  ]
```

## Packages pris en charge

Les langages de programmation et packages de systèmes d'exploitation suivants sont pris en charge pour la collecte de licences.

| Cible | Gestionnaire de packages | Source d'informations sur les licences | Type |
|---|---|---|---|
| Alma Linux | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages | Système d'exploitation |

| Cible | Gestionnaire de packages | Source d'informations sur les licences | Type |
|---|---|---|---|
| | | • /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | |
| Amazon Linux | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |

| Cible | Gestionnaire de packages | Source d'informations sur les licences | Type |
| --- | --- | --- | --- |
| CentOS | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |
| Fedora | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |

| Cible | Gestionnaire de packages | Source d'informations sur les licences | Type |
| --- | --- | --- | --- |
| OpenSUSE | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |
| Oracle Linux | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |

| Cible | Gestionnaire de packages | Source d'informations sur les licences | Type |
|---|---|---|---|
| Photon OS | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |
| RHEL | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |

| Cible | Gestionnaire de packages | Source d'informations sur les licences | Type |
|---|---|---|---|
| Rocky Linux | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |
| SLES | RPM | • /usr/lib/sysimage/rpm/rpmdb.sqlite<br>• /usr/lib/sysimage/rpm/Packages<br>• /usr/lib/sysimage/rpm/Packages.db<br>• /var/lib/rpm/rpmdb.sqlite<br>• /var/lib/rpm/Packages<br>• /var/lib/rpm/Packages.db | Système d'exploitation |
| Alpine Linux | APK | `/lib/apk/db/installed` | Système d'exploitation |
| Chainguard | APK | `/lib/apk/db/installed` | Système d'exploitation |

| Cible | Gestionnaire de packages | Source d'informations sur les licences | Type |
|---|---|---|---|
| Debian | DPKG | `/usr/share/doc/*/copyright` | Système d'exploitation |
| Ubuntu | DPKG | `/usr/share/doc/*/copyright` | Système d'exploitation |
| Node.js | Javascript | `node_modules/*/package.json` | Langage de programmation |
| PHP | Package Composer | • `composer.lock`<br>• `/vendor/composer/installed.json` | Langage de programmation |
| Go | Go | `LICENSE` | Langage de programmation |
| Python | Python/Egg/Wheel | • `.dist-info/METADATA`<br>• `.egg-info`<br>• `.egg-info/PKG-INFO` | Langage de programmation |
| Ruby | RubyGem | `*.gemspec` | Langage de programmation |
| Rust | crate | `Cargo.toml` | Langage de programmation |

## Normalisation des expressions de licence

Le format d'expressions de licence SPDX fournit une représentation précise des termes de licence trouvés dans les logiciels open source. Le générateur Amazon Inspector SBOM normalise toutes les

informations de licence dans des expressions de licence SPDX grâce aux règles décrites dans cette section. Les règles assurent la cohérence et la compatibilité des informations de licence.

Cartographie abrégée des identifiants SPDX

Tous les noms de licence sont mappés à des identifiants abrégés SPDX. Par exemple, `MIT License` est abrégée en `MIT`.

Combinaison de licences multiples

Vous pouvez associer plusieurs licences à l'`AND`opérateur. Voici un exemple de commande qui montre comment formater votre commande.

```
MIT AND Apache-2.0
```

Préfixe de licence personnalisé

Les licences personnalisées sont préfixées par`LicenseRef`, par exemple`LicenseRef-CompanyPrivate`.

Préfixe d'exception personnalisé

Les exceptions personnalisées sont préfixées par`AdditionRef-`, par exemple`AdditionRef-CustomException`.

# Qu'est-ce que l'URL d'un package ?

Une URL de package ou PURL est un format standardisé utilisé pour identifier les packages logiciels, les composants et les bibliothèques dans différents systèmes de gestion de packages. Ce format facilite le suivi, l'analyse et la gestion des dépendances dans les projets logiciels, en particulier lors de la génération d'une nomenclature logicielle (SBOMs).

## Structure PURL

La structure PURL est similaire à une URL et se compose de plusieurs composants :

- `pkg`— Le préfixe littéral
- `type`— Le type de package

- `namespace`— Le regroupement
- `name`— Le nom du package
- `version`— La version du package
- `qualifiers`— Paires clé-valeur supplémentaires
- `subpath`— Le chemin du fichier dans le package

Exemple de PURL

Voici un exemple de ce à quoi pourrait ressembler une URL.

```
pkg:<type>/<namespace>/<name>@<version>?<qualifiers>#<subpath>
```

## Le PURL générique

Un PURL générique est utilisé pour représenter les progiciels et les composants qui ne correspondent pas aux écosystèmes de packages établis, tels que npmpypi, oumaven. Il identifie les composants logiciels et capture les métadonnées susceptibles de ne pas correspondre à des systèmes de gestion de packages spécifiques. Un PURL générique est utile pour divers projets logiciels, qu'il s'agisse de fichiers binaires compilés ou de plateformes telles que Apache et. WordPress Cela permet de l'appliquer à un large éventail de cas d'utilisation, y compris les fichiers binaires compilés, les plateformes Web et les distributions de logiciels personnalisées.

Principaux cas d'utilisation

- Supporte les fichiers binaires compilés et est utile pour Go et Rust
- Prend en charge les plateformes Web, telles que Apache etWordPress, où un package peut ne pas être associé aux gestionnaires de packages traditionnels.
- Prend en charge les logiciels existants personnalisés en permettant aux organisations de référencer des logiciels développés en interne ou des systèmes dépourvus de packages formels.

Exemple de format

Voici un exemple du format générique de PURL.

```
pkg:generic/<namespace>/<name>@<version>?<qualifiers>
```

### Exemples supplémentaires du format générique PURL

Vous trouverez ci-dessous des exemples supplémentaires du format PURL générique.

#### GoBinaire compilé

Ce qui suit représente le `inspector-sbomgen binary` compilé avec unGo.

```
pkg:generic/inspector-sbomgen?go_toolchain=1.22.5
```

#### RustBinaire compilé

Ce qui suit représente le `myrustapp` binaire compilé avecRust.

```
pkg:generic/myrustapp?rust_toolchain=1.71.0
```

#### Projet Apache

Ce qui suit fait référence à un projet http sous l'espace de Apache noms.

```
pkg:generic/apache/httpd@1.0.0
```

#### Logiciel WordPress

Ce qui suit fait référence à un WordPress logiciel de base.

```
pkg:generic/wordpress/core/wordpress@6.0.0
```

#### WordPressthème

Ce qui suit fait référence à un WordPress thème personnalisé.

```
pkg:generic/wordpress/theme/mytheme@1.0.0
```

#### WordPress plugin

Ce qui suit fait référence à un WordPress plugin personnalisé.

```
pkg:generic/wordpress/plugin/myplugin@1.0.0
```

# Gestion des références de version non résolues ou non standard dans le générateur Amazon Inspector SBOM

Le générateur Amazon Inspector SBOM localise et analyse les artefacts pris en charge au sein d'un système en identifiant les dépendances directement à partir des fichiers source. Il ne s'agit pas d'un gestionnaire de packages et il ne résout pas les plages de versions, ne déduit pas les versions sur la base de références dynamiques ou ne gère pas les recherches dans le registre. Il collecte les dépendances uniquement telles qu'elles sont définies dans les artefacts de la source du projet. Dans de nombreux cas, les dépendances figurant dans les manifestes de package, telles que`package.json`, ou `pom.xml`requirements.txt, sont spécifiées à l'aide de versions non résolues ou basées sur des plages. Cette rubrique contient des exemples de ce à quoi peuvent ressembler ces dépendances.

## Recommandations

Le générateur Amazon Inspector SBOM extrait les dépendances des artefacts source, mais ne résout ni n'interprète les plages de versions ni les références dynamiques. Pour une analyse plus précise des vulnérabilités SBOMs, nous vous recommandons d'utiliser des identifiants de version sémantiques résolus dans les dépendances du projet.

## Java

En effetJava, les Maven projets peuvent utiliser des plages de versions pour définir les dépendances dans le `pom.xml` fichier.

```
<dependency>
    <groupId>org.inspector</groupId>
    <artifactId>inspector-api</artifactId>
    <version>(,1.0]</version>
</dependency>
```

La plage indique que toute version inférieure ou égale à 1.0 est acceptable. Toutefois, si une version n'est pas une version résolue, le générateur Amazon Inspector SBOM ne la collectera pas car elle ne peut pas être mappée à une version spécifique.

## JavaScript

En JavaScript effet, le `package.json` fichier peut inclure des plages de versions similaires aux suivantes :

```
"dependencies": {
    "ky": "^1.2.0",
    "registry-auth-token": "^5.0.2",
    "registry-url": "^6.0.1",
    "semver": "^7.6.0"
}
```

L'^opérateur indique que toute version supérieure ou égale à la version spécifiée est acceptable. Toutefois, si la version spécifiée n'est pas une version résolue, le générateur SBOM d'Amazon Inspector ne la collectera pas, car cela peut générer des faux positifs lors de la détection d'une vulnérabilité.

## Python

En Python effet, le `requirements.txt` fichier peut inclure des entrées contenant une expression booléenne.

```
requests>=1.0.0
```

L'>=opérateur indique que toute version supérieure ou égale à `1.0.0` est acceptable. Comme cette expression particulière ne spécifie pas de version exacte, le générateur Amazon Inspector SBOM ne peut pas collecter une version de manière fiable pour l'analyse des vulnérabilités.

Le générateur SBOM d'Amazon Inspector ne prend pas en charge les identifiants de version non standard ou ambigus, tels que les versions bêta, les plus récentes ou les instantanés.

```
pkg:maven/org.example.com/testmaven@1.0.2%20Beta-RC-1_Release
```

> **Note**
>
> L'utilisation d'un suffixe non standard, tel queBeta-RC-1_Release, n'est pas conforme au versionnement sémantique standard et ne peut pas être évaluée pour détecter les vulnérabilités du moteur de détection Amazon Inspector.

# Utilisation CycloneDX espaces de noms avec Amazon Inspector

Amazon Inspector vous fournit CycloneDX espaces de noms et noms de propriétés que vous pouvez utiliser avec SBOMs. Cette section décrit toutes les propriétés clé/valeur personnalisées qui peuvent être ajoutées aux composants dans CycloneDX SBOMs. Pour plus d'informations, consultez la taxonomie des propriétés CycloneDx sur le GitHub site Web.

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

L'API Amazon Inspector Scan utilise l'espace de `amazon:inspector:sbom_scanner` noms et possède les propriétés suivantes :

| Propriété | Description |
|---|---|
| `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 est attendu conformément au catalogue CISA Known Exploited Vulnerabilities. |
| `amazon:inspector:sbom_scanner:critical_vulnerabilities` | Nombre total de vulnérabilités critiques détectées dans le SBOM. |
| `amazon:inspector:sbom_scanner:exploit_available` | Indique si un exploit est disponible pour la vulnérabilité donnée. |

| Propriété | Description |
| --- | --- |
| `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:fixed_version: component_bom_ref` | Fournit la version corrigée du composant indiqué pour la vulnérabilité donnée. |
| `amazon:inspector:sbom_scanner:high_vulnerabilities` | Nombre total de vulnérabilités très graves 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:is_malicious` | Indique si OpenSSF identifie les composants concernés comme malveillants. |
| `amazon:inspector:sbom_scanner:low_vulnerabilities` | Nombre total de vulnérabilités de faible gravité 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:path` | Le chemin d'accès au fichier qui fournit les informations du package objet. |
| `amazon:inspector:sbom_scanner:priority` | Priorité recommandée pour corriger une vulnérabilité donnée. Les valeurs par ordre décroissant sont « IMMÉDIAT », « URGENT », « MODÉRÉ » et « STANDARD ». |
| `amazon:inspector:sbom_scanner:priority_intelligence` | La qualité des informations utilisées pour déterminer la priorité d'une vulnérabilité donnée. Les valeurs incluent « VÉRIFIÉ » ou « NON VÉRIFIÉ ». |

| Propriété | Description |
| --- | --- |
| `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_generator`taxonomie des espaces de noms

Le générateur Amazon Inspector SBOM utilise l'espace de `amazon:inspector:sbom_generator` noms et possède les propriétés suivantes :

| Propriété | Description |
| --- | --- |
| `amazon:inspector:sbom_generator:cpu_architecture` | Architecture du processeur du système en cours d'inventaire (x86_64). |
| `amazon:inspector:sbom_generator:ec2:instance_id` | L'ID de l' EC2 instance Amazon. |
| `amazon:inspector:sbom_generator:live_patching_enabled` | Une valeur booléenne indiquant si les correctifs en direct sont activés sur Amazon Amazon EC2 Linux. |
| `amazon:inspector:sbom_generator:live_patched_cves` | Liste des CVEs correctifs mis à jour en direct sur Amazon Amazon EC2 Linux. |
| `amazon:inspector:sbom_generator:dockerfile_finding: inspector_finding_id` | Indique qu'une découverte d'Amazon Inspector dans un composant est liée à Dockerfile chèques. |
| `amazon:inspector:sbom_generator:image_id` | Le hachage appartenant au fichier de configuration de l'image du conteneur (également appelé ID d'image). |
| `amazon:inspector:sbom_generator:image_arch` | Architecture de l'image du conteneur. |

| Propriété | Description |
| --- | --- |
| `amazon:inspector:sbom_generator:image_author` | Auteur de l'image du conteneur. |
| `amazon:inspector:sbom_generator:image_docker_version` | La version du docker utilisée pour créer l'image du conteneur. |
| `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:duplicate_purl` | Indique la URL du package dupliqué trouvée par un autre scanner. |
| `amazon:inspector:sbom_generator:kernel_name` | Nom du noyau du système en cours d'inventaire. |
| `amazon:inspector:sbom_generator:kernel_version` | Version du noyau du système inventoriée. |
| `amazon:inspector:sbom_generator:kernel_component` | Une valeur booléenne indiquant si un package objet est un composant du noyau |
| `amazon:inspector:sbom_generator:running_kernel` | Une valeur booléenne qui indique si le package objet est le noyau en cours d'exécution |
| `amazon:inspector:sbom_generator:layer_diff_id` | Le hachage de la couche d'image du conteneur non compressée. |
| `amazon:inspector:sbom_generator:replaced_by` | La valeur qui remplace la valeur actuelle Go module. |
| `amazon:inspector:sbom_generator:os_hostname` | Le nom d'hôte du système en cours d'inventaire. |
| `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` . |

| Propriété | Description |
| --- | --- |
| `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:file_size_bytes` | Indique la taille du fichier d'un artefact donné. |
| `amazon:inspector:sbom_generator:unresolved_version` | Indique une chaîne de version qui n'a pas été résolue par le gestionnaire de packages. |
| `amazon:inspector:sbom_generator:experimental:transitive_dependency` | Indique les dépendances indirectes d'un gestionnaire de packages. |

# Intégration des scans Amazon Inspector dans votre pipeline CI/CD

L'intégration Amazon Inspector CI/CD utilise le générateur Amazon Inspector SBOM et l'API Amazon Inspector Scan pour produire des rapports de vulnérabilité pour les images de conteneurs. Le générateur Amazon Inspector SBOM crée une nomenclature logicielle (SBOM) pour les archives, les images de conteneurs, les répertoires, les systèmes locaux, les compilés et les fichiers binaires. Go Rust L'API Amazon Inspector Scan scanne le SBOM pour créer un rapport contenant des informations détaillées sur les vulnérabilités détectées. Vous pouvez intégrer les scans d'images de conteneurs Amazon Inspector à votre CI/CD pipeline to scan for software vulnerabilities and produce vulnerability reports, which allow you to investigate and remediate risks before deployment. To set up your CI/CD integration, you can use plugins or create a custom CI/CD intégration à l'aide du générateur Amazon Inspector SBOM et de l'API Amazon Inspector Scan.

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 la CI/CD solutions. For complete instructions on setting up the CI/CD integration using a plugin, select the plugin for your CI/CD solution suivante :

- Plug-in Jenkins
- TeamCity plugin
- GitHub actions

## Intégration personnalisée

Si Amazon Inspector ne fournit pas de plug-ins pour votre CI/CD solution, you can create your own custom CI/CD intégration à l'aide d'une combinaison du générateur SBOM Amazon Inspector et de

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 d'une intégration de pipeline CI/CD personnalisée avec Amazon Inspector Scan.

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

Pour utiliser l'intégration Amazon Inspector CI/CD, vous devez vous inscrire à un. Compte AWS Ils Compte AWS doivent avoir un rôle IAM qui accorde à votre pipeline CI/CD 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 doté d'un accès 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 l'https://portal.aws.amazon.com/billing/inscription.
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 racine 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, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

## Création d'un utilisateur doté d'un accès 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 racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .

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

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

Création d'un utilisateur doté d'un accès 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.

   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 doté d'un accès 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.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

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

# 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 (). SBOMs 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 https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de la console IAM, cliquez sur Politiques, puis choisissez 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`.

# Vérifications des fichiers Dockerfile par Amazon Inspector

Cette section décrit comment utiliser le générateur Amazon Inspector SBOM pour scanner Dockerfiles et stocker des images afin de détecter les erreurs Docker de configuration susceptibles d'introduire des failles de sécurité.

Rubriques

- Utilisation des Sbomgen vérifications Dockerfile
- Vérifications Dockerfile prises en charge

## Utilisation des Sbomgen vérifications Dockerfile

Les vérifications Dockerfile sont effectuées automatiquement lorsqu'un fichier `*.Dockerfile` est nommé `Dockerfile` ou découvert et lorsqu'une image Docker est numérisée.

Vous pouvez désactiver les vérifications Dockerfile à l'aide de l'`--skip-scanners dockerfile`argument. Vous pouvez également combiner les vérifications Dockerfile avec n'importe quel scanner disponible, tel que le système d'exploitation ou les packages tiers.

Exemples de commandes de vérification Docker

Les exemples de commandes suivants montrent comment générer des images SBOMs pour Dockerfiles et des conteneurs Docker, ainsi que pour des systèmes d'exploitation et des packages tiers.

```
# generate SBOM only containing Docker checks for Dockerfiles in a local directory
./inspector-sbomgen directory --path ./project/ --scanners dockerfile

# generate SBOM for container image will by default include Dockerfile checks
./inspector-sbomgen container --image image:tag

# generate SBOM only containing Docker checks for specific Dockerfiles and Alpine,
 Debian, and Rhel OS packages in a local directory
/inspector-sbomgen directory --path ./project/ --scanners dockerfile,dpkg,alpine-
apk,rhel-rpm

# generate SBOM only containing Docker checks for specific Dockerfiles in a local
 directory
./inspector-sbomgen directory --path ./project/ --skip-scanners dockerfile
```

Exemple de composant de fichier

Voici un exemple de recherche Dockerfile pour un composant de fichier.

```
{
     "bom-ref": "comp-2",
      "name": "dockerfile:data/docker/Dockerfile",
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:dockerfile_finding:IN-DOCKER-001",
          "value": "affected_lines:27-27"
        }
      ],
      "type": "file"
    },
```

Exemple de composant de réponse aux vulnérabilités

Voici un exemple de découverte par Dockerfile d'un composant de réponse à une vulnérabilité.

```
{
      "advisories": [
        {
```

```
          "url": "https://docs.docker.com/develop/develop-images/instructions/"
        }
      ],
      "affects": [
        {
          "ref": "comp-2"
        }
      ],
      "analysis": {
        "state": "in_triage"
      },
      "bom-ref": "vuln-13",
      "created": "2024-03-27T14:36:39Z",
      "description": "apt-get layer caching: Using apt-get update alone in a RUN
statement causes caching issues and subsequent apt-get install instructions to fail.",
      "id": "IN-DOCKER-001",
      "ratings": [
        {
          "method": "other",
          "severity": "info",
          "source": {
            "name": "AMAZON_INSPECTOR",
            "url": "https://aws.amazon.com/inspector/"
          }
        }
      ],
      "source": {
        "name": "AMAZON_INSPECTOR",
        "url": "https://aws.amazon.com/inspector/"
      },
      "updated": "2024-03-27T14:36:39Z"
    },
```


> **Note**
>
> Si vous appelez Sbomgen sans l'`--scan-sbom`indicateur, vous ne pouvez afficher que les résultats bruts de Dockerfile.

## Vérifications Dockerfile prises en charge

SbomgenLes vérifications Dockerfile sont prises en charge dans les cas suivants :

- Le paquet binaire Sudo
- utilitaires APT pour Debian
- Secrets codés en dur
- Conteneurs pour racines
- Indicateurs de commande affaiblissant l'exécution
- Variables d'environnement affaiblissant l'exécution

Chacune de ces vérifications Dockerfile est associée à une note de gravité correspondante, qui est indiquée en haut des rubriques suivantes.

> **Note**
>
> Les recommandations décrites dans les rubriques suivantes sont basées sur les meilleures pratiques du secteur.

## Le paquet binaire Sudo

> **Note**
>
> L'indice de gravité de cette vérification est Info.

Nous vous recommandons de ne pas installer ou utiliser le paquet binaire Sudo car il présente un comportement imprévisible en matière de TTY et de transfert de signal. Pour plus d'informations, consultez la section Utilisateur sur le site Web de Docker Docs. Si votre cas d'utilisation nécessite des fonctionnalités similaires à celles du package binaire Sudo, nous vous recommandons d'utiliser Gosu.

## Debianutilitaires APT

> **Note**
>
> L'indice de sévérité de cette vérification est élevé.

Les meilleures pratiques d'utilisation des utilitaires Debian APT sont les suivantes.

Combinaison de **`apt-get`** commandes dans une seule **`Run`** instruction pour éviter les problèmes de mise en cache

Nous vous recommandons de combiner `apt-get` les commandes dans une seule instruction RUN à l'intérieur de votre conteneur Docker. L'utilisation `apt-get update` en elle-même entraîne des problèmes de mise en cache et l'échec `apt-get install` des instructions ultérieures. Pour plus d'informations, consultez apt-get sur le site Web de Docker Docs.

> **Note**
>
> Le comportement de mise en cache décrit peut également se produire à l'intérieur de votre Docker conteneur si le logiciel de conteneur Docker est obsolète.

Utilisation de l'utilitaire de ligne de commande APT de manière non interactive

Nous recommandons d'utiliser l'utilitaire de ligne de commande APT de manière interactive. L'utilitaire de ligne de commande APT est conçu comme un outil pour l'utilisateur final et son comportement change d'une version à l'autre. Pour plus d'informations, consultez Utilisation des scripts et différences par rapport aux autres outils APT sur le site Web de Debian.

## Secrets codés en dur

> **Note**
>
> L'indice de gravité de cette vérification est critique.

Les informations confidentielles contenues dans votre Dockerfile sont considérées comme un secret codé en dur. Les secrets codés en dur suivants peuvent être identifiés par le biais de vérifications de fichiers Sbomgen Docker :

- AWS clé d'accès IDs — `AKIAIOSFODNN7EXAMPLE`
- AWS clés secrètes — `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
- DockerHub jetons d'accès personnels — `dckr_pat_thisisa27charexample1234567`
- GitHub jetons d'accès personnels — `ghp_examplev61wY7Pj1YnotrealUoY123456789`
- GitLab jetons d'accès personnels — `glpat-12345example12345678`

### Conteneurs pour racines

> **Note**
>
> Le marqueur de gravité de cette vérification est Info.

Nous recommandons d'exécuter des conteneurs Docker sans privilèges root. Pour les charges de travail conteneurisées qui ne peuvent pas être exécutées sans les privilèges root, nous vous recommandons de créer vos applications selon le principe du minimum de privilèges. Pour plus d'informations, consultez la section Utilisateur sur le site Web de Docker Docs.

### Variables d'environnement affaiblissant l'exécution

> **Note**
>
> L'indice de sévérité de cette vérification est élevé.

Plusieurs utilitaires de ligne de commande ou environnements d'exécution de langage de programmation permettent de contourner les valeurs par défaut sécurisées, ce qui permet une exécution par le biais de méthodes non sécurisées.

NODE_TLS_REJECT_UNAUTHORIZED=0

Lorsque Node.js les processus s'exécutent avec la `NODE_TLS_REJECT_UNAUTHORIZED` valeur définie sur`0`, la validation du certificat TLS est désactivée. Pour plus d'informations, consultez NODE_TLS_REJECT_UNAUTHORIZED=0 sur le site Web Node.js.

GIT_SSL_NO_VERIFY=*

Lorsque les processus de ligne de commande git s'exécutent avec `GIT_SSL_NO_VERIFY` set, Git ignore la vérification des certificats TLS. Pour plus d'informations, consultez la section Variables d'environnement sur le site Web Git.

PIP_TRUSTED_HOST=*

Lorsque les processus de ligne de commande Python pip s'exécutent avec `PIP_TRUSTED_HOST` set, Pip ignore la vérification des certificats TLS sur le domaine spécifié. Pour plus d'informations, consultez --trusted-host sur le site Web de Pip.

NPM_CONFIG_STRICT_SSL=Faux

Lorsque les processus de ligne de commande Node.js npm s'exécutent avec la valeur `NPM_CONFIG_STRICT_SSL` définie sur false, l'utilitaire Node Package Manager (npm) se connecte au registre NPM sans valider les certificats TLS. Pour plus d'informations, consultez strict-ssl sur le site Web de npm Docs.

### Indicateurs de commande affaiblissant l'exécution

> **Note**
>
> L'indice de sévérité de cette vérification est élevé.

À l'instar des variables d'environnement qui affaiblissent le temps d'exécution, plusieurs utilitaires de ligne de commande ou environnements d'exécution de langage de programmation permettent de contourner les valeurs par défaut sécurisées, ce qui permet une exécution par le biais de méthodes non sécurisées.

**`npm --strict-ssl=false`**

Lorsque les processus de ligne de commande Node.js npm sont exécutés avec l'`--strict-ssl=false`indicateur, l'utilitaire Node Package Manager (npm) se connecte au registre NPM sans valider les certificats TLS. Pour plus d'informations, consultez strict-ssl sur le site Web de npm Docs.

**`apk --allow-untrusted`**

Lorsque l'Alpine Package Keeperutilitaire est exécuté avec l'`--allow-untrusted`indicateur, il `apk` installe des packages sans signature ou sans signature fiable. Pour plus d'informations, consultez le référentiel suivant sur le site Web d'Apline.

**`apt-get --allow-unauthenticated`**

Lorsque l'utilitaire de `apt-get` paquetage Debian est lancé avec l'`--allow-unauthenticated`indicateur, `apt-get` il ne vérifie pas la validité du paquet. Pour plus d'informations, consultez apt-get (8) sur le site web de Debian.

**`pip --trusted-host`**

Lorsque l'utilitaire Python pip est exécuté avec l'`--trusted-host`indicateur, le nom d'hôte spécifié ignore la validation du certificat TLS. Pour plus d'informations, consultez --trusted-host sur le site Web de Pip.

**`rpm --nodigest, --nosignature, --noverify, --nofiledigest`**

Lorsque le gestionnaire de packages basé sur le RPM `rpm` est exécuté avec les `--nofiledigest` indicateurs`--nodigest`,`--nosignature`, et`--noverify`, le gestionnaire de packages RPM ne valide pas les en-têtes, les signatures ou les fichiers du package lors de l'installation d'un package. Pour plus d'informations, consultez la page de manuel RPM suivante sur le site Web RPM.

**`yum-config-manager --setopt=sslverify false`**

Lorsque le gestionnaire de packages basé sur RPM `yum-config-manager` est exécuté avec l'`--setopt=sslverify`indicateur défini sur false, le gestionnaire de packages YUM ne valide pas les certificats TLS. Pour plus d'informations, consultez la page de manuel YUM suivante sur le site Web de Man7.

**`yum --nogpgcheck`**

Lorsque le gestionnaire de packages basé sur le RPM `yum` est exécuté avec l'`--nogpgcheck`indicateur, le gestionnaire de packages YUM ignore la vérification des signatures GPG sur les packages. Pour plus d'informations, consultez yum (8) sur le site Web de Man7.

**`curl --insecure, curl -k`**

Lorsqu'elle `curl` est exécutée avec l'`-k`indicateur `--insecure` ou, la validation du certificat TLS est désactivée. Par défaut, chaque connexion sécurisée établie est vérifiée avant le transfert. `curl` Cette option permet de `curl` sauter l'étape de vérification et de procéder sans vérification. Pour plus d'informations, consultez la page de manuel Curl suivante sur le site Web de Curl.

**`wget --no-check-certificate`**

Lorsqu'elle `wget` est exécutée avec l'`--no-check-certificate`indicateur, la validation du certificat TLS est désactivée. Pour plus d'informations, consultez la page de manuel Wget suivante sur le site Web de GNU.

# Contrôles de suppression des bases de données de packages de systèmes d'exploitation dans les conteneurs

> **Note**
>
> L'indice de gravité de cette vérification est Info.

La suppression d'une base de données de packages de système d'exploitation réduit la capacité de scanner l'inventaire complet du logiciel d'une image de conteneur. Ces bases de données doivent rester intactes pendant les étapes de création du conteneur.

Les contrôles de suppression d'une base de données de packages de système d'exploitation sont pris en charge par les gestionnaires de packages suivants :

Package Keeper (APK)

Les images de conteneur utilisant le gestionnaire de packages APK pour les logiciels installés doivent garantir que les fichiers système APK ne sont pas supprimés lors d'une compilation. Pour plus d'informations, consultez la documentation des fichiers système APK manpages sur le Arch Linux site Web.

Gestionnaire de paquets Debian (DPKG)

Les conteneurs utilisant le gestionnaire de paquets DPKG, tels que les images basées sur Debian, Ubuntu ou Distroless, doivent s'assurer que la base de données DPKG n'est pas supprimée lors de la construction d'un conteneur. Pour plus d'informations, consultez la documentation des fichiers système des pages de manuel de DPKG sur le Ubuntu site Web.

Gestionnaire de packages RPM (RPM)

Les conteneurs utilisant le RPM Package Manager (yum/dnf), tels qu'Amazon Linux ou Red Hat Enterprise Linux, doivent s'assurer que la base de données RPM n'est pas supprimée lors de la création d'un conteneur. Pour plus d'informations, consultez la documentation des fichiers système des pages de manuel RPM sur le site Web de RPM.

# Création d'une intégration de pipeline CI/CD personnalisée avec Amazon Inspector Scan

Nous vous recommandons d'utiliser les plug-ins Amazon Inspector CI/CD si le CI/CD plugins are available for your CI/CD solution. If the Amazon Inspector CI/CD plugins aren't available for your CI/CD solution, you can use a combination of the Amazon Inspector SBOM Generator and the Amazon Inspector Scan API to create a custom CI/CD integration. The following steps describe how to create a custom CI/CD pipeline Amazon Inspector est intégré à Amazon Inspector Scan.

> **Tip**
>
> Vous pouvez utiliser le générateur de SBOM d'Amazon Inspector (Sbomgen) pour ignorer les étapes 3 et 4 si vous souhaitez générer et scanner votre SBOM en une seule commande.

## Étape 1. Configuration Compte AWS

Configurez un Compte AWS qui donne accès à l'API Amazon Inspector Scan. Pour de plus amples informations, veuillez consulter Configuration d'un AWS compte pour utiliser l'intégration Amazon Inspector CI/CD.

## Étape 2. Installation du Sbomgen binaire

Installez et configurez le Sbomgen binaire. Pour de plus amples informations, veuillez consulter Installation de l'Sbomgen.

## Étape 3. Utiliser Sbomgen

Utilisez le Sbomgen pour créer un fichier SBOM pour une image de conteneur que vous souhaitez numériser.

Vous pouvez utiliser l'exemple suivant. *image:id*Remplacez-le par le nom de l'image que vous souhaitez numériser. *sbom_path.json*Remplacez-le par l'emplacement où vous souhaitez enregistrer la sortie SBOM.

exemple

```
./inspector-sbomgen container --image image:id -o sbom_path.json
```

## Étape 4 : Appel de l'API Amazon Inspector Scan

Appelez l'`inspector-scan`API pour analyser le SBOM généré et fournir un rapport de vulnérabilité.

Vous pouvez utiliser l'exemple suivant. Remplacez *`sbom_path.json`* par l'emplacement d'un fichier SBOM valide compatible avec CycloneDX. *`ENDPOINT`*Remplacez-le par le point de terminaison de l'API correspondant à l' Région AWS endroit où vous êtes actuellement authentifié. Remplacez *`REGION`* par la région correspondante.

exemple

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

Pour une liste complète des points de Régions AWS terminaison, voir Régions et points de terminaison.

## (Facultatif) Étape 5. Générez et scannez des SBOM en une seule commande

> **Note**
>
> Effectuez cette étape uniquement si vous avez ignoré les étapes 3 et 4.

Générez et scannez votre SBOM en une seule commande à l'aide du `--scan-bom` drapeau.

Vous pouvez utiliser l'exemple suivant. *`image:id`*Remplacez-le par le nom de l'image que vous souhaitez numériser. Remplacez *`profile`* par le profil correspondant. Remplacez *`REGION`* par la région correspondante. Remplacez */tmp/scan.json* par l'emplacement du fichier scan.json dans le répertoire tmp.

exemple

```
./inspector-sbomgen container --image image:id --scan-sbom --aws-profile
profile --aws-region REGION -o /tmp/scan.json
```

Pour une liste complète des points de Régions AWS terminaison, voir Régions et points de terminaison.

# 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. Avec le Jenkins plugin Amazon Inspector, vous pouvez ajouter des analyses de vulnérabilité Amazon Inspector à votre Jenkins pipeline. 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**
>
> N'ajoutez les informations d'identification du docker que 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 Jenkins 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. L'option automatique permet au plugin de télécharger la version la plus récente. Cela garantit également que vous disposez toujours des dernières fonctionnalités, mises à jour de sécurité et corrections de bogues.

   a. (Option 1) Choisissez Automatique pour télécharger la dernière version d'inspectors-sbomgen. Cette option détecte automatiquement le système d'exploitation et l'architecture du processeur actuellement utilisés.

   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) Dans le champ Nom de l'artefact du rapport, entrez un nom personnalisé pour les artefacts générés pendant le processus de création. Cela permet de les identifier et de les gérer de manière unique.

   d. (Facultatif) Pour Skip files, spécifiez un ou plusieurs répertoires que vous souhaitez exclure de l'analyse. Envisagez cette option pour les répertoires qui n'ont pas besoin d'être analysés en raison de leur taille.

   e. (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.

   f. (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/). *`AccountNumber`* *`RoleName`*

      ii. (Facultatif) Pour les informations d'identification AWS, spécifiez les AWS informations d'identification 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.

   g. (Facultatif) Sélectionnez Activer les seuils de vulnérabilité. Avec cette option, vous pouvez déterminer si votre build échoue si une vulnérabilité analysée dépasse une valeur. Si toutes les valeurs sont égales`0`, le build réussit, quel que soit le nombre de vulnérabilités analysées. Pour le score EPSS, la valeur peut être comprise entre 0 et 1. Si une vulnérabilité analysée dépasse une valeur, la génération échoue et toutes les vulnérabilités CVEs dont le score EPSS est supérieur à la valeur s'affichent dans la console.

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 SBOMGen déclaratif

- Pour ajouter Amazon Inspector Scan à une version, utilisez l'exemple de syntaxe suivant. En fonction de l'architecture de système d'exploitation que vous préférez pour le téléchargement d'Amazon Inspector SBOM Generator, remplacez-le par *SBOMGEN_SOURCE* LinuxAMD64 ou LinuxARM64. Remplacez-le *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 SBOMGen déclaratif

- Pour ajouter Amazon Inspector Scan à une version, utilisez l'exemple de syntaxe suivant. *SBOMGEN_PATH*Remplacez-le 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 Docker d'identification si vous utilisez un référentiel privé. Vous pouvez éventuellement activer les seuils de vulnérabilité et spécifier des valeurs pour chaque gravité.

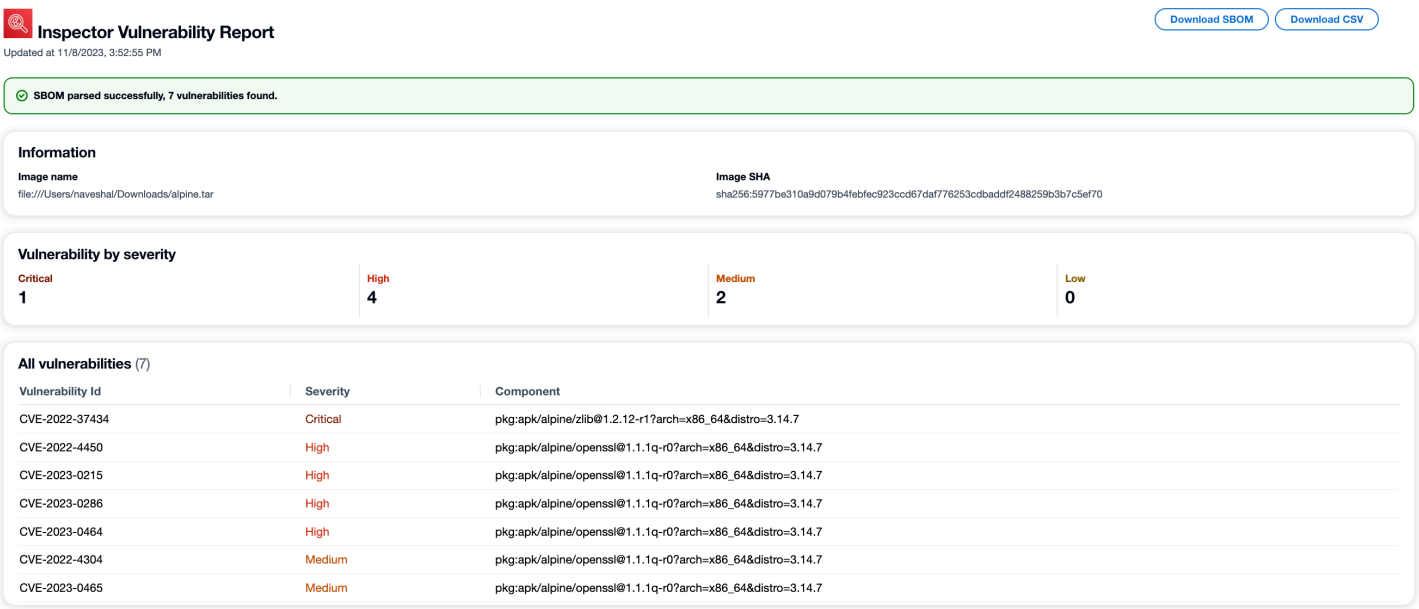
> **Note**
>
> SbomgenPlacez-le dans le répertoire Jenkins et fournissez le chemin d'accès au répertoire Jenkins dans le plugin (tel que*/opt/folder/arm64/inspector-sbomgen*).

```
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`.

## Impossible de charger l'image à partir de sources tarball, locales ou distantes

Erreur :

```
2024/10/16 02:25:17 [ImageDownloadFailed]: failed to load image from tarball, local, or remote sources.
```

> **Note**
>
> Cette erreur peut se produire si le plug-in Jenkins ne peut pas lire l'image du conteneur, si l'image du conteneur n'est pas trouvée dans le Docker moteur et si l'image du conteneur n'est pas trouvée dans le registre de conteneurs distant.

Résolution :

Vérifiez les points suivants :

- L'utilisateur du plugin Jenkins dispose d'autorisations de lecture pour l'image que vous souhaitez numériser.
- L'image que vous souhaitez numériser est présente dans le Docker moteur.
- L'URL de votre image distante est correcte.
- Vous êtes authentifié auprès du registre distant (le cas échéant).

## 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 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. Avec le TeamCity plugin Amazon Inspector, vous pouvez ajouter des analyses de vulnérabilité Amazon Inspector à votre TeamCity pipeline. 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 TeamCity plugin Amazon Inspector TeamCity sur le site de vente au https://plugins.jetbrains.com/plugin/23236- amazon-inspector-scanner. Pour plus d'informations sur la façon d'intégrer Amazon Inspector Scan dans votre pipeline CI/CD, consultez la section Intégration des scans Amazon Inspector dans votre pipeline CI/CD. Pour obtenir la liste des systèmes d'exploitation et des langages de programmation pris en charge par Amazon Inspector, consultez Systèmes d'exploitation et langages de programmation pris en charge. Les étapes suivantes décrivent comment 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 deSbomgen.

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.

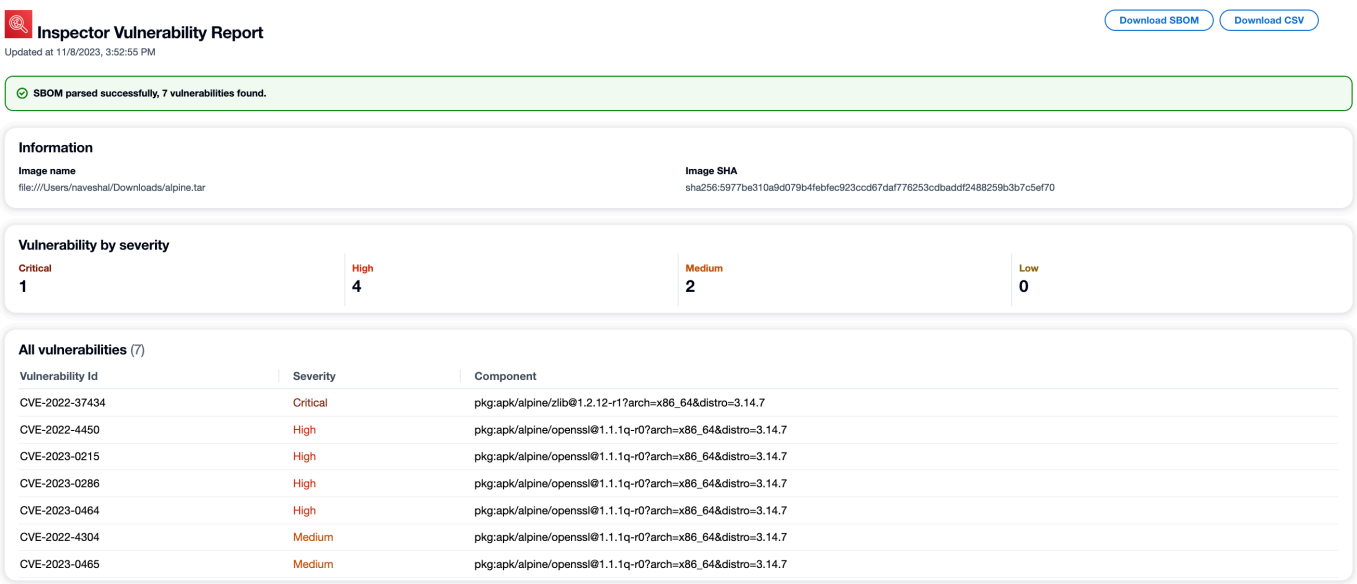
- (Facultatif) Pour l'authentification Docker, entrez votre nom d'utilisateur Docker et votre mot de passe Docker. Procédez ainsi uniquement si l'image de votre conteneur se trouve dans un dépôt privé.
- (Facultatif) Pour AWS l'authentification, entrez l'ID de votre clé d' AWS accès et votre clé AWS 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 :




# Utilisation d'Amazon Inspector avec des GitHub actions

Vous pouvez utiliser Amazon Inspector GitHub actionspour ajouter des analyses de vulnérabilité Amazon Inspector à vos GitHub flux de travail. Cela utilise le générateur Amazon Inspector SBOM

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 de vulnérabilité d'Amazon Inspector peuvent être configurées pour réussir ou échouer les flux de travail en fonction du nombre et de la gravité des vulnérabilités détectées. Vous pouvez consulter la dernière version de l'action Amazon Inspector sur le GitHubsite Web. Pour plus d'informations sur la façon d'intégrer Amazon Inspector Scan dans votre pipeline CI/CD, consultez la section Intégration des scans Amazon Inspector dans votre pipeline CI/CD. Pour obtenir la liste des systèmes d'exploitation et des langages de programmation pris en charge par Amazon Inspector, consultez Systèmes d'exploitation et langages de programmation pris en charge.

## Utilisation d'Amazon Inspector avec des GitLab composants

Vous pouvez utiliser Amazon Inspector avec des composants GitLab CI/CD pour ajouter des analyses de vulnérabilité Amazon Inspector à vos GitLab projets. Cela utilise le générateur Amazon Inspector SBOM 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 de vulnérabilité d'Amazon Inspector peuvent être configurées pour réussir ou échouer les flux de travail en fonction du nombre et de la gravité des vulnérabilités détectées. Vous pouvez consulter la dernière version du composant Amazon Inspector sur le GitLabsite Web. Pour plus d'informations sur la façon d'intégrer Amazon Inspector Scan dans votre pipeline CI/CD, consultez la section Intégration des scans Amazon Inspector dans votre pipeline CI/CD. Pour obtenir la liste des systèmes d'exploitation et des langages de programmation pris en charge par Amazon Inspector, consultez Systèmes d'exploitation et langages de programmation pris en charge.

## Utilisation d'CodeCatalystactions avec Amazon Inspector

Vous pouvez utiliser Amazon Inspector avec Amazon CodeCatalyst pour ajouter des analyses de vulnérabilité Amazon Inspector à vos CodeCatalyst flux de travail. Cela utilise le générateur Amazon Inspector SBOM 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 de vulnérabilité d'Amazon Inspector peuvent être configurées pour réussir ou échouer les flux de travail en fonction du nombre et de la gravité des vulnérabilités détectées. Pour plus d'informations sur la façon d'intégrer Amazon Inspector Scan dans votre pipeline CI/CD, consultez la section Intégration des scans Amazon Inspector dans votre pipeline CI/CD. Pour obtenir la liste des systèmes d'exploitation et des langages de programmation pris en charge par Amazon Inspector, consultez Systèmes d'exploitation et langages de programmation pris en charge.

# Utilisation des actions de scan d'Amazon Inspector avec CodePipeline

Vous pouvez utiliser Amazon Inspector AWS CodePipeline en ajoutant des analyses de vulnérabilité à vos flux de travail. Cette intégration tire parti du générateur Amazon Inspector SBOM et de l'API Amazon Inspector Scan pour produire des rapports détaillés à la fin de votre build. L'intégration vous aide à étudier et à corriger les risques avant le déploiement. Il s'agit `InspectorScan` d'une action de calcul géré CodePipeline qui automatise la détection et la correction des failles de sécurité dans votre code open source. Vous pouvez utiliser cette action avec le code source de l'application dans votre référentiel tiers, tel que GitHub Bitbucket Cloud, ou avec des images pour des applications de conteneur. Pour plus d'informations, voir la référence InspectorScan à l'action d'appel dans le guide de AWS CodePipeline l'utilisateur.

# Évaluation de la couverture de votre AWS environnement par Amazon Inspector

Vous pouvez évaluer la couverture de votre AWS environnement par Amazon Inspector depuis l'écran de gestion des comptes de la console Amazon Inspector, qui affiche des détails et des statistiques sur le statut des scans effectués par Amazon Inspector pour vos comptes et vos ressources.

> **Note**
>
> Si vous êtes l'administrateur délégué d'une organisation, vous pouvez consulter les détails et les statistiques de tous les comptes de l'organisation.

La procédure suivante explique comment évaluer la couverture de votre environnement Amazon Inspector.

Pour évaluer la couverture de votre AWS environnement par Amazon Inspector

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Gestion des comptes.
3. Pour consulter la couverture, sélectionnez l'un des onglets suivants :

   - Choisissez Comptes pour consulter la couverture au niveau du compte.
   - Choisissez Instances pour vérifier la couverture des instances Amazon Elastic Compute Cloud (Amazon EC2).
   - Choisissez Container repositories pour vérifier la couverture des référentiels Amazon Elastic Container Registry (Amazon ECR).
   - Choisissez Images de conteneurs pour vérifier la couverture des images de conteneurs Amazon ECR.
   - Choisissez les fonctions Lambda pour vérifier la couverture des fonctions Lambda.

Les rubriques suivantes décrivent les informations fournies par chacun de ces onglets.

Rubriques

# 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 de plus amples informations, veuillez consulter Types de scan automatisés dans 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 de plus amples informations, veuillez consulter Activation des scans Amazon Inspector pour les comptes membres.

# Évaluation de la couverture des EC2 instances Amazon

L'onglet Instances affiche EC2 les instances Amazon de 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 EC2 instance 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 EC2 instances 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 de plus amples informations, veuillez consulter Numérisation des EC2 instances Amazon.

Dans chaque onglet, la colonne Compte Compte AWS indique le propriétaire d'une instance.

EC2 balises d'instance : 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 EC2 instance, cliquez sur le lien dans la colonne EC2 instance. 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, consultezAfficher les informations relatives aux résultats de vos recherches sur Amazon Inspector.

## Numérisation des valeurs d'état pour les EC2 instances Amazon

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.

- Limite de stockage d'instance sans agent dépassée : Amazon Inspector utilise ce statut lorsque la taille combinée de tous les volumes attachés à une instance est supérieure à 1 200 Go ou lorsque plus de 8 volumes sont attachés à une instance.
- Le délai de collecte des instances sans agent est dépassé : Amazon Inspector expire pendant la tentative d'exécution d'un scan sans agent sur une instance.
- EC2 instance 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.
- EC2 Instance non gérée : Amazon Inspector ne surveille ni ne scanne l'instance. L'instance n'est pas gérée par AWS Systems Manager.

  Pour remédier à ce problème, vous pouvez utiliser 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, consultezValeurs de statut des EC2 instances Amazon.
- Surveillance active avec erreurs partielles : cet état indique que le EC2 scan est actif, mais que des erreurs y sont associéesInspection approfondie d'Amazon Inspector pour les instances Amazon basées sur Linux 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 d'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 un scan en attente. Toutefois, si ce statut persiste après 6 heures, utilisez Amazon EC2 Systems Manager pour vous assurer que les associations Amazon Inspector requises existent et sont en cours d'exécution pour l'instance.

Pour plus de détails sur la configuration des paramètres de numérisation pour une EC2 instance, consultezNumérisation des EC2 instances Amazon.

# 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 nouvelle numérisation Amazon 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 nouvelle analyse d'Amazon 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 de plus amples informations, veuillez consulter 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, consultezAfficher les informations relatives aux résultats de vos recherches sur Amazon Inspector.

## 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 : numérisation Amazon ECR avec Amazon Inspector. 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 de plus amples informations, veuillez consulter Fonctions Lambda 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 de plus amples informations, veuillez consulter 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 (CVEs) 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 activation 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.

# Gérer plusieurs comptes dans Amazon Inspector avec AWS Organizations

Vous pouvez utiliser Amazon Inspector pour gérer plusieurs comptes au sein d'une organisation. Pour ce faire, vous devez activer Amazon Inspector avec le compte AWS Organizations de gestion et spécifier un administrateur délégué. L'administrateur délégué gère Amazon Inspector pour une organisation et peut effectuer des tâches pour le compte de l'organisation. Les rubriques suivantes décrivent la différence entre un compte d'administrateur délégué et un compte de membre, comment désigner et supprimer un administrateur délégué, et comment gérer les comptes de membres.

Rubriques



## Comprendre le compte administrateur délégué et le compte membre dans Amazon Inspector

Lorsque vous utilisez Amazon Inspector dans un environnement multi-comptes, le compte d'administrateur délégué a accès à des métadonnées spécifiques. Les métadonnées incluent le scan standard pour Amazon EC2, Amazon ECR et Lambda, ainsi que le scan du code Lambda. Il inclut également les résultats des recherches de sécurité pour les comptes des membres. Cette section fournit des informations sur les actions que le compte d'administrateur délégué peut effectuer et les comptes de membre peuvent effectuer.

### 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 :

- Seul le compte AWS Organizations de gestion peut désigner et supprimer un administrateur délégué.
- Lorsque vous désignez un administrateur délégué, vous devez appartenir à la même organisation que les comptes de membres que vous souhaitez gérer.

- 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 EC2 qui seront utilisés pour 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 SBOMs pour tous les comptes membres de l'organisation.
- Définissez le mode de EC2 scan Amazon pour tous les comptes membres de l'organisation. Pour de plus amples informations, veuillez consulter 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 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 toutes SBOMs 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 compte d'administrateur délégué pour Amazon Inspector

L'administrateur délégué est un compte qui gère un service pour une organisation. Cette rubrique explique comment désigner un administrateur délégué pour Amazon Inspector.

## Considérations

Avant de désigner un administrateur délégué, prenez note des points suivants :

L'administrateur délégué peut gérer un maximum de 10 000 membres.

- Si vous dépassez les 10 000 comptes membres, vous recevez une notification via le Amazon CloudWatch Personal Health Dashboard et un e-mail envoyé au compte administrateur délégué.

L'administrateur délégué est régional.

- Amazon Inspector est un service régional. Vous devez répéter les étapes de la procédure partout Région AWS où vous prévoyez d'utiliser Amazon Inspector.

Une organisation ne peut avoir qu'un seul administrateur délégué.

- Si vous désignez un compte comme administrateur délégué dans l'un d' Région AWS entre eux, ce compte doit être l'administrateur délégué dans tous les autres Régions AWS.

Le changement d'administrateur délégué ne désactive pas Amazon Inspector pour les comptes des membres.

- Si vous supprimez un administrateur délégué, les comptes des membres deviennent des comptes autonomes et les paramètres de scan ne sont pas affectés.

Toutes les fonctionnalités de votre AWS organisation doivent être activées.

- Il s'agit du paramètre par défaut pour AWS 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 la déclaration suivante à la fin de votre politique IAM pour accorder ces autorisations. Pour plus d'informations, consultez la section Gestion des politiques IAM.

```
{
    "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 décrit comment désigner un administrateur délégué pour votre organisation. Avant de terminer la procédure, assurez-vous que vous appartenez à la même organisation que les comptes de membres que vous souhaitez confier à l'administrateur délégué.

> **Note**
>
> Vous devez utiliser le compte AWS Organizations de gestion pour effectuer cette procédure. Seul le compte AWS Organizations de gestion peut désigner un administrateur délégué. Des autorisations peuvent être nécessaires pour désigner un administrateur délégué. Pour de plus amples informations, veuillez consulter Autorisations requises pour désigner un administrateur délégué.

Lorsque vous activez Amazon Inspector pour la première fois, Amazon Inspector crée le rôle lié au service `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

### Console

Pour désigner un administrateur délégué pour Amazon Inspector

1. Connectez-vous au compte de AWS Organizations gestion, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le Région AWS sélecteur pour spécifier l' Région AWS endroit où vous souhaitez désigner l'administrateur délégué.
3. Dans le volet de navigation, sélectionnez Paramètres généraux.
4. Sous Administrateur délégué, entrez l'identifiant à 12 chiffres de celui que Compte AWS vous souhaitez désigner comme administrateur délégué.
5. Choisissez Déléguer, puis sélectionnez à nouveau Déléguer.

Lorsque vous désignez un administrateur délégué, tous les types de scan sont activés par défaut pour le compte. Si vous souhaitez activer Amazon Inspector pour le compte AWS Organizations de gestion, procédez comme suit.

Pour activer Amazon Inspector pour le compte AWS Organizations de gestion

1. Connectez-vous au compte d'administrateur délégué, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Dans le volet de navigation, sélectionnez Gestion des comptes.
3. Sous Comptes, sélectionnez le compte AWS Organizations de gestion, puis sélectionnez Activer.
4. Sélectionnez les types de scan que vous souhaitez activer pour le compte AWS Organizations de gestion, puis choisissez Soumettre.

### 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.

## Activation des scans Amazon Inspector pour les comptes membres

Si vous êtes l'administrateur délégué d'une organisation, vous pouvez activer Amazon et EC2 Amazon ECR pour les comptes des membres de l'organisation. Une fois que vous avez activé la recherche d'un compte membre, Amazon Inspector est automatiquement activé pour ce compte, et le compte est associé au compte d'administrateur délégué. Pour plus d'informations sur les types de numérisation Amazon Inspector, consultezTypes de scan automatisés dans Amazon Inspector. Cette section décrit comment activer l'analyse des comptes des membres.

### Activer l'analyse des comptes des membres

Vous pouvez activer l'analyse des comptes des membres de différentes manières. Les procédures suivantes décrivent comment activer le scan pour tous les comptes de membre et pour des comptes de membre spécifiques en tant qu'administrateur délégué, ainsi que comment activer le scan en tant que compte de membre.

Pour activer automatiquement le scan de tous les comptes membres

1. Connectez-vous à l'aide des informations d'identification du compte administrateur délégué, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le sélecteur de région pour choisir l' Région AWS endroit où vous souhaitez activer le scan pour tous les comptes membres.
3. Dans le volet de navigation, sélectionnez Gestion des comptes. L'onglet Comptes affiche tous les comptes membres associés au compte AWS Organizations de gestion.
4. Sous Organisation, cochez la case à côté du numéro de compte. Choisissez ensuite Activer pour sélectionner les options de numérisation que vous souhaitez appliquer aux comptes des membres. Vous pouvez sélectionner les types de numérisation suivants :

   - EC2 Numérisation Amazon
   - Numérisation Amazon ECR
   - Numérisation standard Lambda

- Analyse du code Lambda

- Après avoir sélectionné vos types de numérisation préférés, choisissez Enregistrer.

> **Note**
>
> Si vous avez plusieurs pages de comptes, vous devez répéter cette étape sur chaque page. Vous pouvez choisir l'icône représentant une roue dentée pour modifier le nombre de comptes affichés sur chaque page.

5. Activez le paramètre Activer automatiquement l'Inspecteur pour les nouveaux comptes membres et sélectionnez les options d'analyse que vous souhaitez appliquer aux nouveaux comptes membres ajoutés à votre organisation. Vous pouvez sélectionner les types de numérisation suivants :

   - EC2 Numérisation Amazon
   - Numérisation Amazon ECR
   - Numérisation standard Lambda
   - Analyse du code Lambda

   - Après avoir sélectionné vos types de numérisation préférés, choisissez Activer.

   > **Note**
   >
   > Le paramètre Activer automatiquement l'inspecteur pour les nouveaux comptes membres active Amazon Inspector pour tous les futurs membres de votre organisation. Si le nombre de comptes de membres est supérieur à 5 000, ce paramètre est automatiquement désactivé. Si le nombre total de comptes de membres diminue à moins de 5 000, le paramètre est automatiquement réactivé.

6. (Recommandé) Répétez chacune de ces étapes pour chaque fois Région AWS que vous souhaitez activer l'analyse des comptes des membres.

Pour activer la numérisation de comptes de membres spécifiques

1. Connectez-vous à l'aide des informations d'identification du compte administrateur délégué, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le sélecteur de région pour choisir l' Région AWS endroit où vous souhaitez activer le scan pour tous les comptes membres.
3. Dans le volet de navigation, sélectionnez Gestion des comptes. L'onglet Comptes affiche tous les comptes membres associés au compte AWS Organizations de gestion.
4. Sous Organisation, cochez la case à côté de chaque numéro de compte membre dont vous souhaitez activer la recherche. Choisissez ensuite Activer pour sélectionner les options de numérisation que vous souhaitez appliquer aux comptes des membres. Vous pouvez sélectionner les types de numérisation suivants :

   - EC2 Numérisation Amazon
   - Numérisation Amazon ECR
   - Numérisation standard Lambda
   - Analyse du code Lambda

   - Après avoir sélectionné vos types de numérisation préférés, choisissez Enregistrer.

   > **Note**
   >
   > Si vous avez plusieurs pages de comptes, vous devez répéter cette étape sur chaque page. Vous pouvez choisir l'icône représentant une roue dentée pour modifier le nombre de comptes affichés sur chaque page.

5. (Recommandé) Répétez chacune de ces étapes pour chaque fois Région AWS que vous souhaitez activer le scan pour des membres spécifiques.

Pour activer le scan en tant que compte membre

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le sélecteur de région pour choisir l' Région AWS endroit où vous souhaitez activer le scan pour tous les comptes membres.

3. Dans le volet de navigation, sélectionnez Gestion des comptes. L'onglet Comptes affiche tous les comptes membres associés au compte AWS Organizations de gestion.
4. Sous Organisation, cochez la case à côté de votre numéro de compte. Choisissez ensuite Activer pour sélectionner les options de numérisation que vous souhaitez appliquer. Vous pouvez sélectionner les types de numérisation suivants :

   - EC2 Numérisation Amazon
   - Numérisation Amazon ECR
   - Numérisation standard Lambda
   - Analyse du code Lambda

   - Après avoir sélectionné vos types de numérisation préférés, choisissez Enregistrer.
5. (Recommandé) Répétez ces étapes dans chaque région où vous souhaitez activer le scan pour votre compte de membre.

> **Note**
>
> Si votre compte AWS Organizations de gestion possède un compte d'administrateur délégué pour Amazon Inspector, vous pouvez activer votre compte en tant que compte membre pour consulter les détails du scan.

## Dissociation des comptes membres dans Amazon Inspector

En tant qu'administrateur délégué, vous devrez peut-être dissocier un compte membre du vôtre. Lorsque vous dissociez un compte membre, Amazon Inspector est toujours activé dans le compte et le compte devient un compte autonome. Vous n'êtes également plus autorisé à gérer Amazon Inspector pour le compte. Cependant, vous pouvez associer à tout moment des comptes de membres précédemment dissociés à votre compte. Cette section décrit comment dissocier les comptes des membres en tant qu'administrateur délégué.

Console

Pour dissocier les comptes des membres à l'aide de la console

1. Connectez-vous à l'aide des informations d'identification du compte administrateur délégué, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home
2. Utilisez le sélecteur de région pour choisir l' Région AWS endroit où vous souhaitez dissocier les comptes des membres.
3. Dans le volet de navigation, sélectionnez Gestion des comptes.
4. Sous Organisation, cochez la case à côté de chaque numéro de compte que vous souhaitez dissocier.
5. Choisissez le menu Actions, puis Dissocier le compte.

API

Pour dissocier les comptes des membres à l'aide de l'API

Exécutez l'opération DisassociateMemberAPI. Dans la demande, indiquez le compte IDs que vous souhaitez dissocier.

## Supprimer l'administrateur délégué dans Amazon Inspector

Vous devrez peut-être supprimer le compte d'administrateur délégué Amazon Inspector. Vous pouvez le faire depuis le compte AWS Organizations de gestion. Lorsque vous supprimez le compte d'administrateur délégué Amazon Inspector, Amazon Inspector est toujours activé sur le compte et sur tous ses comptes membres. Le compte d'administrateur délégué et tous ses comptes de membre deviennent des comptes autonomes et conservent leurs paramètres de numérisation d'origine. Cette section décrit comment supprimer le compte d'administrateur délégué.

### Supprimer l'administrateur délégué Amazon Inspector

Les procédures suivantes décrivent comment supprimer l'administrateur délégué Amazon Inspector et comment associer des comptes de membres au compte d'administrateur délégué.

Pour plus d'informations sur la façon d'attribuer un administrateur délégué Amazon Inspector, consultez Désigner un compte d'administrateur délégué pour Amazon Inspector.

> **Note**
>
> Une fois que vous avez désigné un administrateur délégué Amazon Inspector, celui-ci doit associer les comptes des membres manuellement.

Pour supprimer l'administrateur délégué

1. Connectez-vous à l' AWS Management Console aide du compte AWS Organizations de gestion.
2. Ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
3. Utilisez le sélecteur de région pour choisir l' Région AWS endroit où vous souhaitez supprimer l'administrateur délégué.
4. Dans le volet de navigation, sélectionnez Paramètres généraux.
5. Sous Administrateur délégué, choisissez Supprimer, puis confirmez votre action.

Pour associer des membres à un nouvel administrateur délégué

1. Connectez-vous à l'aide des informations d'identification du compte administrateur délégué, puis ouvrez la console Amazon Inspector sur https://console.aws.amazon.com/inspector/v2/home.
2. Utilisez le sélecteur de région pour choisir l' Région AWS endroit où vous souhaitez associer les membres.
3. Dans le volet de navigation, sélectionnez Gestion des comptes.
4. Sous Organisation, cochez la case à côté du numéro de compte.
5. Choisissez Actions, puis Add member (Ajouter un membre).

# Marquage des ressources Amazon Inspector

Une étiquette est une étiquette que vous ajoutez à une AWS ressource. Les balises vous aident à classer les AWS ressources en fonction de critères spécifiques. Les balises sont constituées d'une paire clé-valeur. La clé du tag est une étiquette générale. La valeur du tag est une description de la clé du tag. Amazon Inspector vous permet de définir des règles de suppression de balises et des configurations de scan CIS. Vous pouvez ajouter jusqu'à 50 balises à chacune de vos ressources Amazon Inspector.

## Principes fondamentaux du balisage

Une balise est constituée d'une paire clé-valeur. La clé du tag est une étiquette générale. La valeur du tag est une description de la clé du tag. Cette rubrique décrit les principes fondamentaux du balisage des ressources Amazon Inspector. Lorsque vous balisez des ressources Amazon Inspector, tenez compte des points suivants :

- Vous pouvez étiqueter les règles de suppression et les configurations de scan CIS.
- Vous pouvez ajouter jusqu'à 50 balises à chacune de vos ressources Amazon Inspector.
- Les clés de tag doivent être uniques.
- Une clé de balise ne peut avoir qu'une seule valeur de balise.
- Les clés de balise et les valeurs de balise peuvent comporter un maximum de 128 caractères UTF-8. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : `_ . : / = + -@`.
- Vous ne pouvez pas utiliser le `aws` préfixe dans aucune de vos balises ni modifier les balises avec ce préfixe. Les balises avec le `aws` préfixe sont réservées à l'usage de AWS.
- Les balises attribuées à une ressource Amazon Inspector ne sont disponibles que dans votre AWS compte et dans l' Région AWS endroit où vous les avez créées.
- Lorsque vous supprimez une ressource, toutes les balises qui lui sont associées sont également supprimées.

Pour plus d'informations sur les balises, consultez la section Meilleures pratiques et stratégies du Guide de l'utilisateur AWS des ressources de balisage et de l'éditeur de balises.

> **Note**
>
> Les balises ne sont pas destinées à stocker des informations confidentielles ou sensibles. N'utilisez jamais de balises pour stocker ce type de données. Les tags peuvent être accessibles depuis d'autres AWS services.

# Ajout de balises

Vous pouvez ajouter des balises aux ressources Amazon Inspector. Ces ressources incluent les règles de suppression et les configurations de scan CIS. Les balises vous aident à classer les AWS ressources en fonction de critères spécifiques. Cette rubrique explique comment ajouter des balises aux ressources Amazon Inspector.

## Ajouter des balises aux ressources Amazon Inspector

Vous pouvez étiqueter les règles de suppression et les configurations de scan CIS. Les procédures suivantes décrivent comment ajouter des balises dans la console et avec l'API Amazon Inspector.

### Ajouter des tags dans la console

Vous pouvez ajouter des balises aux ressources Amazon Inspector dans la console.

Ajouter des balises aux règles de suppression

Vous pouvez ajouter des balises aux règles de suppression lors de la création. Pour plus d'informations, consultez la section Création d'une règle de suppression.

Vous pouvez également modifier une règle de suppression pour inclure des balises. Pour plus d'informations, consultez la section Modification d'une règle de suppression.

Ajouter des balises à une configuration de scan CIS

Vous pouvez ajouter des balises à une configuration de scan CIS lors de sa création. Pour plus d'informations, consultez la section Création d'une configuration de scan CIS.

Vous pouvez également modifier une configuration de scan CIS pour inclure des balises. Pour plus d'informations, consultez la section Modification d'une configuration de scan CIS.

## Ajouter des balises à l'aide de l'API Amazon Inspector

Vous pouvez ajouter des balises aux ressources Amazon Inspector à l'aide de l'API Amazon Inspector.

### Ajouter des balises aux ressources Amazon Inspector

Utilisez l'`TagResource`API pour ajouter des balises aux ressources Amazon Inspector. Vous devez inclure l'ARN de la ressource et la paire clé-valeur de la balise dans la commande. L'exemple de commande suivant utilise un ARN de ressource vide comme filtre de suppression. La clé est `CostAllocation` et la valeur est`dev`. Pour plus d'informations sur les types de ressources pour Amazon Inspector, consultez la section Actions, ressources et clés de condition pour Amazon Inspector2 dans le Service Authorization Reference.

```
aws inspector2 tag-resource \
--resource-arn "arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/
filter/${FilterId}" \
--tags CostAllocation=dev \
--region us-west-2
```

### Ajout de balises aux règles de suppression lors de la création

Utilisez l'`CreateFilter`API pour ajouter des balises à une règle de suppression lors de sa création.

```
aws inspector2 create-filter \
--name "ExampleSuppressionRuleECR" \
--action SUPPRESS \
--filter-criteria 'resourceType=[{comparison="EQUALS", value="AWS_ECR_IMAGE"}]' \
--tags Owner=ApplicationSecurity \
--region us-west-2
```

### Ajouter des balises à une configuration de scan CIS

Utilisez l'`CreateCisScanConfiguration`API pour ajouter une balise à une configuration de scan CIS.

```
aws inspector2 create-cis-scan-configuration \
--scan-name "CreateConfigWithTagsSample" \
--security-level LEVEL_2 \
--targets accountIds=SELF,targetResourceTags={InspectorCisScan=True} \
--schedule 'daily={startTime={timeOfDay=11:10,timezone=UTC}}' \
```

```
--tags Owner=SecurityEngineering \
--region us-west-2
```

# Suppression de balises

Vous pouvez supprimer des balises des ressources Amazon Inspector. Ces ressources incluent les règles de suppression et les configurations de scan CIS. Les balises vous aident à classer les AWS ressources en fonction de critères spécifiques. Cette rubrique explique comment supprimer des balises des ressources Amazon Inspector.

## Supprimer des balises des ressources Amazon Inspector

Vous pouvez supprimer des balises des règles de suppression et des configurations de scan CIS. Les procédures suivantes décrivent comment supprimer des balises dans la console et à l'aide de l'API Amazon Inspector.

### Supprimer des tags dans la console

Vous pouvez supprimer des balises des ressources Amazon Inspector dans la console.

Supprimer les balises des règles de suppression

Vous pouvez supprimer un tag d'une règle de suppression en modifiant la règle de suppression pour ne plus inclure le tag. Pour plus d'informations, consultez la section Modification d'une règle de suppression.

Supprimer des balises d'une configuration de scan CIS

Vous pouvez supprimer une balise d'une configuration de scan CIS en modifiant la configuration de scan CIS pour ne plus inclure la balise. Pour plus d'informations, consultez la section Modification d'une configuration de scan CIS.

### Supprimer des balises à l'aide de l'API Amazon Inspector

Vous pouvez supprimer une balise d'une ressource Amazon Inspector à l'aide de l'API Amazon Inspector.

Supprimer des balises des ressources Amazon Inspector

Utilisez l'`UntagResource`API pour supprimer les balises des ressources Amazon Inspector.

L'extrait suivant montre comment supprimer une balise d'une ressource Amazon Inspector à l'aide de. `UntagResource` Vous devez inclure l'ARN de la ressource et la clé pour le tag dans la commande. L'exemple suivant utilise un ARN de ressource vide comme filtre de suppression. La clé est `CostAllocation`. Pour plus d'informations sur les types de ressources pour Amazon Inspector, consultez la section Actions, ressources et clés de condition pour Amazon Inspector2 dans le Service Authorization Reference.

```
aws inspector2 untag-resource \
--resource-arn "arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}" \
--tag-keys CostAllocation \
--region us-west-2
```

# Surveillance de l'utilisation et des coûts dans Amazon Inspector

Vous pouvez utiliser la console et l'API Amazon Inspector pour prévoir les coûts mensuels d'Amazon Inspector pour votre environnement. Si vous êtes l'administrateur Amazon Inspector d'un environnement à comptes multiples, vous pouvez consulter le coût total de votre environnement et les statistiques de coûts pour tous les comptes membres. Cette section explique comment accéder aux statistiques d'utilisation et calculer les coûts d'utilisation.

## 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. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 :

EC2 Numérisation Amazon

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 à EC2 analyser. 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 Amazon EC2 Scanning, il s'agit du nombre total d'heures pendant lesquelles Amazon Amazon Inspector a fourni une couverture active pour chaque EC2 instance d'un compte au cours des 30 derniers jours. Par exemple, les EC2 heures de couverture sont les heures entre le moment où Amazon Inspector a découvert l'instance et celui où elle est résiliée ou arrêtée, ou jusqu'à ce qu'elle soit 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 :
  - EC2 numérisation : le coût reflète le nombre moyen d' EC2 instances 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

Dans Amazon Inspector, chaque type de scan fait l'objet d'un suivi gratuit. Lorsque vous activez un type de scan, vous vous inscrivez automatiquement à un essai gratuit de 15 jours pour ce type de scan. Une fois que l'essai gratuit commence, il expire automatiquement dans 15 jours, même si vous désactivez le type de scan.

> **Note**
>
> L'essai gratuit ne s'applique pas à la numérisation CIS.

# 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 plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- 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 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Amazon Inspector ou une autre entreprise

Services AWS à l'aide de la console AWS CLI, de l'API ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez 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

Par défaut, Amazon Inspector stocke les données au repos à l'aide de solutions de AWS chiffrement. Amazon Inspector chiffre les données, telles que les suivantes :

- Inventaire des ressources collecté avec AWS Systems Manager.
- Inventaire des ressources analysé à partir des images d'Amazon Elastic Container Registry
- Résultats de sécurité générés à l'aide de clés de chiffrement AWS détenues par AWS Key Management Service

Vous ne pouvez pas gérer, utiliser ou consulter les clés AWS détenues. Cependant, il n'est pas nécessaire de prendre des mesures ou de modifier les programmes 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 à la recherche de 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 annulée 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 du. AWS KMS APIs 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 tentez 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. AWS Systems Manager collecte des données de télémétrie à partir d' EC2 instances appartenant au client auxquelles il les envoie AWS via un canal protégé par le protocole TLS (Transport Layer Security) à des fins d'évaluation. 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. Pour plus d'informations, consultez la section Protection des données dans Systems Manager pour comprendre comment SSM chiffre les données en transit.

## 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

- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment Amazon Inspector fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour Amazon Inspector
- AWS politiques gérées pour Amazon Inspector
- Utilisation de rôles liés à un service pour Amazon Inspector
- Résolution des problèmes d'identité et d'accès à Amazon Inspector

## 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 la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS  Signature Version 4 pour les demandes 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 plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center  et Authentification multifactorielle AWS dans IAM 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 racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine 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 une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des 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 d'effectuer une rotation des 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 nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les 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 plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM 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. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). 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 Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez 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 Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de 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 EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

# Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

## Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. 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 (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

### Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur

l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule 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 (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) 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 Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

## Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

# Comment Amazon 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

| Fonctionnalité 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 |
| ACLs | 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, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. 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 intercompte 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 Accès intercompte aux ressources dans IAM 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 politique 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 auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Amazon Inspector et leurs caractéristiques ARNs, 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

## ACLs dans Amazon Inspector

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des

entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

## Utilisation d'informations d'identification temporaires avec 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 Passage d'un rôle utilisateur à un rôle IAM (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 sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

## Rôles de service pour Amazon Inspector

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de 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 aux services : 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 IAM (console) 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 ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Inspector dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Amazon Inspector
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Autoriser l'accès en lecture seule à toutes les ressources Amazon Inspector
- Autoriser un accès complet à toutes les ressources Amazon Inspector

### 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 par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez 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 d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez 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 l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM 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 politiques avec 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec 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 politique 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 politique.

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 propres 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 de l'autorisation

Cette politique inclut les autorisations suivantes.

- `inspector2`— Permet un accès complet aux fonctionnalités d'Amazon Inspector.
- `iam`— Permet à Amazon Inspector de créer les rôles `AWSServiceRoleForAmazonInspector2` liés aux services et. `AWSServiceRoleForAmazonInspector2Agentless` `AWSServiceRoleForAmazonInspector2`est nécessaire pour qu'Amazon Inspector puisse effectuer des opérations telles que la récupération d'informations sur vos EC2 instances Amazon, les référentiels Amazon ECR et les images de conteneurs. Amazon Inspector doit également analyser votre réseau VPC et décrire les comptes associés à votre organisation. `AWSServiceRoleForAmazonInspector2Agentless`est nécessaire pour qu'Amazon Inspector puisse effectuer des opérations, telles que la récupération d'informations sur vos EC2 instances Amazon et vos instantanés Amazon EBS. Il est également nécessaire de déchiffrer les instantanés Amazon EBS chiffrés à l'aide de clés. AWS KMS 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. Lorsque vous activez 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": [
  {
   "Sid": "AllowFullAccessToInspectorApis",
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessToCodeGuruApis",
   "Effect": "Allow",
   "Action": [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
```

```
    "Resource": "*"
   },
   {
    "Sid": "AllowAccessToCreateSlr",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "iam:AWSServiceName": [
       "agentless.inspector2.amazonaws.com",
       "inspector2.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AllowAccessToOrganizationApis",
    "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 de l'autorisation

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 EC2 instances Amazon 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 EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès

dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Détails de l'autorisation

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 ServiceRolePolicy — Mises à jour d'une politique existante | Amazon Inspector a ajouté une nouvelle autorisation qui permet à Amazon Inspector de décrire les adresses IP et les passerelles Internet. | 29 avril 2025 |
| AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante | Amazon Inspector a ajouté de nouvelles autorisations qui permettent un accès en lecture seule aux actions Amazon ECS et Amazon EKS. | 25 mars 2025 |
| AmazonInspector2 ServiceRolePolicy — Mises à jour d'une politique existante | Amazon Inspector a ajouté de nouvelles autorisations qui permettent à Amazon Inspector de renvoyer des balises de fonction AWS Lambda. | 31 juillet 2024 |
| AmazonInspector2 FullAccess — Mises à jour d'une politique existante | Amazon Inspector a ajouté des autorisations qui permettent à Amazon Inspector de créer le rôle lié à un service. `AWSServic` | 24 avril 2024 |

| Modification | Description | Date |
| --- | --- | --- |
| | `eRoleForAmazonInspector2Agentless` Cela permet aux utilisateurs d'effectuer des scans basés sur des agents et des scans sans agent lorsqu'ils activent Amazon Inspector. | |
| 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 |
| 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 Agentless ServiceRolePolicy — Nouvelle politique | Amazon Inspector a ajouté une nouvelle politique de rôle liée au service afin de permettre l'analyse des instances sans agent. 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 |

| 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 scanner les configurations réseau des EC2 instances Amazon faisant partie des groupes cibles d'Elastic Load Balancing. | 31 août 2023 |
| 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 |

| 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 de récupérer les informations relatives à l'état de numérisation du code Lambda et aux résultats de leur compte. | 2 mai 2023 |
| 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 |

| Modification | Description | Date |
| --- | --- | --- |
| 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 EC2 approfondie d'Amazon. | 17 avril 2023 |
| 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 |

| 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 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 |
| 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 |

| 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 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 |
| 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 |

| Modification | Description | Date |
| --- | --- | --- |
| 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 |
| 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 qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne 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 la politique gérée nommée `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 EC2 instances Amazon 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 — Autorise à 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 d' EC2 instances faisant partie des groupes cibles d'Elastic Load Balancing.
- Utilisez les actions Amazon ECS et Amazon EKS pour autoriser un accès en lecture seule afin de visualiser les clusters et les tâches et de décrire les tâches.

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:DescribeAddresses",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "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",
    "lambda:ListTags",
```

```
    "cloudwatch:GetMetricData"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GatherInventory",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateAssociation",
    "ssm:StartAssociationsOnce",
    "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": "GatherInventoryDeleteAssociation",
   "Effect": "Allow",
   "Action": [
    "ssm:DeleteAssociation"
   ],
   "Resource": [
    "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"
     }
    }
   },
   {
    "Sid": "AllowListAccessToECSAndEKS",
    "Effect": "Allow",
    "Action": [
        "ecs:ListClusters",
        "ecs:ListTasks",
        "eks:ListClusters"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
    },
    {
    "Sid": "AllowAccessToECSTasks",
    "Effect": "Allow",
    "Action": [
        "ecs:DescribeTasks"
    ],
    "Resource": "arn:aws:ecs:*:*:task/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   }
  ]
}
```

## 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 l'API AWS Management Console, dans le AWS CLI ou dans 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 plus d'informations, consultez Modification d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

## 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 à un 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 EC2 instance 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 nommé`AmazonInspector2AgentlessServiceRolePolicy`, 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 EC2 instances, volumes et instantanés.
  - Utilisez les actions de EC2 balisage Amazon pour étiqueter les instantanés à numériser à l'aide de la `InspectorScan` clé de balise.
  - Utilisez les actions Amazon EC2 Snapshot pour créer des instantanés, les étiqueter avec la clé de `InspectorScan` balise, puis supprimer les instantanés des volumes Amazon EBS marqués avec la `InspectorScan` clé de balise.
- 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 l'API AWS Management Console, dans le AWS CLI ou dans 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 plus d'informations, consultez Modification d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

### 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 supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM AWS CLI, le ou l' AWS API pour supprimer le rôle lié au service AWSService RoleForAmazonInspector 2Agentless. 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
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon Inspector

### 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 un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

## Je 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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, 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 en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

## Surveillance d'Amazon Inspector

La surveillance joue un rôle important dans le maintien de la disponibilité, de la fiabilité et des performances d'Amazon Inspector et d'autres AWS solutions. AWS fournit des outils permettant de surveiller Amazon Inspector, de signaler les problèmes qui se produisent et de prendre des mesures pour y remédier :

- Amazon EventBridge est un AWS service qui utilise des événements pour connecter les composants de l'application entre eux, ce qui vous permet de créer plus facilement des applications évolutives pilotées par des événements. EventBridge fournit un flux de données en temps réel à partir de vos applications, applications Software-as-a-Service (SaaS), AWS services et itinéraires, afin que vous puissiez surveiller les événements qui se produisent dans les services et créer des architectures axées sur les événements.
- AWS CloudTrailest un AWS service qui capture les appels d'API et les événements connexes effectués par ou pour votre compte Compte AWS. CloudTrail envoie les fichiers journaux dans un

compartiment Amazon S3 que vous spécifiez, afin que vous puissiez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date à laquelle les appels ont eu lieu.

## 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, cette activité 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 à l'aide de 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 il 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 de suivi
- 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 individuelle d'une source quelconque. Les événements incluent des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne

constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

## 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 :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

## Résilience dans Amazon 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 à 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. Comme indiqué dans le modèle de responsabilitéAWS partagée sous « Sécurité du cloud », AWS il est chargé de protéger l'infrastructure exécutant tous les services du AWS cloud. AWS est également responsable de toute réponse aux incidents associée au service Amazon Inspector.

En tant que AWS client, vous partagez la responsabilité du maintien de la sécurité dans le AWS cloud. Cela signifie que vous contrôlez la sécurité que vous choisissez de mettre en œuvre, qui inclut tous les AWS outils et fonctionnalités auxquels vous accédez. Cela signifie également 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 qui répond à tous les objectifs de vos applications exécutées dans le AWS cloud, vous pouvez détecter les écarts auxquels vous pouvez réagir. La réponse aux incidents étant un sujet complexe, consultez les ressources suivantes pour mieux comprendre l'impact de la réponse aux incidents et la manière dont vos choix peuvent influencer les objectifs de votre entreprise : guide de réponse aux incidents de AWSAWS sécurité, meilleures pratiques en matière de sécurité et cadre d'adoption du AWS cloud : perspective de sécurité.

# Accédez à Amazon Inspector via un point de terminaison d'interface (AWS PrivateLink

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre VPC et Amazon Inspector. Vous pouvez accéder à Amazon Inspector comme s'il se trouvait dans votre VPC, sans passer par une passerelle Internet, un appareil NAT, une connexion VPN ou AWS Direct Connect une connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour accéder à Amazon Inspector.

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par le demandeur qui servent de point d'entrée pour le trafic destiné à Amazon Inspector.

Pour plus d'informations, consultez la section Accès Services AWS par AWS PrivateLink le biais du AWS PrivateLink guide.

## Considérations relatives à Amazon Inspector

Avant de configurer un point de terminaison d'interface pour Amazon Inspector, consultez les considérations du AWS PrivateLink guide.

Amazon Inspector permet d'appeler toutes ses actions d'API via le point de terminaison de l'interface.

Les politiques de point de terminaison VPC ne sont pas prises en charge pour Amazon Inspector. Par défaut, l'accès complet à Amazon Inspector est autorisé via le point de terminaison de l'interface. Vous pouvez également associer un groupe de sécurité aux interfaces réseau du point de terminaison afin de contrôler le trafic vers Amazon Inspector via le point de terminaison de l'interface.

## Création d'un point de terminaison d'interface pour Amazon Inspector

Vous pouvez créer un point de terminaison d'interface pour Amazon Inspector à l'aide de la console Amazon VPC ou du AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Lorsque vous créez un point de terminaison d'interface pour Amazon Inspector, utilisez l'un des noms de service suivants :

```
com.amazonaws.region.inspector2
```

```
com.amazonaws.region.inspector-scan
```

Remplacez *region* par le Région AWS code correspondant à ce qui s'applique Région AWS.

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à Amazon Inspector en utilisant son nom DNS régional par défaut, par exemple, `service-name.us-east-1.amazonaws.com` ou `service-name.us-east-1.api.aws.com` pour l'est des États-Unis (Virginie du Nord).

# Intégrations avec Amazon Inspector

Amazon Inspector s'intègre à d'autres AWS services. Ces services peuvent ingérer les données d'Amazon Inspector, afin que vous puissiez consulter vos résultats de différentes manières. Consultez les options d'intégration suivantes pour en savoir plus.

## Intégration d'Amazon Inspector à Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) est AWS un registre d'images de conteneurs géré qui prend en charge les registres privés. Les registres privés Amazon ECR hébergent des images de conteneurs dans une architecture hautement disponible et évolutive. Vous pouvez utiliser Amazon Inspector pour scanner les images de conteneurs stockées dans votre référentiel Amazon ECR afin de détecter les packages de systèmes d'exploitation et de langages de programmation vulnérables. Pour de plus amples informations, veuillez consulter Intégration d'Amazon Inspector à Amazon Elastic Container Registry (Amazon ECR).

## Intégration d'Amazon Inspector avec AWS Security Hub

AWS Security Hubfournit une vue complète de votre état de sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes du secteur de la sécurité et aux meilleures pratiques. Security Hub collecte des données de sécurité à partir de AWS comptes, de services et de produits pris en charge. Vous pouvez utiliser Security Hub pour ingérer les données des résultats d'Amazon Inspector et créer un emplacement central pour les résultats de tous vos AWS services intégrés et produits AWS Partner Network. Pour de plus amples informations, veuillez consulter Intégration d'Amazon Inspector avec AWS Security Hub.

## Intégration d'Amazon Inspector à Amazon Elastic Container Registry (Amazon ECR)

Amazon Elastic Container Registry est un registre de conteneurs entièrement géré qui prend en charge les images et artefacts Docker et AWS OCI. Si vous utilisez Amazon ECR, vous pouvez activer le scan amélioré pour votre registre de conteneurs. Lorsque vous activez le scan amélioré, Amazon Inspector détecte et scanne automatiquement les images de vos conteneurs 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 et de gérer la fréquence et l'étendue des scans dans la console Amazon ECR. Pour

plus d'informations, consultez Numérisation d'images de conteneurs Amazon ECR avec Amazon Inspector.

### 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, consultezTypes de scan automatisés dans 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 de plus amples informations, veuillez consulter Désactivation d'Amazon Inspector.

## Intégration d'Amazon Inspector avec AWS Security Hub

AWS Security Hub fournit une vue complète de l'état de votre sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub collecte des données de sécurité à partir de AWS comptes, de services et de produits pris en charge. Vous pouvez utiliser les informations fournies par Security Hub pour analyser vos tendances en matière de sécurité et identifier les problèmes de sécurité les plus prioritaires. Lorsque vous activez l'intégration, vous pouvez envoyer les résultats d'Amazon Inspector à Security Hub, et Security Hub peut les inclure dans son analyse de votre niveau de sécurité.

Dans Security Hub, les problèmes de sécurité sont suivis en tant que résultats. Certains de ces résultats peuvent résulter de problèmes détectés par d'autres AWS services ou produits tiers. Security Hub utilise un ensemble de règles pour détecter les problèmes de sécurité et générer des résultats. Security Hub fournit des outils qui vous aident à gérer les résultats. Security Hub archive les résultats d'Amazon Inspector une fois qu'ils ont été fermés dans Amazon Inspector. Vous pouvez également consulter l'historique de vos résultats et les détails de vos résultats, ainsi que suivre l'état d'une enquête sur un résultat.

Les résultats du Security Hub utilisent un format JSON standard appelé AWS Security Finding Format (ASFF). L'ASFF inclut des informations sur la source du problème, les ressources concernées et l'état actuel de vos conclusions.

Rubriques



## Afficher les résultats d'Amazon Inspector dans AWS Security Hub

Vous pouvez consulter les résultats d'Amazon Inspector Classic et d'Amazon Inspector dans Security Hub.

> **Note**
>
> Pour filtrer uniquement en fonction des résultats d'Amazon Inspector, ajoutez-les `"aws/inspector/ProductVersion": "2"` à la barre de filtre. Ce filtre exclut les résultats d'Amazon Inspector Classic du tableau de bord Security Hub.

Exemple de recherche provenant 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"
}
```

# Activation et configuration de l'intégration d'Amazon Inspector à Security Hub

Vous pouvez activer l'intégration avec Amazon Inspector AWS Security Hub en activant Security Hub. Une fois que vous avez activé Security Hub, l'intégration avec Amazon Inspector AWS Security Hub est automatiquement activée et Amazon Inspector commence à envoyer toutes ses conclusions à Security Hub en utilisant le format ASFF (AWS Security Finding Format).

## Désactiver le flux des résultats d'une intégration

Pour empêcher Amazon Inspector d'envoyer des résultats à Security Hub, vous pouvez utiliser la console ou l'API Security Hub et AWS CLI...

## Affichage des contrôles de sécurité pour Amazon Inspector dans Security Hub

Security Hub analyse les résultats des produits pris en charge AWS et des produits tiers et effectue des contrôles de sécurité automatisés et continus par rapport aux règles afin de générer ses propres conclusions. Les règles sont représentées par des contrôles de sécurité, qui vous aident à déterminer si les exigences d'une norme sont respectées.

Amazon Inspector utilise des contrôles de sécurité pour vérifier si les fonctionnalités d'Amazon Inspector sont ou doivent être activées. Les principales fonctions sont notamment :

- EC2 Numérisation Amazon
- Numérisation Amazon ECR
- Numérisation standard Lambda
- Analyse du code Lambda

Pour plus d'informations, consultez la section Contrôles Amazon Inspector dans le guide de AWS Security Hub l'utilisateur.

# Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector

Amazon Inspector peut scanner les applications logicielles installées sur les sites suivants :

- Instances Amazon Elastic Compute Cloud (Amazon EC2)

  > **Note**
  >
  > Pour les EC2 instances Amazon, Amazon Inspector peut détecter les vulnérabilités des packages dans les systèmes d'exploitation qui prennent en charge le scan basé sur des agents. Amazon Inspector peut également détecter les vulnérabilités des packages dans les systèmes d'exploitation et les langages de programmation qui prennent en charge le scan hybride. Amazon Inspector ne recherche pas les vulnérabilités de la chaîne d'outils. La version du compilateur de langage de programmation utilisée pour créer l'application introduit ces vulnérabilités.

- Images de conteneurs stockées dans les référentiels Amazon Elastic Container Registry (Amazon ECR)

  > **Note**
  >
  > Pour les images de conteneurs ECR, Amazon Inspector peut détecter les vulnérabilités du système d'exploitation et des packages de langage de programmation. Amazon Inspector ne recherche pas les vulnérabilités de la chaîne d'outils dansRust. La version du compilateur de langage de programmation utilisée pour créer l'application introduit ces vulnérabilités.

- AWS Lambda fonctions

  > **Note**
  >
  > Pour les fonctions Lambda, Amazon Inspector peut détecter les vulnérabilités des packages de langage de programmation et les vulnérabilités du code. Amazon Inspector ne recherche pas les vulnérabilités de la chaîne d'outils. La version du compilateur de langage de programmation utilisée pour créer l'application introduit ces vulnérabilités.

Lorsqu'Amazon Inspector analyse les ressources, Amazon Inspector s'approvisionne dans plus de 50 flux de données pour identifier les vulnérabilités et les risques courants (CVEs). Parmi ces sources, on peut citer les avis de sécurité des fournisseurs, les flux de données et les flux de renseignements sur les menaces, ainsi que la base de données nationale sur les vulnérabilités (NVD) et le MITRE. Amazon Inspector met à jour les données relatives aux vulnérabilités à partir des flux sources au moins une fois par jour.

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 langages de programmation et les environnements d'exécution pris en charge par Amazon Inspector pour les différentes ressources et les différents types de scan. Ils répertorient également les systèmes d'exploitation abandonnés.

> **Note**
>
> 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

Cette section répertorie les systèmes d'exploitation pris en charge par Amazon Inspector.

## Systèmes d'exploitation pris en charge : Amazon EC2 Scanning

Le tableau suivant répertorie les systèmes d'exploitation pris en charge par Amazon Inspector pour l'analyse des EC2 instances Amazon. Il indique l'avis de sécurité du fournisseur pour chaque système d'exploitation et indique quels systèmes d'exploitation prennent en charge l'analyse par agent et l'analyse sans agent.

Lorsque vous utilisez la méthode d'analyse basée sur un agent, vous configurez l'agent SSM pour effectuer des analyses continues sur toutes les instances éligibles. Amazon Inspector vous recommande de configurer une version de l'agent SSM supérieure à 3.2.2086.0. Pour plus d'informations, consultez la section Travailler avec l'agent SSM dans le guide de l'utilisateur d'Amazon EC2 Systems Manager.

Les détections du système d'exploitation Linux ne sont prises en charge que pour le référentiel du gestionnaire de packages par défaut (rpm et dpkg) et n'incluent pas les applications tierces, les référentiels de support étendu (RHEL EUS, E4S, AUS et TUS) et les référentiels facultatifs (flux d'applications). Amazon Inspector analyse le noyau en cours d'exécution à la recherche de vulnérabilités. Pour certains systèmes d'exploitation, par exempleUbuntu, un redémarrage est nécessaire pour que les mises à niveau apparaissent dans les résultats actifs.

| 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 |
| Serveur Debian (Bullseye) | 11 | DSA | Oui | Oui |
| Serveur Debian (Bookworm) | 12 | DSA | Oui | Oui |
| Fedora | 40 | CVE | Oui | Oui |

| Système d'exploitation | Version | Conseils de sécurité destinés aux fournisseurs | Support de numérisation sans agent | Support de numérisation basé sur un agent |
|---|---|---|---|---|
| Fedora | 41 | CVE | Oui | Oui |
| openSUSE Leap | 15,6 | CVE | Oui | Oui |
| Oracle Linux (Oracle) | 8 | ELSA | Oui | Oui |
| Oracle Linux (Oracle) | 9 | ELSA | Oui | Oui |
| Red Hat Enterprise Linux (RHEL) | 8 | RHSA | Oui | Oui |
| 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) | 15,6 | GROTTE DE SUSE | Oui | Oui |
| Ubuntu (Xenial) | 16,04 | USB, Ubuntu Pro (esm-infra et esm-apps) | Oui | Oui |
| Ubuntu (Bionic) | 18,04 | USB, Ubuntu Pro (esm-infra et esm-apps) | 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 | USB, Ubuntu Pro (esm-infra et esm-apps) | Oui | Oui |
| Ubuntu (Jammy) | 22,04 | USB, Ubuntu Pro (esm-infra et esm-apps) | Oui | Oui |
| Ubuntu (Noble Numbat) | 24.04 | USN, Ubuntu Pro (esm-infra & esm-apps) | Oui | Oui |
| Ubuntu (Oracular Oriole) | 24.10 | USN | Oui | Oui |
| Windows Server | 2016 | MSKB | Non | Oui |
| Windows Server | 2019 | MSKB | Non | Oui |
| Windows Server | 2022 | MSKB | Non | Oui |
| Windows Server | 2025 | 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 |

| Système d'exploitation | Version | Conseils de sécurité destinés aux fournisseurs | Support de numérisation sans agent | Support de numérisation basé sur un agent |
|---|---|---|---|---|
| macOS (Sonoma) | 14 | APPLE-SA | Non | Oui |

## Systèmes d'exploitation pris en charge : numérisation Amazon ECR avec Amazon Inspector

Le tableau suivant répertorie les systèmes d'exploitation pris en charge par Amazon Inspector pour la numérisation d'images de conteneurs dans les référentiels Amazon ECR. Il indique également l'avis de sécurité du fournisseur pour chaque système d'exploitation.

| Système d'exploitation | Version | Conseils de sécurité destinés aux fournisseurs |
|---|---|---|
| Alpine Linux (Alpine) | 3.18 | Alpine SecDB |
| Alpine Linux (Alpine) | 3.19 | Alpine SecDB |
| Alpine Linux (Alpine) | 3.20 | Alpine SecDB |
| Alpine Linux (Alpine) | 3.21 | Alpine SecDB |
| AlmaLinux | 8 | ALSA |
| AlmaLinux | 9 | ALSA |
| Amazon Linux (AL2) | AL2 | ALAS |
| Amazon Linux 2023 (AL2023) | AL2023 | ALAS |
| BusyBox | — | — |
| Chainguard | – | CVE |

| Système d'exploitation | Version | Conseils de sécurité destinés aux fournisseurs |
|---|---|---|
| Debian Server (Bullseye) | 11 | DSA |
| Debian Server (Bookworm) | 12 | DSA |
| Fedora | 40 | CVE |
| Fedora | 41 | CVE |
| openSUSE Leap | 15,6 | CVE |
| Oracle Linux (Oracle) | 8 | ELSA |
| Oracle Linux (Oracle) | 9 | ELSA |
| Photon OS | 4 | PHSA |
| Photon OS | 5 | PHSA |
| 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) | 15.6 | SUSE CVE |
| Ubuntu (Xenial) | 16.04 | USN, Ubuntu Pro (esm-infra & esm-apps) |
| Ubuntu (Bionic) | 18.04 | USN, Ubuntu Pro (esm-infra & esm-apps) |

| Système d'exploitation | Version | Conseils de sécurité destinés aux fournisseurs |
|---|---|---|
| Ubuntu (Focal) | 20.04 | USN, Ubuntu Pro (esm-infra & esm-apps) |
| Ubuntu (Jammy) | 22.04 | USN, Ubuntu Pro (esm-infra & esm-apps) |
| Ubuntu (Noble Numbat) | 24.04 | USN, Ubuntu Pro (esm-infra & esm-apps) |
| Ubuntu (Oracular Oriole) | 24.10 | USN |
| Wolfi | – | CVE |

## Systèmes d'exploitation pris en charge : scan CIS

Le tableau suivant répertorie les systèmes d'exploitation pris en charge par Amazon Inspector pour les scans CIS. Il indique également la version de référence CIS pour chaque système d'exploitation.

> **Note**
>
> Les normes CIS sont destinées aux systèmes d'exploitation x86_64. Certaines vérifications peuvent ne pas être évaluées ou renvoyer des instructions de correction non valides sur les ressources basées sur ARM.

| Système d'exploitation | Version | Version de référence CIS |
|---|---|---|
| Amazon Linux 2 | AL2 | 3.0.0 |
| Amazon Linux 2023 | AL2023 | 1.0.0 |
| Red Hat Enterprise Linux (RHEL) | 8 | 3.0.0 |

| Système d'exploitation | Version | Version de référence CIS |
|---|---|---|
| Red Hat Enterprise Linux (RHEL) | 9 | 2.0.0 |
| Rocky Linux | 8 | 2.0.0 |
| Rocky Linux | 9 | 1.0.0 |
| Ubuntu (Bonic) | 18,04 | 2.1.0 |
| Ubuntu (Focal) | 20,04 | 2.0.1 |
| Ubuntu (Jammy) | 22,04 | 1.0.0 |
| Ubuntu (Noble Numbat) | 24,04 | 1.0.0 |
| Windows Server | 2016 | 3.0.0 |
| Windows Server | 2019 | 2.0.0 |
| Windows Server | 2022 | 2.0.0 |

## Systèmes d'exploitation abandonnés

Les tableaux suivants indiquent quels systèmes d'exploitation ont été abandonnés et à quel moment ils l'ont été.

Même si Amazon Inspector ne fournit pas un support complet pour les systèmes d'exploitation abandonnés suivants, Amazon Inspector continue de scanner les EC2 instances Amazon et les images des conteneurs Amazon ECR qui les exécutent. Pour des raisons de sécurité, nous vous recommandons de passer à la version prise en charge d'un système d'exploitation abandonné. Les résultats générés par Amazon Inspector pour un système d'exploitation abandonné ne doivent être utilisés qu'à titre informatif.

Conformément à la politique du fournisseur, les systèmes d'exploitation suivants ne reçoivent plus de mises à jour correctives. Il est possible que de nouveaux avis de sécurité ne soient pas publiés pour les systèmes d'exploitation abandonnés. Les fournisseurs peuvent supprimer les alertes de sécurité et les détections existantes de leurs flux pour les systèmes d'exploitation qui atteignent la fin

du support standard. Par conséquent, Amazon Inspector peut arrêter de générer des résultats pour des données connues CVEs.

Systèmes d'exploitation abandonnés : Amazon EC2 Scanning

| Système d'exploitation | Version | Interrompu |
|---|---|---|
| Amazon Linux (AL1) | 2012 | 31 décembre 2021 |
| CentOS Linux (CentOS) | 7 | 30 juin 2024 |
| CentOS Linux (CentOS) | 8 | 31 décembre 2021 |
| Serveur Debian (Jessie) | 8 | 30 juin 2020 |
| Serveur Debian (Stretch) | 9 | 30 juin 2022 |
| Serveur Debian (Buster) | 10 | 30 juin 2024 |
| Fedora | 33 | 30 novembre 2021 |
| Fedora | 34 | 7 juin 2022 |
| Fedora | 35 | 13 décembre 2022 |
| Fedora | 36 | 16 mai 2023 |
| Fedora | 37 | 15 décembre 2023 |
| Fedora | 38 | 21 mai 2024 |
| Fedora | 39 | 26 novembre 2024 |
| openSUSE Leap | 15,2 | 1er décembre 2021 |
| OpenSUSE Leap | 15.3 | 1er décembre 2022 |
| openSUSE Leap | 15,4 | 7 décembre 2023 |
| OpenSUSE Leap | 15.5 | December 31, 2024 |
| Oracle Linux (Oracle) | 6 | 1er mars 2021 |

| Système d'exploitation | Version | Interrompu |
| --- | --- | --- |
| Oracle Linux (Oracle) | 7 | 31 décembre 2024 |
| Red Hat Enterprise Linux (RHEL) | 6 | 30 novembre 2020 |
| Red Hat Enterprise Linux (RHEL) | 7 | 30 juin 2024 |
| SUSE Linux Enterprise Server (SLES) | 12 | 30 juin 2016 |
| SUSE Linux Enterprise Server (SLES) | 12.1 | 31 mai 2017 |
| SUSE Linux Enterprise Server (SLES) | 12.2 | 31 mars 2018 |
| SUSE Linux Enterprise Server (SLES) | 12.3 | 30 juin 2019 |
| SUSE Linux Enterprise Server (SLES) | 12.4 | 30 juin 2020 |
| SUSE Linux Enterprise Server (SLES) | 12,5 | 31 octobre 2024 |
| 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 |
| SUSE Linux Enterprise Server (SLES) | 15,3 | 31 décembre 2022 |

| Système d'exploitation | Version | Interrompu |
| --- | --- | --- |
| SUSE Linux Enterprise Server (SLES) | 15,4 | 31 décembre 2023 |
| SUSE Linux Enterprise Server (SLES) | 15,5 | 31 décembre 2024 |
| Ubuntu (Fidèle) | 12,04 | 28 avril 2017 |
| Ubuntu (Fidèle) | 14,04 | 1er avril 2024 |
| 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 |
| Ubuntu (Minotaure mantique) | 23,10 | 11 juillet 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) | 3.2 | 1er mai 2017 |
| Alpine Linux (Alpine) | 3.3 | 1er novembre 2017 |
| Alpine Linux (Alpine) | 3.4 | 1 mai 2018 |
| Alpine Linux (Alpine) | 3,5 | 1er novembre 2018 |

| Système d'exploitation | Version | Interrompu |
|---|---|---|
| Alpine Linux (Alpine) | 3.6 | 1er mai 2019 |
| Alpine Linux (Alpine) | 3.7 | 1er novembre 2019 |
| Alpine Linux (Alpine) | 3.8 | 1er mai 2020 |
| Alpine Linux (Alpine) | 3.9 | 1er novembre 2020 |
| Alpine Linux (Alpine) | 3,10 | 1er mai 2021 |
| Alpine Linux (Alpine) | 3,11 | 1er novembre 2021 |
| 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 |
| Alpine Linux (Alpine) | 3.16 | May 23, 2024 |
| Alpine Linux (Alpine) | 3.17 | November 22, 2024 |
| Amazon Linux (AL1) | 2012 | 31 décembre 2021 |
| CentOS Linux (CentOS) | 7 | 30 juin 2024 |
| CentOS Linux (CentOS) | 8 | 31 décembre 2021 |
| Serveur Debian (Jessie) | 8 | 30 juin 2020 |
| Serveur Debian (Stretch) | 9 | 30 juin 2022 |
| Serveur Debian (Buster) | 10 | 30 juin 2024 |
| Fedora | 33 | 30 novembre 2021 |
| Fedora | 34 | 7 juin 2022 |

| Système d'exploitation | Version | Interrompu |
|---|---|---|
| Fedora | 35 | 13 décembre 2022 |
| Fedora | 36 | 16 mai 2023 |
| Fedora | 37 | 15 décembre 2023 |
| Fedora | 38 | 21 mai 2024 |
| Fedora | 39 | 26 novembre 2024 |
| openSUSE Leap | 15,2 | 1er décembre 2021 |
| OpenSUSE Leap | 15.3 | 1er décembre 2022 |
| OpenSUSE Leap | 15.4 | December 7, 2023 |
| OpenSUSE Leap | 15.5 | December 31, 2024 |
| Oracle Linux (Oracle) | 6 | 1er mars 2021 |
| Oracle Linux (Oracle) | 7 | 31 décembre 2024 |
| Photon OS | 2 | 2 décembre 2021 |
| Photon OS | 3 | 1er mars 2024 |
| Red Hat Enterprise Linux (RHEL) | 6 | 30 juin 2020 |
| Red Hat Enterprise Linux (RHEL) | 7 | 30 juin 2024 |
| SUSE Linux Enterprise Server (SLES) | 12 | 30 juin 2016 |
| SUSE Linux Enterprise Server (SLES) | 12.1 | 31 mai 2017 |

| Système d'exploitation | Version | Interrompu |
| --- | --- | --- |
| SUSE Linux Enterprise Server (SLES) | 12.2 | 31 mars 2018 |
| SUSE Linux Enterprise Server (SLES) | 12.3 | 30 juin 2019 |
| SUSE Linux Enterprise Server (SLES) | 12.4 | 30 juin 2020 |
| SUSE Linux Enterprise Server (SLES) | 12,5 | 31 octobre 2024 |
| 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 |
| SUSE Linux Enterprise Server (SLES) | 15,3 | 31 décembre 2022 |
| SUSE Linux Enterprise Server (SLES) | 15,4 | 31 décembre 2023 |
| SUSE Linux Enterprise Server (SLES) | 15,5 | 31 décembre 2024 |
| Ubuntu (Fidèle) | 12,04 | 28 avril 2017 |
| Ubuntu (Fidèle) | 14,04 | 1er avril 2024 |
| Ubuntu (Groovy) | 20,10 | 22 juillet 2021 |
| Ubuntu (Hirsute) | 21,04 | 20 janvier 2022 |

| Système d'exploitation | Version | Interrompu |
| --- | --- | --- |
| Ubuntu (Impish) | 21,10 | 31 juillet 2022 |
| Ubuntu (Kinetic) | 22.10 | July 20, 2023 |
| Ubuntu (Lunar Lobster) | 23.04 | January 25, 2024 |
| Ubuntu (Minotaure mantique) | 23,10 | 11 juillet 2024 |

# Langages de programmation pris en charge

Cette section répertorie les langages de programmation pris en charge par Amazon Inspector.

## Langages de programmation pris en charge : Amazon EC2 Agentless Scanning

Amazon Inspector prend actuellement en charge les langages de programmation suivants lors de l'exécution de scans sans agent sur des EC2 instances Amazon éligibles. Pour plus d'informations, consultez la section Numérisation sans agent.

> **Note**
>
> Amazon Inspector ne recherche pas les vulnérabilités de la chaîne d'outils dans Go etRust. La version du compilateur de langage de programmation utilisée pour créer l'application introduit ces vulnérabilités.

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

## Langages de programmation pris en charge : Amazon EC2 Deep Inspection

Amazon Inspector prend actuellement en charge les langages de programmation suivants lors de l'exécution de scans d'inspection approfondis sur les instances Amazon EC2 Linux. Pour plus d'informations, consultez l'inspection approfondie d'Amazon Inspector pour les instances Amazon EC2 basées sur Linux.

- Java(formats d'archive .ear, .jar, .par et .war)
- JavaScript
- Python

Amazon Inspector utilise Systems Manager Distributor pour déployer le plugin afin d'inspecter en profondeur votre EC2 instance Amazon.

> **Note**
>
> L'inspection approfondie n'est pas prise en charge pour les systèmes d'exploitation Bottlerocket.

Pour effectuer des analyses d'inspection approfondies, Systems Manager Distributor et Amazon Inspector doivent prendre en charge le système d'exploitation de votre EC2 instance Amazon. Pour plus d'informations sur les systèmes d'exploitation pris en charge dans Systems Manager Distributor, consultez la section Plateformes et architectures de packages prises en charge dans le Guide de l'utilisateur de Systems Manager.

## 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 :

> **Note**
>
> Amazon Inspector ne recherche pas les vulnérabilités de la chaîne d'outils dansRust. La version du compilateur de langage de programmation utilisée pour créer l'application introduit ces vulnérabilités.

- C#
- Go
- Gochaîne d'outils
- Java
- JavaJDK
- JavaScript
- PHP
- Python
- Ruby
- Rust

# Environnements d'exécution pris en charge

Cette section répertorie les environnements d'exécution pris en charge par Amazon Inspector.

## Runtimes pris en charge : analyse standard Amazon Inspector Lambda

Le scan standard Amazon Inspector Lambda prend actuellement en charge les environnements d'exécution suivants pour les langages de programmation qu'il peut utiliser lors de l'analyse des fonctions Lambda à la recherche de vulnérabilités dans des progiciels tiers :

> **Note**
>
> Amazon Inspector ne recherche pas les vulnérabilités de la chaîne d'outils dans Go etRust. La version du compilateur de langage de programmation utilisée pour créer l'application introduit ces vulnérabilités.

- Go
  - go1.x
- Java
  - java8
  - java8.al2
  - java11

  - java17
  - java21
- .NET
  - .NET 6
  - .NET 8
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
  - nodejs22.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
  - python3.12
  - python3.13
- Ruby
  - ruby2.7
  - ruby3.2
  - ruby3.3
- Custom runtimes
  - AL2
  - AL2023

# Runtimes pris en charge : analyse du code Lambda par Amazon Inspector

Le scan de code Lambda par Amazon Inspector prend actuellement en charge les environnements d'exécution suivants pour les langages de programmation qu'il peut utiliser lors de l'analyse des fonctions Lambda à la recherche de vulnérabilités dans le code :

- Java
  - java8
  - java8.al2
  - java11
  - java17
- .NET
  - .NET 6
  - .NET 8
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
  - python3.12
- Ruby
  - ruby2.7
  - ruby3.2
  - ruby3.3

# Désactivation d'Amazon Inspector

Vous pouvez désactiver Amazon Inspector dans la console Amazon Inspector ou à l'aide de l'API Amazon Inspector. Si vous désactivez tous les types de scan pour un compte, Amazon Inspector est automatiquement désactivé pour ce compte.

Si vous désactivez Amazon Inspector pour un compte, tous les types de scan sont désactivés pour ce compte. En outre, tous les paramètres de scan d'Amazon Inspector, y compris les filtres, les règles de suppression et les résultats, sont supprimés pour le compte.

Lorsque vous désactivez Amazon Inspector Amazon EC2 Scanning, Amazon Inspector supprime les associations SSM suivantes :

- `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 de plus amples informations, veuillez consulter Windows EC2 Instance de numérisation.

> **Note**
>
> Une fois que vous avez désactivé Amazon Inspector, vous n'avez plus à payer de frais de service. Cependant, vous pouvez réactiver Amazon Inspector à tout moment.

Pour plus d'informations sur la façon de désactiver les types de scan pour différentes ressources, voir Désactivation d'un type de scan.

Prérequis

En fonction du type de compte, tenez compte des points suivants :

- Si votre compte est un compte Amazon Inspector autonome, vous pouvez désactiver Amazon Inspector à tout moment.
- Si votre compte est un compte membre dans un environnement multi-comptes, vous ne pouvez pas désactiver Amazon Inspector. Vous devez contacter l'administrateur délégué de votre organisation pour désactiver Amazon Inspector.

- Si vous êtes l'administrateur délégué d'une organisation, vous devez dissocier tous les comptes de ses membres avant de désactiver Amazon Inspector.

> **Note**
>
> Lorsque vous désactivez Amazon Inspector en tant qu'administrateur délégué, vous désactivez la fonctionnalité d'activation automatique pour votre organisation.

# Désactiver Amazon Inspector

> **Note**
>
> Avant de désactiver Amazon Inspector, pensez à exporter vos résultats.

Console

Pour désactiver Amazon Inspector

1. Connectez-vous à l'aide de vos informations d'identification, puis ouvrez la console Amazon Inspector sur 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 le compte IDs que vous désactivez et indiquez `EC2, ECR, LAMBDA` `resourceTypes` pour désactiver tous les scans, ce qui désactivera le compte.

# Quotas Amazon Inspector

Cette section répertorie les quotas Amazon Inspector par Région AWS.

| Ressource | Par défaut | Commentaires |
| --- | --- | --- |
| Comptes membres | 10 000 | Le nombre maximum de comptes membres associés à un compte d'administrateur délégué Amazon Inspector. La limite est basée sur les quotas pour AWS Organizations. |
| 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 EC2 du réseau Amazon | 10 000 | Le nombre maximum de résultats sur le EC2 réseau Amazon par AWS compte. Vous ne pouvez pas demander d'augmentation de quota. |
| Configurations de numérisation CIS | 500 | Nombre maximal de configurations de scan CIS. Vous ne pouvez pas demander |

| Ressource | Par défaut | Commentaires |
| --- | --- | --- |
| | | d'augmentation de quota. |

Pour obtenir la liste des quotas associés à Amazon Inspector Classic, consultez la section Quotas de service Amazon Inspector Classic dans le Références générales AWS. Pour obtenir la liste des quotas associés à AWS Organizations, consultez la section sur les quotas de AWS Organizations service dans le Références générales AWS.

# Régions et points de terminaison

Cette rubrique inclut des tableaux qui présentent les points de terminaison pour Amazon Inspector et Amazon Inspector Scan. Il inclut également des tableaux qui indiquent les fonctionnalités Régions AWS compatibles avec Amazon Inspector.

Pour savoir Régions AWS où Amazon Inspector est disponible, consultez le point de terminaison et les quotas Amazon Inspector dans le Référence générale d'Amazon Web Services.

## Points de terminaison de service pour Amazon Inspector

Le tableau suivant présente les points de terminaison de service pour Amazon Inspector. La convention de dénomination pour les points de terminaison Amazon Inspector est`inspector2.`*`Region`*`.amazonaws.com`.

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| USA Est (Virginie du Nord) | us-east-1 | inspector2.us-east-1.amazonaws.com<br>inspector2.us-east-1.api.aws.com<br>inspector2-fips.us-east-1.amazonaws.com | HTTPS |
| USA Est (Ohio) | us-east-2 | inspector2.us-east-2.amazonaws.com<br>inspector2.us-east-2.api.aws.com<br>inspector2-fips.us-east-2.amazonaws.com | HTTPS |
| USA Ouest (Californie du Nord) | us-west-1 | inspector2.us-west-1.amazonaws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| | | inspector2.us-west-1.api.aws.com<br><br>inspector2-fips.us-west-1.amazonaws.com | |
| USA Ouest (Oregon) | us-west-2 | inspector2.us-west-2.amazonaws.com<br><br>inspector2.us-west-2.api.aws.com<br><br>inspector2-fips.us-west-2.amazonaws.com | HTTPS |
| Afrique (Le Cap) | af-south-1 | inspector2.af-south-1.amazonaws.com<br><br>inspector2.af-south-1.api.aws.com | HTTPS |
| Asie-Pacifique (Hong Kong) | ap-east-1 | inspector2.ap-east-1.amazonaws.com<br><br>inspector2.ap-east-1.api.aws.com | HTTPS |
| Asie-Pacifique (Jakarta) | ap-southeast-3 | inspector2.ap-southeast-3.amazonaws.com<br><br>inspector2.ap-southeast-3.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Asie-Pacifique (Mumbai) | ap-south-1 | inspector2.ap-south-1.amazonaws.com<br><br>inspector2.ap-south-1.api.aws.com | HTTPS |
| Asie-Pacifique (Osaka) | ap-northeast-3 | inspector2.ap-northeast-3.amazonaws.com<br><br>inspector2.ap-northeast-3.api.aws.com | HTTPS |
| Asie-Pacifique (Séoul) | ap-northeast-2 | inspector2.ap-northeast-2.amazonaws.com<br><br>inspector2.ap-northeast-2.api.aws.com | HTTPS |
| Asie-Pacifique (Singapour) | ap-southeast-1 | inspector2.ap-southeast-1.amazonaws.com<br><br>inspector2.ap-southeast-1.api.aws.com | HTTPS |
| Asie-Pacifique (Sydney) | ap-southeast-2 | inspector2.ap-southeast-2.amazonaws.com<br><br>inspector2.ap-southeast-2.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Asie-Pacifique (Tokyo) | ap-northeast-1 | inspector2.ap-northeast-1.amazonaws.com<br><br>inspector2.ap-northeast-1.api.aws.com | HTTPS |
| Canada (Centre) | ca-central-1 | inspector2.ca-central-1.amazonaws.com<br><br>inspector2.ca-central-1.api.aws.com | HTTPS |
| Europe (Francfort) | eu-central-1 | inspector2.eu-central-1.amazonaws.com<br><br>inspector2.eu-central-1.api.aws.com | HTTPS |
| Europe (Irlande) | eu-west-1 | inspector2.eu-west-1.amazonaws.com<br><br>inspector2.eu-west-1.api.aws.com | HTTPS |
| Europe (Londres) | eu-west-2 | inspector2.eu-west-2.amazonaws.com<br><br>inspector2.eu-west-2.api.aws.com | HTTPS |
| Europe (Milan) | eu-south-1 | inspector2.eu-south-1.amazonaws.com<br><br>inspector2.eu-south-1.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Europe (Paris) | eu-west-3 | inspector2.eu-west-3.amazonaws.com<br>inspector2.eu-west-3.api.aws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | inspector2.eu-north-1.amazonaws.com<br>inspector2.eu-north-1.api.aws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | inspector2.eu-central-2.amazonaws.com<br>inspector2.eu-central-2.api.aws.com | HTTPS |
| Moyen-Orient (Bahreïn) | me-south-1 | inspector2.me-south-1.amazonaws.com<br>inspector2.me-south-1.api.aws.com | HTTPS |
| Amérique du Sud (São Paulo) | sa-east-1 | inspector2.sa-east-1.amazonaws.com<br>inspector2.sa-east-1.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| AWS GovCloud (USA Est) | us-gov-east-1 | inspecteur2. us-gov-east-1. amazonaws .com<br><br>inspecteur2. us-gov-east-1. api.aws.com<br><br>inspector2-fips. us-gov-east-1. amazonaws.com | HTTPS |
| AWS GovCloud (US-Ouest) | us-gov-west-1 | inspecteur2. us-gov-west-1. amazonaws .com<br><br>inspecteur2. us-gov-west-1. api.aws.com<br><br>inspector2-fips. us-gov-west-1. amazonaws.com | HTTPS |

# 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<br><br>inspector-scan.us-east-2.api.aws.com<br><br>inspector-scan-fips.us-east-2.amazonaws.com | HTTPS |
| USA Est (Virginie du Nord) | us-east-1 | inspector-scan.us-east-1.amazonaws.com<br><br>inspector-scan.us-east-1.api.aws.com<br><br>inspector-scan-fips.us-east-1.amazonaws.com | HTTPS |
| USA Ouest (Californie du Nord) | us-west-1 | inspector-scan.us-west-1.amazonaws.com<br><br>inspector-scan.us-west-1.api.aws.com<br><br>inspector-scan-fips.us-west-1.amazonaws.com | HTTPS |
| USA Ouest (Oregon) | us-west-2 | inspector-scan.us-west-2.amazonaws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| | | inspector-scan.us-west-2.api.aws.com<br><br>inspector-scan-fips.us-west-2.amazonaws.com | |
| Afrique (Le Cap) | af-south-1 | inspector-scan.af-south-1.amazonaws.com<br><br>inspector-scan.af-south-1.api.aws.com | HTTPS |
| Asie-Pacifique (Hong Kong) | ap-east-1 | inspector-scan.ap-east-1.amazonaws.com<br><br>inspector-scan.ap-east-1.api.aws.com | HTTPS |
| Asie-Pacifique (Jakarta) | ap-southeast-3 | inspector-scan.ap-southeast-3.amazonaws.com<br><br>inspector-scan.ap-southeast-3.api.aws.com | HTTPS |
| Asie-Pacifique (Mumbai) | ap-south-1 | inspector-scan.ap-south-1.amazonaws.com<br><br>inspector-scan.ap-south-1.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Asie-Pacifique (Osaka) | ap-northeast-3 | inspector-scan.ap-northeast-3.amazonaws.com<br>inspector-scan.ap-northeast-3.api.aws.com | HTTPS |
| Asie-Pacifique (Séoul) | ap-northeast-2 | inspector-scan.ap-northeast-2.amazonaws.com<br>inspector-scan.ap-northeast-2.api.aws.com | HTTPS |
| Asie-Pacifique (Singapour) | ap-southeast-1 | inspector-scan.ap-southeast-1.amazonaws.com<br>inspector-scan.ap-southeast-1.api.aws.com | HTTPS |
| Asie-Pacifique (Sydney) | ap-southeast-2 | inspector-scan.ap-southeast-2.amazonaws.com<br>inspector-scan.ap-southeast-2.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Asie-Pacifique (Tokyo) | ap-northeast-1 | inspector-scan.ap-northeast-1.amazonaws.com<br><br>inspector-scan.ap-northeast-1.api.aws.com | HTTPS |
| Canada (Centre) | ca-central-1 | inspector-scan.ca-central-1.amazonaws.com<br><br>inspector-scan.ca-central-1.api.aws.com | HTTPS |
| Europe (Francfort) | eu-central-1 | inspector-scan.eu-central-1.amazonaws.com<br><br>inspector-scan.eu-central-1.api.aws.com | HTTPS |
| Europe (Irlande) | eu-west-1 | inspector-scan.eu-west-1.amazonaws.com<br><br>inspector-scan.eu-west-1.api.aws.com | HTTPS |
| Europe (Londres) | eu-west-2 | inspector-scan.eu-west-2.amazonaws.com<br><br>inspector-scan.eu-west-2.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Europe (Milan) | eu-south-1 | inspector-scan.eu-south-1.amazonaws.com<br><br>inspector-scan.eu-south-1.api.aws.com | HTTPS |
| Europe (Paris) | eu-west-3 | inspector-scan.eu-west-3.amazonaws.com<br><br>inspector-scan.eu-west-3.api.aws.com | HTTPS |
| Europe (Stockholm) | eu-north-1 | inspector-scan.eu-north-1.amazonaws.com<br><br>inspector-scan.eu-north-1.api.aws.com | HTTPS |
| Europe (Zurich) | eu-central-2 | inspector-scan.eu-central-2.amazonaws.com<br><br>inspector-scan.eu-central-2.api.aws.com | HTTPS |
| Moyen-Orient (Bahreïn) | me-south-1 | inspector-scan.me-south-1.amazonaws.com<br><br>inspector-scan.me-south-1.api.aws.com | HTTPS |

| Nom de la région | Région | Point de terminaison | Protocole |
|---|---|---|---|
| Amérique du Sud (São Paulo) | sa-east-1 | inspector-scan.sa-east-1.amazonaws.com<br><br>inspector-scan.sa-east-1.api.aws.com | HTTPS |
| AWS GovCloud (USA Est) | us-gov-east-1 | inspecteur-scan. us-gov-east-1. amazonaws.com<br><br>inspecteur-scan. us-gov-east-1. api.aws.com<br><br>inspector-scan-fips. us-gov-east-1. amazonaws.com | HTTPS |
| AWS GovCloud (US-Ouest) | us-gov-west-1 | inspecteur-scan. us-gov-west-1. amazonaws.com<br><br>inspecteur-scan. us-gov-west-1. api.aws.com<br><br>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 par Région AWS.

## EC2 Numérisation sans agent pour les régions Amazon EC2

Le tableau suivant indique les domaines dans Régions AWS lesquels le scan sans agent EC2 est actuellement disponible pour Amazon.

| Nom de la région | Code région |
|---|---|
| USA Est (Virginie du Nord) | us-east-1 |
| USA Est (Ohio) | us-east-2 |
| USA Ouest (Californie du Nord) | us-west-1 |
| US West (Oregon) | us-west-2 |
| Afrique (Le Cap) | af-south-1 |
| Asie-Pacifique (Hong Kong) | ap-east-1 |
| Asie-Pacifique (Tokyo) | ap-northeast-1 |
| Asie-Pacifique (Séoul) | ap-northeast-2 |
| Asie-Pacifique (Osaka) | ap-northeast-3 |
| Asie-Pacifique (Mumbai) | ap-south-1 |
| Asie-Pacifique (Singapour) | ap-southeast-1 |
| Asie-Pacifique (Sydney) | ap-southeast-2 |
| Asie-Pacifique (Jakarta) | ap-southeast-3 |
| Canada (Centre) | ca-central-1 |
| Europe (Stockholm) | eu-north-1 |
| Europe (Francfort) | eu-central-1 |
| Europe (Zurich) | eu-central-2 |
| Europe (Irlande) | eu-west-1 |

| Nom de la région | Code région |
| --- | --- |
| Europe (Londres) | eu-west-2 |
| Europe (Paris) | eu-west-3 |
| Europe (Milan) | eu-south-1 |
| Moyen-Orient (Bahreïn) | me-south-1 |
| Amérique du Sud (São Paulo) | sa-east-1 |
| AWS GovCloud (USA Est) | us-gov-east-1 |
| AWS GovCloud (US-Ouest) | us-gov-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 |
| --- | --- |
| USA Est (Virginie du Nord) | us-east-1 |
| USA Ouest (Oregon) | us-west-2 |
| 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 |

| Nom de la région | Code région |
| --- | --- |
| Asie-Pacifique (Singapour) | ap-southeast-1 |

> **Important**
>
> Si vous essayez d'activer le scan de code Lambda avec l'API Amazon Inspector Enable alors que le scan de code Région AWS Lambda n'est pas disponible, le message d'erreur de refus d'accès suivant s'affiche :
>
> ```
> An error occurred (AccessDeniedException) when calling the Enable operation:
>  Lambda code scanning is not supported in unsupported-Région AWS
> ```

### AWS GovCloud (US) Régions

Pour obtenir les dernières informations, consultez Amazon Inspector dans le guide de AWS GovCloud (US) l'utilisateur.

# Historique du document

Le tableau suivant décrit les modifications importantes apportées à chaque version du guide de l'utilisateur d'Amazon Inspector, à compter de novembre 2021. Pour recevoir des notifications concernant les mises à jour de la documentation, vous pouvez vous abonner à un flux RSS.

| Modification | Description | Date |
| --- | --- | --- |
| Nouvelle fonction | Amazon Inspector peut désormais afficher les images de conteneurs activement utilisées et la date à laquelle les images de conteneur ont été utilisées pour la dernière fois sur un cluster. Pour plus d'informations, voir Mappage d'images de conteneurs à des conteneurs en cours d'exécution. | 16 mai 2025 |
| Mises à jour des systèmes d'exploitation pris en charge | Amazon Inspector ajoute la prise en charge de BusyBox Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge par Amazon Inspector. | 13 mai 2025 |
| Politique mise à jour | Amazon Inspector ajoute une nouvelle autorisation au rôle lié au service nommé. `AmazonInspector2ServiceRolePolicy` Cette autorisation vous permet de décrire les adresses IP et les passerelles Internet. Pour plus d'informations, consultez les | 29 avril 2025 |

| | | |
|---|---|---|
| | politiques AWS gérées pour Amazon Inspector. | |
| Mise à jour pour le plugin | Amazon Inspector a été informé d'un scénario dans lequel le plug-in Amazon Inspector SSM pourrait générer une détection de vulnérabilité pour`CVE-2025-22871` . Il a été confirmé que le plug-in Amazon Inspector SSM n'est pas concerné CVEs, et une mise à jour a été déployée pour résoudre cette détection. | 21 avril 2025 |
| Mise à jour pour le plugin | Amazon Inspector a été informé d'un scénario dans lequel le plug-in Amazon Inspector SSM pourrait générer une détection de vulnérabilité pour `CVE-2020-8911` `CVE-2020-8912` , et`CVE-2024-45337` . Il a été confirmé qu'Amazon Inspector n'est pas concerné CVEs et une mise à jour a été déployée pour résoudre cette détection. | 18 avril 2025 |
| Mises à jour du chapitre Amazon Inspector SBOM Generator | Amazon Inspector met à jour la version d'Amazon Inspector SBOM Generator . Pour plus d'informations, consultez Versions précédentes d'Amazon Inspector SBOM Generator. | 16 avril 2025 |

| | | |
|---|---|---|
| Mises à jour du chapitre Amazon Inspector SBOM Generator | Amazon Inspector ajoute une nouvelle rubrique au chapitre Amazon Inspector SBOM Generator. Cette rubrique décrit comment Sbomgen suivre les informations de licence dans une nomenclature logicielle. Pour plus d'informations, consultez la section Collection de licences Amazon Inspector SBOM Generator. | 16 avril 2025 |
| Mises à jour des politiques gérées | Amazon Inspector ajoute des autorisations qui permettent un accès en lecture seule aux actions Amazon ECS et Amazon EKS. Pour plus d'informations, consultez la section Autorisations de rôle liées à un service pour Amazon Inspector. | 25 mars 2025 |
| Mises à jour des systèmes d'exploitation pris en charge | Amazon Inspector n'est plus pris en charge dans SUSE Linux Enterprise Server 12.5 le cadre de la numérisation pour Amazon EC2 et Amazon ECR. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 21 mars 2025 |

| | | |
|---|---|---|
| Mises à jour des systèmes d'exploitation pris en charge | Amazon Inspector ajoute la prise en charge Wolfi de Chainguard et à la numérisation Amazon ECR. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 21 mars 2025 |
| Mises à jour de la table des matières | Amazon Inspector ajoute un chapitre sur le balisage des ressources Amazon Inspector. Pour plus d'informations, consultez la section Marquage des ressources Amazon Inspector. | 25 février 2025 |
| Mises à jour de la table des matières | Amazon Inspector ajoute une nouvelle rubrique au chapitre Amazon Inspector SBOM Generator. Pour plus d'informations, consultez la collection complète des systèmes d'exploitation Amazon Inspector SBOM Generator. | 28 janvier 2025 |

| | | |
|---|---|---|
| Fonctionnalités mises à jour | Amazon Inspector ajoute nodejs202.x et python3.13 à sa liste d'environnements d'exécution pris en charge pour le scan standard Lambda. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 24 janvier 2025 |
| Fonctionnalités mises à jour | Amazon Inspector supprime Oracle Linux (Oracle) 7 et SUSE Linux Enterprise Server (SLES) 15.5 de sa liste de systèmes d'exploitation pris en charge pour Amazon et EC2 Amazon ECR. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 31 décembre 2024 |
| Fonctionnalités mises à jour | Amazon Inspector ajoute la Ubuntu version 24.10 à sa liste de systèmes d'exploitation pris en charge pour Amazon EC2 et Amazon ECR. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 12 décembre 2024 |

| | | |
|---|---|---|
| Mises à jour de la table des matières | Amazon Inspector ajoute de nouvelles rubriques au chapitre Amazon Inspector SBOM Generator. Pour plus d'informations, consultez Amazon Inspector SBOM Generator. | 9 décembre 2024 |
| Fonctionnalités mises à jour | Amazon Inspector met à jour le `amazon:inspector:sbom_generator` tableau pour ajouter et supprimer des espaces de noms. Pour plus d'informations, consultez la section Utilisation des espaces de noms CycloneDX avec Amazon Inspector. | 9 décembre 2024 |
| Fonctionnalités mises à jour | Amazon Inspector met à jour sa fonctionnalité d'intégration CI/CD pour prendre en charge les actions de scan avec. CodePipeline Pour plus d'informations, consultez la section Utilisation des actions de scan d'Amazon Inspector avec CodePipeline. | 26 novembre 2024 |
| Mises à jour de la table des matières | Amazon Inspector réorganise la table des matières pour inclure un chapitre pour le générateur Amazon Inspector SBOM. Pour plus d'informations, consultez Amazon Inspector SBOM Generator. | 22 novembre 2024 |

| | | |
|---|---|---|
| Fonctionnalités mises à jour | Amazon Inspector en retire Fedora 39 de sa liste des systèmes d'exploitation pris en charge pour Amazon EC2 et Amazon ECR. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 22 novembre 2024 |
| Fonctionnalités mises à jour | Amazon Inspector supprime la Alpine version 3.17 de sa liste des systèmes d'exploitation pris en charge pour Amazon ECR. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 22 novembre 2024 |
| Fonctionnalités mises à jour | Amazon Inspector ajoute Sbomgen des versions aux versions précédentes du générateur Amazon Inspector SBOM. | 19 novembre 2024 |
| Fonctionnalités mises à jour | Amazon Inspector est ajouté AL2 en tant qu'environnement d'exécution pris en charge. Pour plus d'informations, consultez Systèmes d'exploitation et langages de programmation pris en charge pour Amazon Inspector. | 26 août 2024 |

| | | |
|---|---|---|
| Fonctionnalités mises à jour | Amazon Inspector a ajouté une nouvelle déclaration à la AmazonInspector2ServiceRolePolicypolitique. La nouvelle instruction permet à Amazon Inspector de renvoyer des balises de fonction AWS Lambda. | 31 juillet 2024 |
| Fonctionnalités mises à jour | Amazon Inspector publie de nouveaux contrôles de sécurité. Pour plus d'informations, consultez la section Contrôles Amazon Inspector dans le guide de AWS Security Hub l'utilisateur. | 11 juillet 2024 |
| Fonctionnalités mises à jour | Le générateur Amazon Inspector SBOM analyse désormais les fichiers Dockerfiles et les images des conteneurs Docker pour détecter les erreurs de configuration susceptibles d'introduire des failles de sécurité. Pour plus d'informations, consultez Amazon Inspector Dockerfile checks. | 10 juin 2024 |

| | | |
|---|---|---|
| Fonctionnalités mises à jour | Amazon Inspector met à jour sa fonctionnalité d'intégration CI/CD pour prendre en charge CodeCatalyst les actions, afin que vous puissiez ajouter des analyses de vulnérabilité Amazon Inspector à vos CodeCatalyst flux de travail. Pour plus d'informations, consultez la section Utilisation CodeCatalyst des actions. | 7 juin 2024 |
| Fonctionnalités mises à jour | Amazon Inspector inclut une option permettant de télécharger un fichier CSV contenant les résultats du scan CIS. Pour plus d'informations, consultez la section Affichage et téléchargement des résultats de scan CIS dans les scans du Center for Internet Security (CIS) pour les EC2 instances Amazon. | 3 mai 2024 |
| Fonctionnalités mises à jour | Amazon Inspector met à jour sa fonctionnalité d'intégration CI/CD afin que vous puissiez ajouter des analyses de vulnérabilité Amazon Inspector à vos GitHub flux de travail. GitHub Actions Pour plus d'informations, consultez la section Utilisation d'Amazon Inspector avec GitHub Actions. | 29 avril 2024 |

| | | |
|---|---|---|
| Fonctionnalités mises à jour | Amazon Inspector met à jour la politique `AmazonInspector2FullAccess` gérée afin de créer le rôle lié au service. `AWSServiceRoleForAmazonInspector2Agentless` Cela permet aux utilisateurs d'effectuer une analyse basée sur un agent et une analyse sans agent lorsqu'ils activent Amazon Inspector. | 24 avril 2024 |
| Fonctionnalités mises à jour | Amazon Inspector met à jour 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 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. | 23 janvier 2024 |
| Nouvelle fonctionnalité | Amazon Inspector peut désormais exécuter des scans du Center for Internet Security (CIS) sur les EC2 instances . 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 EC2 instance 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 EC2 instances Amazon Linux 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 EC2 instances Amazon macOS. Voir Systèmes d'exploitation pris en charge : Amazon EC2 recherche 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 EC2 des instances 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 EC2 instances Amazon faisant 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 on 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 EC2 approfondie d'Amazon. | 17 avril 2023 |

| | | |
|---|---|---|
| Nouvelle fonction | Amazon Inspector ajoute un support supplémentaire pour les EC2 instances Linux 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 Lambda fonctions 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 |

# AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

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.