aws

Guide de l’utilisateur

Amazon Inspector Classic

Version Latest

Amazon Inspector Classic: Guide de l’utilisateur

Table of Contents

Il s'agit du guide de l'utilisateur d'Amazon Inspector Classic. Pour plus d'informations sur le nouvel Amazon Inspector, consultez le guide de l'utilisateur d'Amazon Inspector. Pour accéder à la console Amazon Inspector Classic, ouvrez la console Amazon Inspector à l'adresse https://console.aws.amazon.com/inspector/, puis choisissez Amazon Inspector Classic dans le volet de navigation.

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.

Qu'est-ce qu'Amazon Inspector Classic ?

> **Note**
>
> Le nouvel Amazon Inspector, une version entièrement repensée et redessinée d'Amazon Inspector Classic, est désormais disponible sur l'ensemble du site. Régions AWS Le nouvel Amazon Inspector a étendu sa couverture pour ajouter la prise en charge des images de conteneurs résidant dans Amazon Elastic Container Registry (Amazon ECR) en plus des instances EC2. Le nouvel Amazon Inspector offre un support multi-comptes grâce à l'intégration et à l'analyse continue des vulnérabilités logicielles et de l'accessibilité du réseau sur la base des vulnérabilités et des expositions courantes (CVE). AWS Organizations Nous vous encourageons à explorer et à utiliser ces fonctionnalités ainsi que d'autres fonctionnalités nouvelles et améliorées, et à bénéficier de leur valeur de sécurité considérablement accrue. Pour en savoir plus sur les fonctionnalités et les tarifs du nouvel Amazon Inspector, consultez Amazon Inspector. Pour savoir comment passer au nouvel Amazon Inspector, consultezPassage au nouvel Amazon Inspector.

Amazon Inspector Classic teste l'accessibilité réseau de vos instances Amazon EC2 et l'état de sécurité de vos applications qui s'exécutent sur ces instances. Amazon Inspector Classic évalue les applications pour détecter leur exposition, leurs vulnérabilités et les écarts par rapport aux meilleures pratiques. Après avoir effectué une évaluation, Amazon Inspector Classic produit une liste détaillée des résultats de sécurité, organisée par niveau de gravité.

Avec Amazon Inspector Classic, vous pouvez automatiser les évaluations des vulnérabilités de sécurité tout au long de vos pipelines de développement et de déploiement ou pour les systèmes de production statiques. Cela vous permet d'effectuer régulièrement des tests de sécurité dans le cadre d'opérations de développement et informatiques.

Amazon Inspector Classic propose également un logiciel prédéfini appelé agent que vous pouvez éventuellement installer dans le système d'exploitation des instances EC2 que vous souhaitez évaluer. L'agent surveille le comportement des instances EC2, notamment l'activité du réseau, du système de fichiers et des processus. Il collecte également une grande sélection de données de configuration et de comportement (télémétrie).

> **Important**
>
> AWS ne garantit pas que le respect des recommandations fournies résoudra tous les problèmes de sécurité potentiels. Les résultats générés par Amazon Inspector Classic dépendent du choix des packages de règles inclus dans chaque modèle d'évaluation, de la présence de AWS non-composants dans votre système et d'autres facteurs. Vous êtes responsable de la sécurité des applications, des processus et des outils exécutés sur les AWS services. Pour plus d'informations, consultez le modèle de responsabilitéAWS partagée pour la sécurité.

> **Note**
>
> AWS est responsable de la protection de l'infrastructure mondiale qui gère les services proposés dans le AWS cloud. Cette infrastructure comprend le matériel, les logiciels, les réseaux et les installations qui exécutent AWS les services. AWS fournit plusieurs rapports d'auditeurs tiers qui ont vérifié notre conformité à diverses normes et réglementations en matière de sécurité informatique. Pour plus d'informations, consultez AWS Cloud Compliance.

Pour plus d'informations sur la terminologie Amazon Inspector Classic, consultezTerminologie et concepts Amazon Inspector Classic.

Avantages d'Amazon Inspector Classic

Voici quelques-uns des principaux avantages d'Amazon Inspector Classic :

- Intégrez des contrôles de sécurité automatisés à vos processus habituels de déploiement et de production : évaluez la sécurité de vos AWS ressources à des fins d'investigation, de dépannage ou d'audit actif. Exécutez les évaluations pendant le processus de développement ou exécutez-les dans un environnement de production stable.
- Identifiez les problèmes de sécurité des applications : automatisez l'évaluation de la sécurité de vos applications et identifiez les vulnérabilités de manière proactive. Vous pouvez ainsi développer et corriger les nouvelles applications rapidement, et évaluer leur conformité à vos bonnes pratiques et stratégies.

- Approfondissez votre connaissance de vos AWS ressources : restez informé de l'activité et des données de configuration de vos AWS ressources en consultant les résultats produits par Amazon Inspector Classic.

Caractéristiques d'Amazon Inspector Classic

Voici quelques-unes des principales fonctionnalités d'Amazon Inspector Classic :

- Moteur d'analyse de la configuration et de surveillance des activités : Amazon Inspector Classic fournit un agent qui analyse la configuration du système et des ressources. Il surveille également l'activité pour déterminer à quoi ressemble un objectif d'évaluation, son comportement et ses composants dépendants. La combinaison de ces données télémétriques fournit une vue d'ensemble complète de l'objectif d'évaluation et des problèmes de sécurité ou de conformité potentiels.
- Bibliothèque de contenu intégrée — Amazon Inspector Classic inclut une bibliothèque intégrée de règles et de rapports. Ces ressources comprennent des contrôles par rapport aux bonnes pratiques, aux normes de conformité courantes et aux vulnérabilités. Ces contrôles incluent des étapes recommandées détaillées pour résoudre les problèmes de sécurité potentiels.
- Automatisation via une API — Amazon Inspector Classic peut être entièrement automatisé via une API. Cela vous permet d'intégrer des tests de sécurité dans le processus de conception et de développement, notamment la sélection, l'exécution et la communication des résultats de ces tests.

Accès à Amazon Inspector Classic

Vous pouvez utiliser le service Amazon Inspector Classic de l'une des manières suivantes :

Console Amazon Inspector Classic

Connectez-vous à la console Amazon Inspector Classic AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/inspector/.

La console est une interface basée sur un navigateur qui vous permet d'accéder au service Amazon Inspector Classic et de l'utiliser.

AWS SDK

AWS fournit des kits de développement logiciel (SDK) composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes. Celles-ci comprennent Java,

Python, Ruby, .NET, iOS, Android et bien plus encore. Les SDK constituent un moyen pratique de créer un accès programmatique au service Amazon Inspector Classic. Pour plus d'informations sur les AWS SDK, notamment sur la façon de les télécharger et de les installer, consultez la section Outils pour Amazon Web Services.

API HTTPS classique d'Amazon Inspector

Vous pouvez accéder à Amazon Inspector Classic et par AWS programmation à l'aide de l'API HTTPS Amazon Inspector Classic, qui vous permet d'envoyer des requêtes HTTPS directement au service. Pour plus d'informations, consultez le manuel Amazon Inspector Classic API Reference.

AWS Outils de ligne de commande

Vous pouvez utiliser les outils de ligne de AWS commande pour exécuter des commandes sur la ligne de commande de votre système afin d'effectuer des tâches Amazon Inspector Classic. Les outils de ligne de commande sont également utiles si vous souhaitez créer des scripts qui exécutent AWS des tâches. Pour plus d'informations, consultez l'interface de ligne de AWS commande Amazon Inspector Classic.

Terminologie et concepts Amazon Inspector Classic

Lorsque vous commencez à utiliser Amazon Inspector Classic, vous pouvez tirer parti de la découverte de ses concepts clés.

Agent Amazon Inspector Classic

Agent logiciel que vous pouvez installer sur les instances EC2 qui sont incluses dans l'objectif d'évaluation. L'agent recueille un vaste ensemble de données de configuration (télémétrie). Pour plus d'informations, consultez Agents Amazon Inspector Classic.

Exécution d'évaluation

Processus qui consiste à identifier les problèmes de sécurité potentiels en analysant la configuration de votre objectif d'évaluation en fonction des packages de règles spécifiés. Lors d'une exécution d'évaluation, Amazon Inspector surveille, collecte et analyse des données de configuration (télémétrie) à partir de ressources dans l'objectif spécifié. Amazon Inspector analyse ensuite ces données et les compare à un ensemble de règles de sécurité spécifié dans le modèle d'évaluation utilisé lors de l'exécution d'évaluation. Une exécution d'évaluation terminée produit une liste de résultats, qui sont des problèmes de sécurité potentiels ayant divers niveaux de

gravité. Pour plus d'informations, consultez Modèles d'évaluation et cycles d'évaluation Amazon Inspector Classic.

Objectif d'évaluation

Dans le contexte d'Amazon Inspector Classic, collection de ressources AWS qui fonctionnent ensemble comme une unité pour vous aider à réaliser vos objectifs commerciaux. Amazon Inspector Classic évalue l'état de sécurité des ressources qui constituent l'objectif d'évaluation.

> **Important**
>
> A l'heure actuelle, vos objectifs d'évaluation Amazon Inspector Classic ne peuvent être constitués que d'instances EC2. Pour de plus amples informations, veuillez consulterLimites de service Amazon Inspector Classic

Pour créer un objectif d'évaluation Amazon Inspector Classic, vous devez d'abord baliser vos instances EC2 avec les paires clé-valeur de votre choix. Ensuite, vous pouvez créer une vue de ces instances EC2 balisées qui ont des clés ou des valeurs communes. Pour plus d'informations, consultez Cibles d'évaluation Amazon Inspector Classic.

Modèle d'évaluation

Configuration qui est utilisée au cours de l'exécution d'évaluation. Le modèle comprend les éléments suivants :

- Packages de règles qu'Amazon Inspector Classic utilise pour évaluer votre objectif d'évaluation
- Rubriques Amazon SNS auxquelles vous souhaitez qu'Amazon Inspector Classic envoie des notifications sur les états et résultats de l'exécution d'évaluation
- Balises (paires clé-valeur) que vous pouvez affecter aux résultats qui sont générés par l'exécution d'évaluation
- Durée de l'exécution d'évaluation

Résultat

Problème de sécurité potentiel qu'Amazon Inspector Classic détecte lors de l'exécution d'évaluation de l'objectif spécifié. Les résultats sont affichés dans la console Amazon Inspector Classic ou extraits via l'API. Ils contiennent une description détaillée du problème de sécurité et une recommandation pour le résoudre. Pour plus d'informations, consultez Résultats d'Amazon Inspector Classic.

Règle

Dans le contexte d'Amazon Inspector Classic, contrôle de sécurité est effectué pendant une exécution d'évaluation. Lorsqu'une règle détecte un problème de sécurité potentiel, Amazon Inspector Classic génère un résultat qui décrit le problème.

Package de règles

Dans le contexte d'Amazon Inspector Classic, ensemble de règles. Un package de règles correspond à un objectif de sécurité que vous pourriez avoir. Vous pouvez spécifier votre objectif de sécurité en sélectionnant le package de règles approprié lorsque vous créez un modèle d'évaluation Amazon Inspector Classic. Pour plus d'informations, consultez Règles, packages et règles Amazon Inspector Classic.

Télémétrie

Informations sur les packages installés et la configuration logicielle pour une instance EC2. Amazon Inspector Classic recueille les données au cours d'une exécution d'évaluation.

Limites de service Amazon Inspector Classic

Le tableau suivant indique les limites d'Amazon Inspector Classic pour un compte AWS.

> **Important**
>
> A l'heure actuelle, vos objectifs d'évaluation de ne peuvent être constitués que d'instances EC2.

Les limites d'Amazon Inspector Classic par compte AWS et par région sont les suivantes :

Ressource	Limite par défaut	Commentaires
Les instances dans les évaluations en cours d'exécution	500	Le nombre maximum d'instances EC2 qui peuvent être incluses dans toutes les évaluations en cours d'exécution par compte et par région.

Ressource	Limite par défaut	Commentaires
Exécutions d'évaluation	50000	Nombre maximal d'exécutions d'évaluation que vous pouvez créer par compte et par région. Vous pouvez avoir plusieurs exécutions d'évaluation simultanées sous réserve que les objectifs d'évaluation utilisés pour ces exécutions ne contiennent pas d'instances EC2 se chevauchant.
Modèles d'évaluation	500	Nombre maximal de modèles d'évaluation que vous pouvez avoir à tout moment par compte et par région.
Objectifs d'évaluation	50	Nombre maximal de cibles d'évaluation que vous pouvez avoir à tout moment par compte et par région.

Sauf indication contraire, ces limites peuvent être augmentées sur simple demande en contactant leAWS SupportCenter.

Tarifs d'Amazon Inspector Classic

La tarification d'Amazon Inspector Classic est basée sur le nombre d'instances EC2 incluses dans chaque évaluation et sur les packages de règles utilisés dans ces évaluations.

Tarification du package de règles d'accessibilité au réseau

Les évaluations Amazon Inspector Classic avec les packages de règles d'accessibilité au réseau sont facturées par instance et par évaluation (évaluation des instances) et par mois. Par exemple, si vous exécutez une évaluation sur une instance, il s'agit d'une évaluation d'instance. Si vous exécutez une évaluation sur 10 instances, cela correspond à 10 évaluations d'instances. Le prix commence à 0,15 USD par évaluation d'instance par mois, avec des remises sur volume pour atteindre un niveau aussi bas que 0,04 USD par évaluation d'instance par mois.

Détails de l'essai gratuit

90 premiers jours d'utilisation d'Amazon Inspector Classic	Prix d'évaluation par instance
250 premières évaluations d'instances	0,00$

Informations de tarification

Au cours d'un mois donné	Prix d'évaluation par instance
250 premières évaluations d'instances	0,15$
Les 750 prochaines évaluations d'instances	0,13$
4 000 évaluations d'instances suivantes	0,10 USD
45 000 évaluations d'instances suivantes	0,07$
Toutes les autres évaluations d'instance	0,04$

Tarification des packages de règles d'évaluation des hôtes

Pour toute combinaison de vulnérabilités et d'expositions courantes (CVE), de benchmarks du Center for Internet Security (CIS), de meilleures pratiques de sécurité et d'analyse du comportement d'exécution incluse dans les évaluations

Les packages de règles d'évaluation des hôtes d'Amazon Inspector Classic utilisent un agent déployé sur les instances Amazon EC2 exécutant les applications que vous souhaitez évaluer. Les évaluations effectuées avec les packages de règles hôtes sont facturées par agent par évaluation (évaluation par agent) et par mois. Par exemple, si vous effectuez une évaluation sur un agent, il s'agit d'une évaluation d'agent. Si vous effectuez une évaluation sur 10 agents, cela correspond à 10 évaluations d'agents. Le prix commence à 0,30$ par évaluation d'agent par mois, avec des remises sur volume pour atteindre aussi peu que 0,05$ par évaluation d'agent par mois.

Détails de l'essai gratuit

90 premiers jours d'utilisation d'Amazon Inspector Classic	Prix d'évaluation par agent
250 premières évaluations d'agents	0,00$

Informations de tarification

Au cours d'un mois donné	Prix d'évaluation par agent
250 premières évaluations d'agents	0,30$
Les 750 prochaines évaluations d'agents	0,25$
4 000 prochaines évaluations d'agents	0,15$
Prochaines évaluations des 45 000 agents	0,10 USD
Toutes les autres évaluations des agents	0,05 USD

Systèmes d'exploitation et régions pris en charge par Amazon Inspector Classic

Ce chapitre fournit des informations sur les systèmes d'exploitation et les régions AWS pris en charge par Amazon Inspector Classic.

> **Important**
>
> Actuellement, les cibles d'évaluation Amazon Inspector Classic ne peuvent être constituées que d'instances EC2. Vous pouvez exécuter une évaluation sans agent avec le package de règles d'accessibilité réseau sur toutes les instances EC2, quel que soit le système d'exploitation.

Pour plus d'informations sur les packages de règles Amazon Inspector Classic disponibles sur les systèmes d'exploitation pris en charge, consultezEnsembles de règles Amazon Inspector Classic pour les systèmes d'exploitation pris en charge.

Rubriques

- Systèmes d'exploitation basés sur Linux pris en charge pour l'agent Amazon Inspector Classic
- Systèmes d'exploitation Windows pris en charge pour l'agent Amazon Inspector Classic
- Régions AWS prises en charge

Systèmes d'exploitation basés sur Linux pris en charge pour l'agent Amazon Inspector Classic

Vous pouvez utiliser l'agent Amazon Inspector Classic sur des instances x86 64 bits et Arm EC2. L'agent est compatible avec les versions suivantes des systèmes d'exploitation basés sur Linux :

- Instances x86 64 bits
  - Amazon Linux 2
  - Amazon Linux (2018.03, 2017.09, 2017.03, 2016.09, 2016.03, 2015.09, 2015.03, 2014.09, 2014.03, 2013.09, 2013.03, 2012.09, 2012.03)
  - Ubuntu (20,04 LTS, 18,04 LTS, 16,04 LTS, 14,04 LTS)
  - Debian (10.x, 9,0 - 9,5, 8,0 - 8,7)

  - Red Hat Enterprise Linux (8.x, 7.2 à 7.x, 6.2 à 6.9)
  - CentOS (7,2 à 7,x, 6,2 à 6,9)
- Instances Arm
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18,04 LTS, 16,04 LTS)

Systèmes d'exploitation Windows pris en charge pour l'agent Amazon Inspector Classic

Vous pouvez utiliser l'agent Amazon Inspector Classic uniquement sur les instances EC2 qui exécutent la version 64 bits des systèmes d'exploitation Windows suivants :

- Windows Server 2019 Base
- Windows Server 2016 Base
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Régions AWS prises en charge

Amazon Inspector Classic est pris en charge dans les régions AWS suivantes :

- US Est (Ohio) us-east-2
- USA Est (Virginie du Nord) us-east-1
- US Ouest (N. California) us-west-1
- USA Ouest (Oregon) us-west-2
- Asie-Pacifique (Mumbai) ap-south-1
- Asie-Pacifique (Séoul) ap-northeast-2
- Asie-Pacifique (Sydney) - ap-southeast-2
- Asie-Pacifique (Tokyo) - ap-northeast-1
- Europe (Francfort) eu-central-1

- Europe (Irlande) eu-west-1
- Europe (Londres) eu-west-2
- Europe (Stockholm) eu-north-1
- AWS GovCloud (USA Est) -1 gov-us-east
- AWS GovCloud (US-Ouest) -1 gov-us-west

> **Note**
>
> Le package de règles d'accessibilité du réseau n'est pas disponible dans les régions AWS GovCloud (États-Unis).

Passage au nouvel Amazon Inspector

Le nouvel Amazon Inspector est désormais disponible dans le monde entier en Régions AWS. Le nouvel Amazon Inspector est une version entièrement repensée et redessinée de l'actuel Amazon Inspector, désormais appelé Amazon Inspector Classic. Les fonctionnalités suivantes constituent les principales améliorations apportées à Amazon Inspector :

- Conçu pour évoluer — Le nouvel Amazon Inspector est conçu pour évoluer et s'adapter à un environnement cloud dynamique. Il n'y a aucune limite quant au nombre d'instances ou d'images pouvant être numérisées dans un compte.
- Support pour les images de conteneurs — Le nouvel Amazon Inspector analyse également les images de conteneurs résidant dans Amazon Elastic Container Registry (Amazon ECR) pour détecter les vulnérabilités logicielles.
- Support pour la gestion multi-comptes — Le nouvel Amazon Inspector est intégré à Organizations. Cela vous permet de déléguer un compte administrateur pour Amazon Inspector à votre organisation. Le compte d'administrateur délégué est un compte centralisé qui consolide tous les résultats et permet de configurer tous les comptes des membres.
- Utilise AWS Systems Manager un agent (agent SSM) : avec le nouvel Amazon Inspector, vous n'avez plus besoin d'installer et de gérer un agent Amazon Inspector autonome sur toutes vos instances EC2. Le nouvel Amazon Inspector tire parti de l'agent SSM largement déployé.
- Analyse automatisée et continue : avec Amazon Inspector Classic, vous définissez manuellement les objectifs d'évaluation, les modèles d'évaluation et configurez la fréquence des évaluations. Cependant, la nouvelle version d'Amazon Inspector détecte automatiquement toutes les instances EC2 récemment lancées et les images de conteneurs éligibles envoyées à Amazon ECR et les analyse immédiatement pour détecter les vulnérabilités logicielles et toute exposition involontaire au réseau. Les ressources sont automatiquement réanalysées en fonction de plusieurs déclencheurs, notamment le lancement d'une nouvelle instance EC2, le transfert d'une image de conteneur vers Amazon ECR, l'installation d'un nouveau package dans une instance EC2, l'installation d'un correctif ou la publication d'un nouveau code CVE (Common Vulnerabilities and Exposure) ayant un impact sur les ressources.
- Note de risque Amazon Inspector — Le nouvel Amazon Inspector calcule un score de risque Amazon Inspector pour vous aider à hiérarchiser vos résultats. Le score de risque est calculé en corrélant les informations up-to-date CVE avec des facteurs temporels et environnementaux tels que les informations d'accessibilité et d'exploitabilité du réseau.

- Intégrations supplémentaires : tous les résultats sont regroupés dans une console Amazon Inspector nouvellement conçue et transmis EventBridge à Amazon pour automatiser AWS Security Hub les flux de travail, tels que la billetterie. Les résultats relatifs aux images de conteneurs sont également transmis à Amazon ECR.

Pour en savoir plus sur toutes les fonctionnalités et les tarifs du nouvel Amazon Inspector, consultez le guide de l'utilisateur d'Amazon Inspector.

Bien que nous continuions à prendre en charge Amazon Inspector Classic pendant un certain temps et que les clients puissent utiliser à la fois le nouvel Amazon Inspector et Amazon Inspector Classic sur le même compte, nous vous encourageons vivement à migrer vers le nouvel Amazon Inspector. Les sections suivantes vous expliquent le processus de migration d'Amazon Inspector Classic vers le nouvel Amazon Inspector.

Rubriques

Étape 1 : (Facultatif) Exporter les rapports d'évaluation et les résultats

Pour enregistrer les rapports d'évaluation et les résultats dans Amazon Inspector Classic, générez un rapport d'évaluation.

Pour générer un rapport d'évaluation

1. Dans la page Exécutions d'évaluations, recherchez l'exécution pour laquelle vous souhaitez générer un rapport. Assurez-vous que son statut est « Analyse terminée ».
2. Choisissez l'icône de rapports sous la colonne Rapports de cette exécution d'évaluation.

> **Important**
>
> L'icône de rapport est présent dans la colonne Rapports uniquement pour les exécutions d'évaluation effectuées le 25 avril 2017 ou après. C'est à ce moment-là que les rapports d'évaluation d'Amazon Inspector Classic sont devenus disponibles.

3. Dans la boîte de dialogue Rapport d'évaluation, choisissez le type de rapport que vous souhaitez consulter (rapport de résultats ou rapport complet) et le format du rapport (HTML ou PDF). Choisissez ensuite de Générer le rapport.

Étape 2 : supprimer toutes les séries d'évaluation planifiées dans Amazon Inspector Classic

Pour désactiver Amazon Inspector Classic, supprimez tous les modèles d'évaluation de votre compte s'ils sont actifs Régions AWS. La suppression des modèles d'évaluation interrompt toutes vos futures séries d'évaluation planifiées.

Pour supprimer un modèle d'évaluation

- Sur la page Assessment Templates (Modèles d'évaluation), choisissez le modèle à supprimer, puis choisissez Delete (Supprimer). Lorsque vous êtes invité à confirmer l'opération, choisissez Yes (Oui).

> **Important**
>
> Lorsque vous supprimez un modèle d'évaluation, tous les modèles d'évaluation, toutes les exécutions d'évaluation, tous les résultats et toutes les versions des rapports associés à ce modèle sont également supprimés.

Étape 3 : activer le nouvel Amazon Inspector

Vous pouvez activer le nouvel Amazon Inspector à l'aide des AWS Management Console ou des nouvelles API Amazon Inspector. Pour commencer à utiliser le nouvel Amazon Inspector, consultez Getting Started dans le guide de l'utilisateur d'Amazon Inspector.

Démarrage route route route route route route route route route route route

Ce didacticiel vous montre comment configurer Amazon Inspector Classic et démarrer votre première évaluation par la création et l'exécution de votre première évaluation.

Configuration en un clic

La procédure suivante explique comment créer et exécuter une évaluation automatique à l'aide d'un modèle prédéfini et de paramètres de planification prédéfinis (une fois par semaine ou une seule fois) sur toutes les instances Amazon Elastic Compute Cloud (Amazon EC2) disponibles dans les versions actuellesCompte AWS etRégion AWS.

1. Connectez-vous àAWS Management Console et ouvrez la console Amazon Inspector Classic à l'adresse https://console.aws.amazon.com/inspector/.
2. Sur la page Welcome (Bienvenue), choisissez le type d'évaluation que vous souhaitez exécuter. Les évaluations du réseau analysent les configurations réseau de votreAWS environnement pour détecter les vulnérabilités et ne nécessitent pas d'agent Amazon Inspector Classic. Les évaluations des hôtes analysent les logiciels et les configurations sur l'hôte de vos instances EC2 pour détecter les vulnérabilités et nécessitent l'installation d'un agent sur les instances EC2.

   Choisissez soit Exécuter chaque semaine (recommandé) ou Exécuter une fois. Dès que vous effectuez votre choix, le service crée automatiquement l'évaluation pour vous. Le service exécute en particulier les opérations suivantes :

   a. Crée un rôle lié à un service.

      > **Note**
      >
      > Pour identifier les instances EC2 spécifiées dans les cibles d'évaluation, Amazon Inspector Classic doit énumérer vos instances et vos balises EC2. Amazon Inspector Classic accède à ces ressources par leCompte AWS biais d'un rôle lié à un service appeléAWSServiceRoleForAmazonInspector. Pour plus d'informations sur les rôles liés à un service, consultez Utilisation de rôles liés à un service pour Amazon Inspector Classic et Utilisation des rôles liés à un service.

b. Le cas échéant, installe un agent Amazon Inspector Classic sur toutes les instances EC2 disponibles dans votreCompte AWS région.

> **Note**
>
> Le service installe un agent Amazon Inspector Classic uniquement sur les instances EC2 qui autorisentAWS Systems Manager Run Command. Pour utiliser cette option, assurez-vous que toutes vos instances EC2Région AWS sont actuellesCompte AWS, que l'agent SSM est installé et qu'elles disposent d'un rôle IAM autorisant Run Command. Pour plus d'informations, veuillez consulter Installer l'agent sur plusieurs instances EC2 à l'aide de Systems Manager Run Command.

c. Ajoute ces instances à un objectif d'évaluation.

d. Inclut la cible dans un modèle d' évaluation normalisé avec un ensemble de packages de règles.

e. Exécute l'évaluation de manière hebdomadaire ou une seule fois, selon que vous choisissez Exécuter chaque semaine (recommandé) ou Exécuter une fois.

3. Dans la boîte de dialogue de confirmation, choisissez OK. Amazon Inspector Classic exécute automatiquement votre évaluation.

Configuration avancée

La procédure suivante vous montre comment sélectionner des instances Amazon EC2, des packages de règles et des paramètres de planification spécifiques à inclure dans un objectif et un modèle d'évaluation.

1. Sur la page Bienvenue, sélectionnez Configuration avancée.
2. Sur la page Définition d'un objectif d'évaluation, saisissez le nom de votre objectif d'évaluation.
3. Pour Toutes les instances, vous pouvez laisser la case cochée pour inclure toutes les instances EC2 de votreCompte AWS région dans l'objectif d'évaluation. Si vous souhaitez choisir les instances EC2 à inclure, désactivez la case à cocher Toutes les instances et entrez les balises Key et Value associées aux instances EC2 cibles. Pour plus d'informations sur le balisage de vos instances EC2, consultez Balisage de vos ressources Amazon EC2.
4. Pour les agents d'installation, vous pouvez laisser la case cochée par défaut si vos instances autorisent System Manager Run Command. Le service installe un agent Amazon Inspector Classic sur toutes les instances EC2 de la cible d'évaluation qui le permetAWS Systems

Manager. Pour utiliser cette option, assurez-vous que toutes vos instances EC2Région AWS sont actuellesCompte AWS, que l'agent SSM est installé et qu'elles disposent d'un rôle IAM autorisant Run Command. Pour plus d'informations, veuillez consulter Installer l'agent sur plusieurs instances EC2 à l'aide de Systems Manager Run Command. Si vous souhaitez installer manuellement l'agent, consultez la section Installation des agents Amazon Inspector.

5. Choisissez Next (Suivant).
6. Sur la page Définition d'un objectif d'évaluation, saisissez le nom de votre modèle d'évaluation.
7. Dans Packages de règles, choisissez les packages de règles à inclure dans le modèle d'évaluation. Pour plus d'informations sur les packages de règles, consultez Règles et packages de règles d'Amazon Inspector.
8. Pour Durée, choisissez la durée de l'exécution d'une évaluation.
9. (Facultatif) Dans Calendrier d'évaluation, définissez un calendrier pour les cycles d'évaluation récurrents.
10. Choisissez Next (Suivant).
11. Sur la page Révision, vérifiez vos choix concernant l'objectif et le modèle d'évaluation. Si vous êtes satisfait de votre configuration, choisissez Create Créer) Créer) Créer) Créer) Créer) Créer) Si vous définissez un calendrier d'évaluation pour votre modèle d'évaluation, l'évaluation s'exécutera automatiquement après que vous choisissez créer.

> **Note**
>
> Pour identifier les instances EC2 spécifiées dans les cibles d'évaluation, Amazon Inspector Classic doit énumérer vos instances et vos balises EC2. Amazon Inspector Classic accède à ces ressources par leCompte AWS biais d'un rôle lié à un service appelé`AWSServiceRoleForAmazonInspector`. Pour plus d'informations sur l'utilisation des rôles liés à un service dans Amazon Inspector Classic, veuillez consulterUtilisation de rôles liés à un service pour Amazon Inspector Classic. Pour des informations détaillées sur l'utilisation des rôles liés à un service, veuillez consulter Utilisation des rôles liés à un service, veuillez consulter Utilisation des rôles liés à un service).AWS Identity and Access Management

12. Si vous n'avez pas configuré de calendrier d'évaluation, accédez à votre modèle d'évaluation par le biais de la console, puis choisissez Exécuter.

13. Pour suivre la progression de l'exécution de l'évaluation, dans le volet de navigation de la console, choisissez Exécutions d'évaluation, puis Résultats. Pour plus d'informations sur les résultats, consultez Résultats d'Amazon Inspector Classic.

Didacticiels pour Amazon Inspector Classic

Les didacticiels suivants vous montrent comment exécuter les exécutions d'évaluation Amazon Inspector Classic sur les systèmes d'exploitation Red Hat Enterprise Linux et Ubuntu.

Didacticiels

- Didacticiel : Utilisation d'Amazon Inspector Classic avec Red Hat Enterprise Linux
- Didacticiel : Utilisation d'Amazon Inspector Classic avec Ubuntu Server

Didacticiel Amazon Inspector Classic - Red Hat Enterprise Linux

Avant de suivre les instructions de ce didacticiel, nous vous recommandons de vous familiariser avec les Terminologie et concepts Amazon Inspector Classic.

Ce didacticiel explique comment utiliser Amazon Inspector Classic afin d'analyser le comportement d'une instance EC2 qui exécute le système d'exploitation Red Hat Enterprise Linux 7.5. Il fournit des instructions étape par étape sur la façon de parcourir le flux de travail Amazon Inspector Classic. Le flux de travail inclut la préparation des instances Amazon EC2, l'exécution d'un modèle d'évaluation et l'application des correctifs de sécurité recommandés générés dans les résultats de l'évaluation. Si vous êtes un nouveau utilisateur et que vous souhaitez configurer et exécuter une évaluation Amazon Inspector Classic en un clic, consultez la sectionCréation d'une évaluation de base.

Rubriques

- Étape 1 : Configurez une instance Amazon EC2 à utiliser avec Amazon Inspector Classic
- Étape 2 : Modifier votre instance Amazon EC2
- Étape 3 : Créer un objectif d'évaluation et installer un agent sur l'instance EC2
- Étape 4 : Créer et exécuter votre modèle d'évaluation
- Étape 5 : Localisez et analysez votre résultat
- Étape 6 : Appliquer le correctif recommandé à votre objectif d'évaluation

Étape 1 : Configurez une instance Amazon EC2 à utiliser avec Amazon Inspector Classic

Pour ce didacticiel, créez une instance EC2 exécutant Red Hat Enterprise Linux 7.5, et balisez-la à l'aide de la consoleNomet une valeur de**`InspectorEC2InstanceLinux`**.

> **Note**
>
> Pour plus d'informations sur le balisage des instances EC2, consultez Ressources et balises.

Étape 2 : Modifier votre instance Amazon EC2

Pour ce didacticiel, vous allez modifier votre instance EC2 cible afin de l'exposer au problème de sécurité potentiel CVE-2018-1111. Pour plus d'informations, consultez https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111 et Vulnérabilités et expositions courantes.

Exécutez la commande suivante tout en étant connecté à votre instance **`InspectorEC2InstanceLinux`** :

```
sudo yum install dhclient-12:4.2.5-68.el7
```

Pour obtenir plus d'informations sur la connexion à une instance EC2, consultez la sectionConnectez-vous à votre instancedans leGuide de l'utilisateur Amazon EC2.

Étape 3 : Créer un objectif d'évaluation et installer un agent sur l'instance EC2

Amazon Inspector Classic utilise des objectifs d'évaluation afin de désigner les ressources AWS que vous voulez évaluer.

Pour créer un objectif d'évaluation et installer un agent sur une instance EC2

1. Connectez-vous à la consoleAWS Management Consoleet ouvrez la console Amazon Inspector Classic à l'adressehttps://console.aws.amazon.com/inspector/.
2. Dans le volet de navigation, choisissez Objectifs d'évaluation, puis Créer.

   Procédez comme suit :

   a. Dans Nom, saisissez le nom de votre objectif d'évaluation.

Dans le cadre de ce didacticiel, entrez **`MyTargetLinux`**.

b. PourUtiliser des balises, sélectionnez les instances EC2 que vous voulez ajouter à cet objectif d'évaluation en saisissant des valeurs pour la consoleCléetValeur.

   Dans le cadre de ce didacticiel, sélectionnez l'instance EC2 que vous avez créée à l'étape précédente en entrant **`Name`** dans le champ Clé et **`InspectorEC2InstanceLinux`** dans le champ Valeur.

   Cochez la case Toutes les instances afin d'inclure toutes les instances EC2 de votre compte et de votre région AWS dans cet objectif d'évaluation.

c. Choisissez Save (Enregistrer).

d. Installez un agent Amazon Inspector Classic sur votre instance EC2 balisée. Pour installer un agent sur toutes les instances EC2 incluses dans un objectif d'évaluation, sélectionnez la case Installer des agents.

   > **Note**
   >
   > Vous pouvez également installer l'agent Amazon Inspector Classic à l'aide de la consoleRun Command d'AWS Systems Manager. Pour installer l'agent sur toutes les instances dans l'objectif d'évaluation, vous pouvez spécifier les mêmes balises que celles utilisées pour créer l'objectif d'évaluation. Ou vous pouvez installer l'agent Amazon Inspector Classic sur votre instance EC2 manuellement. Pour plus d'informations, consultez Installation des agents Amazon Inspector Classic.

e. Choisissez Enregistrer.

> **Note**
>
> À ce moment, Amazon Inspector Classic crée un rôle lié au service, nomméAWSServiceRoleForAmazonInspector. Le rôle accorde à Amazon Inspector Classic l'accès nécessaire à vos ressources. Pour plus d'informations, consultez Création d'un rôle lié à un service pour Amazon Inspector Classic.

Étape 4 : Créer et exécuter votre modèle d'évaluation

Pour créer et exécuter votre modèle

1. Dans le volet de navigation, choisissez Modèles d'évaluation, puis Créer.
2. Dans Nom, saisissez le nom de votre modèle d'évaluation. Dans le cadre de ce didacticiel, entrez **`MyFirstTemplateLinux`**.
3. Pour Nom de l'objectif, sélectionnez l'objectif d'évaluation que vous avez créé ci-dessus, **`MyTargetLinux`**.
4. Dans Packages de règles, choisissez les packages de règles que vous voulez utiliser dans ce modèle d'évaluation.

   Pour ce didacticiel, choisissez Vulnérabilités et expositions courantes 1.1.
5. Pour Durée, spécifiez la durée de votre modèle d'évaluation.

   Pour ce didacticiel, sélectionnez 15 minutes.
6. Choisissez Créer et exécuter.

Étape 5 : Localisez et analysez votre résultat

Une exécution d'évaluation terminée produit un ensemble de résultats : les problèmes de sécurité potentiels qu'Amazon Inspector Classic détecte dans votre objectif d'évaluation. Vous pouvez consulter les résultats et suivre les étapes recommandées pour résoudre les problèmes de sécurité potentiels.

Dans ce didacticiel, si vous avez effectué les étapes précédentes, votre exécution d'évaluation produit un résultat correspondant à la vulnérabilité courante CVE-2018-1111.

Pour localiser et analyser votre résultat

1. Dans le volet de navigation, choisissez Assessment runs (Exécutions d'évaluation). Vérifiez que le statut de l'exécution du modèle d'évaluation appelé MyFirstTemplateLinux est défini sur Collecte de données. Cela indique que l'exécution d'évaluation est actuellement en cours, et que les données télémétriques de votre objectif sont collectées et analysées par rapport aux packages de règles sélectionnés.

2. Vous ne pouvez pas consulter les résultats générés par l'exécution d'évaluation alors qu'elle est toujours en cours. Laissez l'exécution d'évaluation s'exécuter pendant toute sa durée. Toutefois, pour ce didacticiel, vous pouvez arrêter l'exécution au bout de quelques minutes.

   Le statut de MyFirstTemplateLinux passe d'abord à Arrêt en cours, puis, quelques minutes plus tard, à Analyse en cours, puis enfin à Analyse terminée. Pour voir ce changement de statut, sélectionnez l'icône Actualiser.

3. Dans le volet de navigation, choisissez Conclusions.

   Vous pouvez voir un nouveau résultat, dont la gravité est élevée, indiquant que l'instance InspectorEC2InstanceLinux est vulnérable à CVE-2018-1111.

   > **Note**
   >
   > Si vous ne voyez pas ce nouveau résultat, sélectionnez l'icône Actualiser.

   Pour développer la vue et voir les détails de ce résultat, sélectionnez la flèche à gauche du résultat. Les détails du résultat incluent les éléments suivants :

   - ARN du résultat
   - Nom de l'exécution d'évaluation qui a produit ce résultat
   - Nom de l'objectif d'évaluation qui a produit ce résultat
   - Nom du modèle d'évaluation qui a produit ce résultat
   - Heure de début de l'exécution d'évaluation
   - Heure de fin de l'exécution d'évaluation
   - Statut de l'exécution d'évaluation
   - Nom du package de règles qui inclut la règle qui a déclenché ce résultat
   - ID d'agent Amazon Inspector Classic
   - Nom du résultat
   - Gravité du résultat
   - Description du résultat
   - Étapes de résolution recommandées que vous pouvez exécuter pour résoudre le problème de sécurité potentiel décrit par le résultat

Étape 6 : Appliquer le correctif recommandé à votre objectif d'évaluation

Pour ce didacticiel, vous avez modifié votre objectif d'évaluation afin de l'exposer au problème de sécurité potentiel CVE-2018-1111. Dans cette procédure, vous appliquez la correction recommandée pour le problème.

Pour appliquer le correctif à votre cible

1. Connectez-vous à l'instance **`InspectorEC2InstanceLinux`** que vous avez créée dans la section précédente et exécutez la commande suivante :

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```

2. Dans la page Modèles d'évaluation, sélectionnez MyFirstTemplateLinux, puis choisissez Exécuter pour commencer une nouvelle exécution d'évaluation à l'aide de ce modèle.
3. Suivez les étapes de Étape 5 : Localisez et analysez votre résultat pour voir les résultats produits par cette nouvelle exécution du modèle MyFirstTemplateLinux.

   Étant donné que vous avez résolu le problème de sécurité CVE-2018-1111, vous ne devrez plus voir de résultat pour celui-ci.

Didacticiel Amazon Inspector Classic - Ubuntu Server

Avant de suivre les instructions de ce didacticiel, nous vous recommandons de vous familiariser avec les Terminologie et concepts Amazon Inspector Classic.

Ce didacticiel montre comment utiliser Amazon Inspector Classic pour analyser le comportement d'une instance EC2 qui exécute le système d'exploitation Ubuntu Server 16.04 LTS. Il fournit des instructions étape par étape sur la façon de parcourir le flux de travail Amazon Inspector Classic.

Si vous êtes un nouveau utilisateur et que vous souhaitez configurer et exécuter une évaluation Amazon Inspector Classic en un clic, consultez la sectionCréation d'une évaluation de base.

Rubriques

- Étape 1 : Configurez une instance Amazon EC2 à utiliser avec Amazon Inspector Classic
- Étape 2 : Créer un objectif d'évaluation et installer un agent sur l'instance EC2
- Étape 3 : Créer et exécuter votre modèle d'évaluation
- Étape 4 : Rechercher et analyser les résultats générés

Étape 1 : Configurez une instance Amazon EC2 à utiliser avec Amazon Inspector Classic

Pour configurer une instance EC2

- Pour ce didacticiel, créez une instance EC2 exécutant Ubuntu Server 16.04 LTS et balisez-la à l'aide de la consoleNomUne clé et une valeur de**`InspectorEC2InstanceUbuntu`**.

> **Note**
>
> Pour plus d'informations sur le balisage des instances EC2, consultez Ressources et balises.

Étape 2 : Créer un objectif d'évaluation et installer un agent sur l'instance EC2

Amazon Inspector Classic utilise des objectifs d'évaluation pour désigner les ressources AWS à évaluer.

Pour créer un objectif d'évaluation et installer un agent sur l'instance EC2

1. Connectez-vous à la consoleAWS Management Consoleet ouvrez la console Amazon Inspector Classic à l'adressehttps://console.aws.amazon.com/inspector/.
2. Dans le volet de navigation, choisissez Objectifs d'évaluation, puis Créer.
3. Dans Nom, saisissez le nom de votre objectif d'évaluation.

   Dans le cadre de ce didacticiel, entrez **`MyTargetUbuntu`**.
4. PourUtiliser des balises, sélectionnez les instances EC2 que vous voulez inclure dans cette objectif d'évaluation en saisissant des valeurs pour la consoleCléetValeur.

   Dans le cadre de ce didacticiel, sélectionnez l'instance EC2 que vous avez créée à l'étape précédente en entrant **`Name`** dans le champ Clé et **`InspectorEC2InstanceUbuntu`** dans le champ Valeur.

Cochez la case à Toutes les instances afin d'inclure toutes les instances EC2 de votre compte et de votre région AWS dans cet objectif d'évaluation.

5. Installez un agent Amazon Inspector Classic sur votre instance EC2 balisée. Pour installer un agent sur toutes les instances EC2 incluses dans un objectif d'évaluation, sélectionnez la case Installer des agents.

> **Note**
>
> Vous pouvez également installer l'agent Amazon Inspector à l'aide de la fonctionnalité Exécuter la commande de Systems Manager. Pour installer l'agent sur toutes les instances dans l'objectif d'évaluation, vous pouvez spécifier les mêmes balises que celles utilisées pour créer l'objectif d'évaluation. Ou vous pouvez installer l'agent Amazon Inspector sur votre instance EC2 manuellement. Pour plus d'informations, consultez Installation des agents Amazon Inspector Classic.

6. Choisissez Enregistrer.

> **Note**
>
> À ce stade, un rôle lié à un service appeléAWSServiceRoleForAmazonInspectorest créé pour accorder à Amazon Inspector Classic l'accès à vos ressources. Pour plus d'informations, consultez Création d'un rôle lié à un service pour Amazon Inspector Classic.

Étape 3 : Créer et exécuter votre modèle d'évaluation

Pour créer et exécuter votre modèle

1. Si vous utilisez Configuration avancée, vous serez dirigé vers la page Définition d'un modèle d'évaluation. Sinon, naviguez vers la page Modèles d'évaluation, puis sélectionnez Créer.
2. Dans Nom, saisissez le nom de votre modèle d'évaluation. Dans le cadre de ce didacticiel, entrez **`MyFirstTemplateUbuntu`**.
3. Pour Nom de l'objectif, sélectionnez l'objectif d'évaluation que vous avez créé ci-dessus, **`MyTargetUbuntu`**.
4. Pour Ensembles de règles, utilisez le menu déroulant pour choisir les packages de règles que vous souhaitez utiliser dans ce modèle d'évaluation.

Pour ce didacticiel, choisissez Vulnérabilités et expositions courantes 1.1.

5. Pour Durée, spécifiez la durée de votre modèle d'évaluation.

   Pour ce didacticiel, choisissez 15 minutes.

6. Si vous utilisez Configuration avancée, choisissez Suivant. Sur la page Révision suivante, choisissez Créer. Sinon ,choisissez Créer et exécuter.

Étape 4 : Rechercher et analyser les résultats générés

Une exécution d'évaluation terminée produit un ensemble de résultats : les problèmes de sécurité potentiels qu'Amazon Inspector Classic détecte dans votre objectif d'évaluation. Vous pouvez consulter les résultats et suivre les étapes recommandées pour résoudre les problèmes de sécurité potentiels.

1. Accédez à la page Exécutions d'évaluations. Vérifiez que le statut de l'exécution du modèle d'évaluation nommé MyFirstTemplateUbuntu que vous avez créé à l'étape précédente est défini sur Collection de données. Cela indique que l'exécution d'évaluation est actuellement en cours, et que les données télémétriques de votre objectif sont collectées et analysées par rapport aux packages de règles sélectionnés.
2. Vous ne pouvez pas consulter les résultats générés par l'exécution d'évaluation alors qu'elle est toujours en cours. Laissez l'exécution d'évaluation s'exécuter pendant toute sa durée.

   Le statut de MyFirstTemplateUbuntu passe d'abord à Arrêt en cours, puis, quelques minutes plus tard, à Analyse en cours, puis enfin à Analyse terminée. Pour voir ce changement de statut, sélectionnez l'icône Actualiser.

3. Accédez à la page de Résultats.

   Pour développer la vue et voir les détails d'une recherche, sélectionnez la flèche à gauche de la recherche. Les détails du résultat incluent les éléments suivants :

   - ARN du résultat
   - Nom de l'exécution d'évaluation qui a produit ce résultat
   - Nom de l'objectif d'évaluation qui a produit ce résultat
   - Nom du modèle d'évaluation qui a produit ce résultat
   - Heure de début de l'exécution d'évaluation

- Heure de fin de l'exécution d'évaluation
- Statut de l'exécution d'évaluation
- Nom du package de règles qui inclut la règle qui a déclenché la recherche
- ID d'agent Amazon Inspector Classic
- Nom du résultat
- Gravité du résultat
- Description du résultat
- Étapes de résolution recommandées que vous pouvez exécuter pour résoudre le problème de sécurité potentiel décrit par le résultat

Étape 5 : Appliquer la correction recommandée à votre objectif d'évaluation

Dans cette procédure, vous appliquez une mise à jour pour résoudre les problèmes qu'a détectés.

1. Connectez-vous à votre instance**`InspectorEC2InstanceUbuntu`**, et effectuez une mise à jour du package.
2. Dans la page Modèles d'évaluation, choisissez MyFirstTemplateUbuntu, puis choisissez Exécuter pour commencer une nouvelle exécution d'évaluation à l'aide de ce modèle.
3. Suivez les étapes de Étape 4 : Rechercher et analyser les résultats générés pour voir les résultats produits par cette nouvelle exécution du modèle MyFirstTemplateUbuntu.

   La mise à jour du package doit avoir corrigé les résultats de la première exécution du modèle.

Sécurité dans Amazon Inspector Classic

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 Classic, consultez AWS Services in Scope .
- 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 Classic. Les rubriques suivantes expliquent comment configurer Amazon Inspector Classic pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS qui vous aident à surveiller et à sécuriser vos ressources Amazon Inspector Classic.

Rubriques

- Bonnes pratiques de sécurité pour Amazon Inspector Classic

Protection des données dans Amazon Inspector Classic

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Inspector Classic. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels

que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon Inspector Classic ou une autre solution services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Rubriques

Chiffrement de données au repos

Les données de télémétrie générées par un agent Amazon Inspector Classic lors des évaluations sont formatées dans des fichiers JSON. Ces fichiers sont transmis near-real-time via TLS à Amazon Inspector Classic, où ils sont chiffrés à l'aide d'une clé per-assessment-run dérivée éphémère AWS KMS.

Les fichiers sont stockés en toute sécurité dans des compartiments S3 dédiés à Amazon Inspector Classic. Le moteur de règles d'Amazon Inspector Classic effectue les opérations suivantes :

- Accède aux données de télémétrie chiffrées dans le compartiment S3
- Déchiffre ces données en mémoire
- Traite les données en fonction des règles d'évaluation configurées pour générer des résultats

Chiffrement des données en transit

En tant que service géré, Amazon Inspector Classic 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 Classic 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.

Identity and Access Management pour Amazon Inspector Classic

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

- Rôles liés à un service pour Amazon Inspector
- Exemples de politiques basées sur l'identité pour Amazon Inspector Classic
- Utilisation de rôles liés à un service pour Amazon Inspector Classic
- Résolution des problèmes d'identité et d'accès à Amazon Inspector Classic

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 Classic.

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 Classic 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 Classic

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 vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent

des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains services AWS utilisent des fonctionnalités dans d'autres services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et service AWS, associées service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal

(utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de

confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon Inspector Classic 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 Classic

Fonction IAM	Assistance Amazon Inspector
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non

Fonction IAM	Assistance Amazon Inspector
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Amazon Inspector et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur 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 Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou

refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour Amazon Inspector

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector Classic

Politiques basées sur les ressources dans Amazon Inspector

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour Amazon Inspector

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions Amazon Inspector, consultez la section Actions définies par Amazon Inspector Classic dans le Service Authorization Reference.

Les actions politiques dans Amazon Inspector utilisent le préfixe suivant avant l'action :

```
inspector
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "inspector:action1",
      "inspector:action2"
         ]
```

La stratégie d'autorisation suivante accorde des autorisations à l'utilisateur pour exécuter toutes les opérations commençant par `Describe` et `List`. Ces opérations affichent des informations sur une ressource Amazon Inspector, telles qu'un objectif d'évaluation ou un résultat. Le caractère générique (*) dans l'`Resource`élément indique que les opérations sont autorisées pour toutes les ressources Amazon Inspector détenues par le compte :

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
            "inspector:Describe*",
            "inspector:List*"
            ],
         "Resource":"*"
      }
   ]
}
```

Exemple 2 : autoriser un utilisateur à effectuer des opérations de description et de liste uniquement sur la base des résultats d'Amazon Inspector

La stratégie d'autorisation suivante accorde des autorisations d'utilisateur pour exécuter uniquement les opérations `ListFindings` et `DescribeFindings`. Ces opérations affichent des informations sur les résultats d'Amazon Inspector. Le caractère générique (*) dans l'`Resource`élément indique que les opérations sont autorisées pour toutes les ressources Amazon Inspector détenues par le compte.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. [Exemples de politiques basées sur l'identité pour Amazon Inspector Classic]

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 de leurs ARN, consultez la section Ressources définies par Amazon Inspector Classic dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon Inspector Classic.

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector Classic

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 Classic 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 Classic.

Pour consulter des exemples de politiques basées sur l'identité d'Amazon Inspector, consultez. Exemples de politiques basées sur l'identité pour Amazon Inspector Classic

ACL dans Amazon Inspector

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Amazon Inspector

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Amazon Inspector

Prend en charge les informations d'identification temporaires	Oui

Certains services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui services AWS fonctionnent avec des informations d'identification temporaires, consultez services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Amazon Inspector

Prend en charge les 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 fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités d'Amazon Inspector. Modifiez les rôles de service uniquement lorsque Amazon Inspector fournit des instructions à cet effet.

Rôles liés à un service pour Amazon Inspector

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour en savoir plus sur la création ou la gestion des rôles liés aux services Amazon Inspector, consultez. Utilisation de rôles liés à un service pour Amazon Inspector Classic

Exemples de politiques basées sur l'identité pour Amazon Inspector Classic

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon Inspector. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Amazon Inspector, y compris le format des ARN pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour Amazon Inspector Classic 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 un utilisateur à effectuer des opérations de description et de liste uniquement sur la base des résultats d'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.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Amazon Inspector

Pour accéder à la console Amazon Inspector Classic, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon Inspector de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Amazon Inspector, associez également Amazon Inspector *ConsoleAccess* ou la politique *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Autoriser un utilisateur à effectuer des opérations de description et de liste uniquement sur la base des résultats d'Amazon Inspector

La stratégie d'autorisation suivante accorde des autorisations d'utilisateur pour exécuter uniquement les opérations `ListFindings` et `DescribeFindings`. Ces opérations affichent des informations sur les résultats d'Amazon Inspector. Le caractère générique (*) dans l'`Resource`élément indique que les opérations sont autorisées pour toutes les ressources Amazon Inspector détenues par le compte.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Utilisation de rôles liés à un service pour Amazon Inspector Classic

Amazon Inspector Classic utilise des rôles AWS Identity and Access Management liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon Inspector Classic. Les rôles liés à un service sont prédéfinis par Amazon Inspector Classic et incluent toutes les autorisations requises par le service pour appeler d'autres personnes en votre services AWS nom.

Un rôle lié à un service facilite la configuration d'Amazon Inspector Classic, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Amazon Inspector Classic définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Amazon Inspector Classic peut assumer ses rôles. 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 pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources Amazon Inspector Classic, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour Amazon Inspector Classic

Amazon Inspector Classic utilise le rôle lié au service nommé AWSServiceRoleForAmazonInspector—. ServiceLinkedRoleDescription

Le rôle AWSServiceRoleForAmazonInspector lié à un service fait confiance aux services suivants pour assumer le rôle :

- `inspector.amazonaws.com`

La politique d'autorisations de rôle nommée AmazonInspectorServiceRolePolicy permet à Amazon Inspector Classic d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `iam:CreateServiceLinkedRole` sur `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector`

Vous devez configurer les autorisations pour autoriser une entité IAM (telle qu'un utilisateur, un groupe ou un rôle IAM) 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.

Création d'un rôle lié à un service pour Amazon Inspector Classic

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous CompleteThisCreateActionInThisService utilisez l'API AWS Management Console AWS CLI, le ou l' AWS API, Amazon Inspector Classic crée pour vous le rôle lié au service.

Modification d'un rôle lié à un service pour Amazon Inspector Classic

Amazon Inspector Classic ne vous permet pas de modifier le rôle AWSServiceRoleForAmazonInspector lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Amazon Inspector Classic

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez pas d'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.

> **Note**
>
> Si le service Amazon Inspector Classic utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Amazon Inspector Classic utilisées par **`AWSServiceRoleForAmazonInspector`**

- Supprimez vos objectifs d'évaluation pour cela Compte AWS dans tous les sites sur Régions AWS lesquels Amazon Inspector Classic est en cours d'exécution. Pour plus d'informations, consultez Cibles d'évaluation Amazon Inspector Classic.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForAmazonInspector service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service Amazon Inspector Classic

Amazon Inspector Classic prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison AWS.

Résolution des problèmes d'identité et d'accès à Amazon Inspector Classic

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 `inspector:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector: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 `inspector:`*`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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon Inspector prend en charge ces fonctionnalités, consultezComment Amazon Inspector Classic 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 connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Journalisation et surveillance dans Amazon Inspector Classic

Amazon Inspector Classic est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans Amazon Inspector Classic. CloudTrail capture tous les appels d'API pour Amazon Inspector Classic sous forme d'événements, y compris les appels depuis la console Amazon Inspector Classic et les appels de code vers les opérations d'API Amazon Inspector Classic.

Pour plus d'informations sur l'utilisation de la CloudTrail connexion dans Amazon Inspector Classic, consultezJournalisation des appels d'API Amazon Inspector Classic avecAWS CloudTrail.

Vous pouvez surveiller Amazon Inspector Classic à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes pour en faire des indicateurs lisibles en temps quasi réel. Par défaut, Amazon Inspector Classic envoie des données métriques par CloudWatch intervalles de 5 minutes.

Pour plus d'informations sur l'utilisation CloudWatch d'Amazon Inspector Classic, consultezSurveillance d'Amazon Inspector Classic à l'aide d'Amazon CloudWatch.

Réponse aux incidents dans Amazon Inspector Classic

La réponse aux incidents pour Amazon Inspector Classic est une AWS responsabilité. AWS dispose d'une politique et d'un programme formels et documentés qui régissent la réponse aux incidents.

AWS les problèmes opérationnels ayant un impact important sont publiés sur le AWS Service Health Dashboard.

Les problèmes opérationnels sont également postés dans les comptes individuels via le AWS Health Dashboard. Pour plus d'informations sur l'utilisation du AWS Health Dashboard, consultez le guide de AWS Health l'utilisateur.

Validation de conformité pour Amazon Inspector Classic

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon Inspector Classic dans le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour obtenir la liste des AWS services concernés par des programmes de conformité spécifiques, voir Services AWS concernés par programme de conformité . 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, consultez Téléchargement de rapports dans AWS Artifact.

Lorsque vous utilisez Amazon Inspector Classic, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides démarrage rapide de la sécurité et de la conformité. Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.
- 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.
- 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— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans Amazon Inspector Classic

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Amazon Inspector Classic est hautement disponible et exécute des requêtes à l'aide de ressources de calcul dans plusieurs zones de disponibilité. Il achemine automatiquement les requêtes de manière appropriée si aucune zone de disponibilité particulière n'est accessible.

Amazon Inspector Classic utilise Amazon S3 comme magasin de données sous-jacent, ce qui rend vos données hautement disponibles et durables. Amazon S3 fournit une infrastructure durable pour stocker les données importantes. Conçu pour offrir une durabilité de 99,999999999 % des objets Vos données sont stockées de manière redondante sur plusieurs installations et sur plusieurs appareils au sein de chaque installation.

Sécurité de l'infrastructure dans Amazon Inspector Classic

En tant que service géré, Amazon Inspector Classic 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 Classic 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.

Pour plus d'informations sur la sécurité du réseau et des agents Amazon Inspector Classic, consultezthe section called "Sécurité du réseau et des agents Amazon Inspector Classic".

Analyse de configuration et de vulnérabilité dans Amazon Inspector Classic

Amazon Inspector Classic propose un logiciel prédéfini appelé agent que vous pouvez éventuellement installer dans le système d'exploitation des instances EC2 que vous souhaitez évaluer. L'agent recueille un vaste ensemble de données de configuration, connu sous le nom de télémétrie. Pour plus d'informations sur les agents Amazon Inspector Classic, consultezAgents Amazon Inspector Classic.

Bonnes pratiques de sécurité pour Amazon Inspector Classic

Amazon Inspector Classic propose un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Ces bonnes pratiques doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Pour consulter la liste des meilleures pratiques en matière de sécurité pour Amazon Inspector Classic, consultezthe section called "Bonnes pratiques de sécurité pour Amazon Inspector Classic".

Agents Amazon Inspector Classic

L'agent Amazon Inspector Classic est une entité qui collecte les informations relatives au package installé et à la configuration logicielle d'une instance Amazon EC2. Bien que cela ne soit pas obligatoire dans tous les cas, vous devez installer l'agent Amazon Inspector Classic sur chacune de vos instances Amazon EC2 cibles afin d'évaluer pleinement leur sécurité.

Pour plus d'informations sur l'installation, la désinstallation et la réinstallation de l'agent, et pour savoir comment vérifier si l'agent installé est en cours d'exécution et comment configurer la prise en charge du proxy pour l'agent, consultez Utilisation des agents Amazon Inspector Classic sur des systèmes d'exploitation basés sur Linux et Utilisation des agents Amazon Inspector Classic sur les systèmes d'exploitation Windows.

> **Note**
>
> Un agent Amazon Inspector Classic n'est pas nécessaire pour exécuter le package de règles d'accessibilité réseau.

> **Important**
>
> L'agent Amazon Inspector Classic s'appuie sur les métadonnées de l'instance Amazon EC2 pour fonctionner correctement. Il accède aux métadonnées d'instance à l'aide de la version 1 ou 2 du service de métadonnées d'instance (IMDSv1ou IMDSv2). Consultez Métadonnées d'instance et données utilisateur pour en savoir plus sur les métadonnées d'instance EC2 et les méthodes d'accès.

Rubriques

- Installation des agents Amazon Inspector Classic
- Utilisation des agents Amazon Inspector Classic sur des systèmes d'exploitation basés sur Linux
- Utilisation des agents Amazon Inspector Classic sur les systèmes d'exploitation Windows
- (Facultatif) Vérifiez la signature du script d'installation de l'agent Amazon Inspector Classic sur les systèmes d'exploitation Linux
- (Facultatif) Vérifiez la signature du script d'installation de l'agent Amazon Inspector Classic sur les systèmes d'exploitation Windows

Privilèges d'agent Amazon Inspector Classic

Vous devez disposer d'autorisations administratives ou root pour installer l'agent Amazon Inspector Classic. Sur les systèmes d'exploitation Linux pris en charge, l'agent se compose d'un exécutable en mode utilisateur qui s'exécute avec un accès racine. Sur les systèmes d'exploitation Windows pris en charge, l'agent se compose d'un service de mise à jour et d'un service d'agent, qui s'exécutent chacun en mode utilisateur avec les privilèges `LocalSystem`.

Sécurité du réseau et des agents Amazon Inspector Classic

L'agent Amazon Inspector Classic initie toutes les communications avec le service Amazon Inspector Classic. Cela signifie que l'agent doit avoir un chemin réseau sortant vers des points de terminaison publics afin de pouvoir envoyer des données télémétriques. Par exemple, l'agent peut se connecter à`arsenal.<region>.amazonaws.com`, ou le point de terminaison peut être un compartiment Amazon S3 situé à`s3.dualstack.<region>.amazonaws.com`. Assurez-vous de le remplacer `<region>` par la AWS région dans laquelle vous exécutez Amazon Inspector Classic. Pour plus d'informations, consultez Plages d'adresses IP AWS. Comme toutes les connexions provenant de l'agent sont établies en sortie, il n'est pas nécessaire d'ouvrir des ports dans vos groupes de sécurité pour autoriser les communications entrantes avec l'agent depuis Amazon Inspector Classic.

L'agent communique régulièrement avec Amazon Inspector Classic via un canal protégé par TLS, qui est authentifié en utilisant soit l' AWS identité associée au rôle de l'instance EC2, soit, si aucun rôle n'est attribué, avec le document de métadonnées de l'instance. Une fois authentifié, l'agent envoie des messages de pulsation au service et reçoit des instructions du service en réponse. Si une évaluation a été planifiée, l'agent reçoit les instructions la concernant. Ces instructions sont des fichiers JSON structurés, qui indiquent à l'agent d'activer ou désactiver des capteurs préconfigurés spécifiques dans l'agent. Chaque action d'instruction est prédéfinie au sein de l'agent. Les instructions arbitraires ne peuvent pas être exécutées.

Au cours d'une évaluation, l'agent collecte les données de télémétrie du système pour les renvoyer à Amazon Inspector Classic via un canal protégé par TLS. L'agent n'apporte aucune modification au système à partir duquel il collecte les données. Une fois que l'agent a collecté les données de télémétrie, il les renvoie à Amazon Inspector Classic pour traitement. Au-delà des données télémétriques qu'il génère, l'agent n'est pas capable de collecter ni de transmettre d'autres données sur le système ou les objectifs d'évaluation qu'il évalue. À l'heure actuelle, il n'existe aucune méthode exposée pour intercepter et étudier les données télémétriques au niveau de l'agent.

Mises à jour des agents Amazon Inspector Classic

Dès que les mises à jour de l'agent Amazon Inspector Classic sont disponibles, elles sont automatiquement téléchargées depuis Amazon S3 et appliquées. Cela permet également de mettre à jour toutes les dépendances nécessaires. La fonctionnalité de mise à jour automatique vous évite d'avoir à suivre et à gérer manuellement le contrôle des versions des agents que vous avez installés sur vos instances EC2. Toutes les mises à jour sont soumises à des processus de contrôle des modifications Amazon audités afin de garantir la conformité aux normes de sécurité applicables.

Afin de garantir la sécurité de l'agent, toutes les communications entre l'agent et le site de publication des mises à jour automatiques (S3) sont effectuées via une connexion TLS, et le serveur est authentifié. Tous les fichiers binaires impliqués dans le processus de mise à jour automatique sont signés numériquement et les signatures sont vérifiées par le programme de mise à jour avant l'installation. Le processus de mise à jour automatique est exécuté uniquement en dehors des périodes d'évaluation. Si des erreurs sont détectées, le processus de mise à jour peut effectuer une restauration et retenter la mise à jour. Enfin, le processus de mise à jour de l'agent sert uniquement à mettre à niveau les fonctionnalités de l'agent. Aucune de vos informations spécifiques n'est jamais envoyée par l'agent à Amazon Inspector Classic dans le cadre du flux de mise à jour. Les seules informations communiquées dans le cadre du processus de mise à jour sont les données télémétriques de réussite ou d'échec de l'installation de base et, le cas échéant, les informations de diagnostic de l'échec de la mise à jour.

Cycle de vie des données télémétriques

Les données de télémétrie générées par l'agent Amazon Inspector Classic lors des tests d'évaluation sont formatées dans des fichiers JSON. Les fichiers sont transmis near-real-time via TLS à Amazon Inspector Classic, où ils sont chiffrés à l'aide d'une clé éphémère per-assessment-run dérivée du KMS. Les fichiers sont stockés en toute sécurité dans un compartiment Amazon S3 dédié à Amazon Inspector Classic. Le moteur de règles d'Amazon Inspector Classic accède

aux données de télémétrie chiffrées du compartiment S3, les déchiffre en mémoire et traite les données conformément aux règles d'évaluation configurées pour générer des résultats. Les données télémétriques qui sont stockées dans S3 sont conservées uniquement pour permettre l'assistance en cas de demandes de support. Elles ne sont pas utilisées ni regroupées par Amazon à d'autres fins. Après 30 jours, les données de télémétrie sont définitivement supprimées conformément à une politique de cycle de vie des compartiments S3 standard pour les données Amazon Inspector Classic. À l'heure actuelle, Amazon Inspector Classic ne fournit pas d'API ni de mécanisme d'accès au compartiment S3 pour la télémétrie collectée.

Contrôle d'accès aux AWS comptes depuis Amazon Inspector Classic

En tant que service de sécurité, Amazon Inspector Classic accède à vos AWS comptes et à vos ressources uniquement lorsqu'il a besoin de trouver des instances EC2 à évaluer en demandant des balises. Pour ce faire, il utilise un accès IAM standard via le rôle créé lors de la configuration initiale du service Amazon Inspector Classic. Au cours d'une évaluation, toutes les communications avec votre environnement sont initiées par l'agent Amazon Inspector Classic installé localement sur les instances EC2. Les objets de service Amazon Inspector Classic créés, tels que les cibles d'évaluation, les modèles d'évaluation et les résultats générés par le service, sont stockés dans une base de données gérée par Amazon Inspector Classic et accessible uniquement à celui-ci.

Limites relatives aux agents Amazon Inspector Classic

Pour plus d'informations sur les limites des agents Amazon Inspector Classic, consultezLimites de service Amazon Inspector Classic.

Installation des agents Amazon Inspector Classic

Vous pouvez installer l'agent Amazon Inspector Classic à l'aide de la commande Systems Manager Run sur plusieurs instances (y compris les instances basées sur Linux et Windows). Vous pouvez également installer l'agent individuellement en vous connectant à chaque instance EC2. Les procédures dans ce chapitre fournissent des instructions pour les deux méthodes.

Vous pouvez également installer rapidement l'agent sur toutes les instances Amazon EC2 incluses dans une cible d'évaluation en cochant la case Installer les agents sur la page Définir une cible d'évaluation de la console.

Rubriques

> **Note**
>
> Les procédures décrites dans ce chapitre s'appliquent à toutes les AWS régions prises en charge par Amazon Inspector Classic.

Installer l'agent sur plusieurs instances EC2 à l'aide de Systems Manager Run Command

Vous pouvez installer l'agent Amazon Inspector Classic sur vos instances EC2 à l'aide de la commande Systems Manager Run. Cela vous permet d'installer l'agent à distance et sur plusieurs instances (Linux et Windows avec la même commande) en une seule fois.

> **Important**
>
> L'installation de l'agent à l'aide de la fonctionnalité Systems Manager Run Command n'est actuellement pas prise en charge pour le système d'exploitation Debian.

> **Important**
>
> Pour utiliser cette option, assurez-vous que l'agent SSM est installé sur votre instance EC2 et que le rôle IAM permet d'exécuter une commande. L'agent SSM est installé par défaut sur les instances Amazon EC2 Windows et sur les instances Amazon Linux. Amazon EC2 Systems Manager nécessite un rôle IAM pour les instances EC2 qui traitent les commandes et un rôle distinct pour les utilisateurs exécutant des commandes. Pour plus d'informations, consultez les sections Installation et configuration de l'agent SSM et Configuration des rôles de sécurité pour SSM.

Pour installer l'agent sur plusieurs instances EC2 à l'aide de la fonctionnalité Exécuter la commande de Systems Manager

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, sous Instances & nodes (Instances et nœuds), choisissez Run Command (Exécuter la commande).
3. Choisissez Run a Command.
4. Pour le document de commande, choisissez le document nommé AmazonInspector-ManageAWSAgent qui appartient à Amazon. Ce document contient le script d'installation de l'agent Amazon Inspector Classic sur les instances EC2.
5. Pour les cibles, vous pouvez sélectionner des instances EC2 à l'aide de différentes méthodes. Pour installer l'agent sur toutes les instances dans l'objectif d'évaluation, vous pouvez spécifier les mêmes balises que celles utilisées pour créer l'objectif d'évaluation.
6. Indiquez vos choix pour le reste des options disponibles en utilisant les instructions fournies dans Exécution des commandes depuis la console, puis sélectionnez Run (Exécuter).

> **Note**
>
> Vous pouvez également installer l'agent sur plusieurs instances EC2 (basées sur Linux et Windows) lorsque vous créez une cible d'évaluation, ou vous pouvez utiliser le bouton Installer les agents avec la commande Exécuter pour une cible existante. Pour plus d'informations, consultez Création d'un objectif d'évaluation.

Installer l'agent sur une instance EC2 Linux

Procédez comme suit pour installer l'agent Amazon Inspector Classic sur une instance EC2 basée sur Linux.

Pour installer l'agent sur une instance EC2 Linux

1. Connectez-vous à votre instance EC2 exécutant un système d'exploitation basé sur Linux sur lequel vous souhaitez installer l'agent Amazon Inspector Classic.

> **Note**
>
> Pour plus d'informations sur les systèmes d'exploitation pris en charge par Amazon Inspector Classic, consultezSystèmes d'exploitation et régions pris en charge par Amazon Inspector Classic.

2. Téléchargez le script d'installation de l'agent en exécutant l'une des commandes suivantes :

   - wget https://inspector-agent.amazonaws.com/linux/latest/install
   - curl -O https://inspector-agent.amazonaws.com/linux/latest/install

3. (Facultatif) Vérifiez que le script d'installation de l'agent n'a pas été modifié ou endommagé. Pour plus d'informations, consultez (Facultatif) Vérifiez la signature du script d'installation de l'agent Amazon Inspector Classic sur les systèmes d'exploitation Linux.

4. Pour installer l'agent, exécutez sudo bash install.

> **Note**
>
> Si vous installez l'agent dans un environnement SELinux, Amazon Inspector Classic peut être détecté comme un daemon déconfiné. Vous pouvez éviter cela en modifiant le domaine du processus d'agent de la valeur par défaut `initrc_t` à`bin_t`. Utilisez les commandes suivantes pour attribuer le `bin_t` contexte aux scripts d'exécution Amazon Inspector Classic avant d'installer l'agent pour SELinux :
> sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
> sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent

> **Note**
>
> Lorsque les mises à jour de l'agent deviennent disponibles, elles sont automatiquement téléchargées depuis Amazon S3 et appliquées. Pour plus d'informations, consultez Mises à jour des agents Amazon Inspector Classic.
> Si vous souhaitez ignorer ce processus de mise à jour automatique, exécutez la commande suivante lorsque vous installez l'agent :
> sudo bash install -u false

> **Note**
>
> (Facultatif) Pour supprimer le script d'installation de l'agent, exécutez la commande rm install.

5. Vérifiez que les fichiers suivants, requis pour assurer l'installation et le fonctionnement corrects de l'agent, sont bien installés :

   - `libcurl4` (requis pour installer l'agent sur Ubuntu 18.04)
   - `libcurl3`
   - `libgcc1`
   - `libc6`
   - `libstdc++6`
   - `libssl1.0.1`
   - `libssl1.0.2` (requis pour installer l'agent sur Debian 9)
   - `libssl1.1`(nécessaire pour installer l'agent sur Ubuntu 20.04 LTS)
   - `libpcap0.8`

Installer l'agent sur une instance EC2 Windows

Procédez comme suit pour installer l'agent Amazon Inspector Classic sur une instance EC2 basée sur Windows.

Pour installer l'agent sur une instance EC2 Windows

1. Connectez-vous à votre instance EC2 exécutant un système d'exploitation Windows, sur laquelle vous souhaitez installer l'agent .

> **Note**
>
> Pour plus d'informations sur les systèmes d'exploitation pris en charge par Amazon Inspector Classic, consultezSystèmes d'exploitation et régions pris en charge par Amazon Inspector Classic.

2. Téléchargez le fichier .exe suivant :

```
https://inspector-agent.amazonaws.com/windows/installer/latest/
AWSAgentInstall.exe
```

3. Ouvrez une fenêtre d'invite de commande (avec autorisations administratives), naviguez jusqu'à l'emplacement où vous avez enregistré le fichier `AWSAgentInstall.exe` et exécutez le fichier .exe pour installer l'agent.

> **Note**
>
> Lorsque les mises à jour de l'agent deviennent disponibles, elles sont automatiquement téléchargées depuis Amazon S3 et appliquées. Pour plus d'informations, consultez Mises à jour des agents Amazon Inspector Classic.
> Si vous souhaitez ignorer ce processus de mise à jour automatique, exécutez la commande suivante lorsque vous installez l'agent :
> AWSAgentInstall.exe AUTOUPDATE=No

Utilisation des agents Amazon Inspector Classic sur des systèmes d'exploitation basés sur Linux

Vous pouvez installer, supprimer, vérifier et modifier le comportement des agents Amazon Inspector Classic. Connectez-vous à votre instance Amazon EC2 exécutant un système d'exploitation basé sur Linux et exécutez l'une des procédures suivantes. Pour plus d'informations sur les systèmes d'exploitation pris en charge par Amazon Inspector Classic, consultezSystèmes d'exploitation et régions pris en charge par Amazon Inspector Classic.

> **Important**
>
> L'agent Amazon Inspector Classic s'appuie sur les métadonnées de l'instance Amazon EC2 pour fonctionner correctement. Il accède aux métadonnées d'instance à l'aide de la version 1 ou 2 du service de métadonnées d'instance (IMDSv1ou IMDSv2). Consultez Métadonnées d'instance et données utilisateur pour en savoir plus sur les métadonnées d'instance EC2 et les méthodes d'accès.

> **Note**
>
> Les commandes de cette section fonctionnent dans toutes les AWS régions prises en charge par Amazon Inspector Classic.

Rubriques

Vérifier que l'agent Amazon Inspector Classic est en cours d'exécution

- Pour vérifier que l'agent est installé et en cours d'exécution, connectez-vous à votre instance EC2 et exécutez la commande suivante :

  sudo /opt/aws/awsagent/bin/awsagent status

  Cette commande renvoie le statut de l'agent en cours d'exécution ou une erreur indiquant que l'agent ne peut pas être contacté.

Arrêt de l'agent Amazon Inspector Classic

- Pour arrêter l'agent, exécutez la commande suivante :

  sudo /etc/init.d/awsagent stop

Démarrage de l'agent Amazon Inspector Classic

- Pour lancer l'agent, exécutez la commande suivante :

  sudo /etc/init.d/awsagent start

Modification des paramètres des agents Amazon Inspector Classic

Une fois l'agent Amazon Inspector Classic installé et exécuté sur votre instance EC2, vous pouvez modifier les paramètres du `agent.cfg` fichier pour modifier le comportement de l'agent. Sur les systèmes d'exploitation Linux, le fichier `agent.cfg` est situé dans le répertoire `/opt/aws/awsagent/etc`. Après avoir modifié et enregistré le fichier `agent.cfg`, vous devez arrêter et redémarrer l'agent pour que les modifications prennent effet.

> **Important**
>
> Nous vous recommandons vivement de ne modifier le fichier `agent.cfg` qu'en suivant les instructions d'AWS Support.

Configuration de la prise en charge du proxy pour un agent Amazon Inspector Classic

Pour obtenir un support de proxy pour un agent sur un système d'exploitation Linux, utilisez un fichier spécifique à l'agent avec des variables d'environnement spécifiques. Pour plus d'informations, consultez https://wiki.archlinux.org/index.php/proxy_settings.

Exécutez l'une des procédures suivantes :

Pour installer un agent sur une instance EC2 qui utilise un serveur proxy

1. Créez un fichier nommé `awsagent.env` et enregistrez-le dans le répertoire `/etc/init.d/`.
2. Modifiez `awsagent.env` pour inclure les variables d'environnement suivantes au format suivant :

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

> **Note**
>
> Remplacez les valeurs dans les exemples précédents uniquement par des combinaisons de nom d'hôte et de numéro de port valides. Spécifiez l'adresse IP du point de terminaison des métadonnées d'instance (169.254.169.254) pour la variable `no_proxy`.

3. Installez l'agent Amazon Inspector Classic en suivant les étapes de la Installer l'agent sur une instance EC2 Linux procédure.

Pour configurer la prise en charge du proxy sur une instance EC2 avec un agent en cours d'exécution

1. Pour configurer la prise en charge du proxy, la version de l'agent qui s'exécute sur votre instance EC2 doit être 1.0.800.1 ou ultérieure. Si vous avez activé le processus de mise à jour pour l'agent, vous pouvez vérifier que votre version d'agent est de 1.0.800.1 ou ultérieure en utilisant la procédure Vérifier que l'agent Amazon Inspector Classic est en cours d'exécution. Si vous n'avez pas activé le processus de mise à jour automatique pour l'agent, vous devez réinstaller l'agent sur cette instance EC2 en suivant la Installer l'agent sur une instance EC2 Linux procédure.
2. Créez un fichier nommé `awsagent.env` et enregistrez-le dans le répertoire `/etc/init.d/`.
3. Modifiez `awsagent.env` pour inclure les variables d'environnement suivantes au format suivant :

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

> **Note**
>
> Remplacez les valeurs dans les exemples précédents uniquement par des combinaisons de nom d'hôte et de numéro de port valides. Spécifiez l'adresse IP du point de terminaison des métadonnées d'instance (169.254.169.254) pour la variable `no_proxy`.

4. Redémarrez l'agent après l'avoir arrêté à l'aide de la commande suivante :

```
sudo /etc/init.d/awsagent restart
```

Les paramètres de proxy sont collectés et utilisés par l'agent et par le processus de mise à jour automatique.

Désinstallation de l'agent Amazon Inspector Classic

Pour désinstaller l'agent

1. Connectez-vous à votre instance EC2 exécutant un système d'exploitation Linux sur lequel vous souhaitez désinstaller l'agent.

   > **Note**
   >
   > Pour plus d'informations sur les systèmes d'exploitation pris en charge par Amazon Inspector Classic, consultezSystèmes d'exploitation et régions pris en charge par Amazon Inspector Classic.

2. Pour désinstaller l'agent, utilisez l'une des commandes suivantes :

   - Exécutez la commande suivante sur Amazon Linux, CentOS et Red Hat :

     ```
     sudo yum remove 'AwsAgent*'
     ```

   - Exécutez la commande suivante sur un serveur Ubuntu :

     ```
     sudo apt-get purge 'awsagent*'
     ```

Utilisation des agents Amazon Inspector Classic sur les systèmes d'exploitation Windows

Vous pouvez démarrer, arrêter et modifier le comportement des agents Amazon Inspector Classic. Connectez-vous à votre instance EC2 exécutant un système d'exploitation Windows et effectuez l'une des procédures décrites dans ce chapitre. Pour de plus amples informations sur les systèmes d'exploitation pris en charge par Amazon Inspector Inspector Inspector tor Inspector tor Inspector tor tor Inspector tor Inspector torSystèmes d'exploitation et régions pris en charge par Amazon Inspector Classic

> **Important**
>
> L'agent Amazon Inspector Il accède aux métadonnées d'instance à l'aide de la version 1 ou 2 du service de métadonnées d'instance (IMDSv1ou IMDSv2). Consultez Métadonnées d'instance et données utilisateur pour en savoir plus sur les métadonnées d'instance EC2 et les méthodes d'accès.

> **Note**
>
> Les commandes de ce chapitre fonctionnent dans toutes lesAWS régions prises en charge par Amazon Inspector Classic.

Rubriques

Démarrage ou arrêt d'un agent Amazon Inspector Classic ou vérification du bon fonctionnement de l'agent

Pour activer, arrêter ou vérifier un agent

1. Sur votre instance EC2, choisissez Démarrer, Exécuter, puis entrez**`services.msc`**.
2. Si l'agent est en cours d'exécution réussie, deux services sont répertoriés avec le statut Démarré ou En cours d'exécution dans la fenêtre Services : AWS Agent Service (Service d'agent AWS) et AWS Agent Updater Service (Service de mise à jour d'agent AWS).
3. Pour démarrer l'agent, cliquez avec le bouton droit sur AWS Agent Service (Service d'agent AWS), puis sélectionnez Démarrer. Si le service est démarré avec succès, son état est mis à jour à Démarré ou En cours d'exécution.
4. Pour arrêter l'agent, cliquez avec le bouton droit sur AWS Agent Service (Service d'agent AWS) et sélectionnez ensuite Arrêter. Si le service est arrêté avec succès, son état est effacé (il est

vide). Nous vous déconseillons d'arrêter le service AWS Agent Updater Service (Service de mise à jour d'agent AWS), car cela désactiverait l'installation de tous les correctifs et améliorations futurs de l'agent.

5. Pour vérifier que l'agent est installé et en cours d'exécution, connectez-vous à votre instance EC2 et ouvrez une invite de commande à l'aide des autorisations administratives. Accédez à `C:\Program Files\Amazon Web Services\AWS Agent`, puis exécutez la commande suivante :

   AWSAgentStatus.exe

   Cette commande renvoie le statut de l'agent en cours d'exécution ou une erreur indiquant que l'agent ne peut pas être contacté.

Modifier les paramètres d'agent Inspector Inspector Inspector Inspector

Une fois l'agent Amazon Inspector Classic installé et exécuté sur votre instance EC2, vous pouvez modifier les paramètres du`agent.cfg` fichier pour modifier le comportement de l'agent. Sur les systèmes d'exploitation Windows, le fichier est situé dans le répertoire `C:\ProgramData\Amazon Web Services\AWS Agent`. Après avoir modifié et enregistré le fichier `agent.cfg`, vous devez arrêter et redémarrer l'agent pour que les modifications prennent effet.

> **Important**
>
> Nous vous recommandons vivement de ne modifier le fichier `agent.cfg` qu'en suivant les instructions d'AWS Support.

Configuration de la prise en charge par proxy pour un agent Amazon Inspector Classic

Pour obtenir la prise en charge du proxy pour un agent sur un système d'exploitation Windows, utilisez le proxy `WinHTTP`. Pour configurer le proxy `WinHTTP` à l'aide de l'utilitaire `netsh`, veuillez consulter Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP).

> **Important**
>
> Seuls les proxys HTTPS sont pris en charge pour les instances Windows.

Exécutez l'une des procédures suivantes :

Pour installer un agent agent sur une instance EC2 qui utilise un serveur proxy

1. Téléchargez le fichier .exe suivant : `https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`
2. Ouvrez une fenêtre ou PowerShell une fenêtre d'invite de commande (à l'aide des autorisations administratives). Accédez à l'emplacement dans lequel vous avez enregistré le `AWSAgentInstall.exe` téléchargé et exécutez la commande suivante :

   ```
   .\AWSAgentInstall.exe /install USEPROXY=1
   ```

Pour configurer la prise en charge des proxy sur une instance EC2 avec un agent en cours d'exécution

1. Pour configurer la prise en charge des proxy, la version de l'agent Amazon Inspector Classic qui s'exécute sur votre instance EC2 doit être 1.0.0.59 ou ultérieure. Si vous avez activé le processus de mise à jour pour l'agent, vous pouvez vérifier que votre version d'agent est de 1.0.0.59 ou ultérieure en utilisant la procédure Démarrage ou arrêt d'un agent Amazon Inspector Classic ou vérification du bon fonctionnement de l'agent. Si vous n'avez pas activé le processus de mise à jour automatique pour l'agent, vous devez réinstaller l'agent sur cette instance EC2 en suivant laInstaller l'agent sur une instance EC2 Windows procédure.
2. Ouvrez l'éditeur de registre (`regedit.exe`).
3. Accédez à la clé de registre suivante : `"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`.
4. À l'intérieur de cette clé de registre, créez une valeur de registre `DWORD(32bit)` nommée `"UseProxy"`.
5. Double-cliquez sur cette valeur et affectez-lui la valeur 1.
6. Saisissez **`services.msc`**, recherchez AWS Agent Service (Service d'agent AWS), puis le AWS Agent Updater Service (Service de mise à jour d'agent AWS) dans la fenêtre Services et redémarrez chaque processus. Une fois les deux processus redémarrés, exécutez le fichier `AWSAgentStatus.exe` (voir étape 5 dans Démarrage ou arrêt d'un agent Amazon Inspector Classic ou vérification du bon fonctionnement de l'agent). Afficher l'état de votre agent et vérifier qu'il utilise le proxy configuré.

Désinstallation de l'agent Amazon Inspector

Pour désinstaller l'agent

1. Connectez-vous à votre instance EC2 exécutant un système d'exploitation Windows sur lequel vous souhaitez désinstaller l'agent Amazon Inspector Classic.

   > **Note**
   >
   > Pour de plus amples informations sur les systèmes d'exploitation pris en charge par Amazon Inspector Inspector Inspector tor Inspector tor Inspector tor tor Inspector tor Inspector torSystèmes d'exploitation et régions pris en charge par Amazon Inspector Classic

2. Sur votre instance EC2, accédez à Panneau de configuration, Ajout/Suppression de programmes.
3. Dans la liste des programmes installés, sélectionnez Agent AWS, puis Désinstaller.

(Facultatif) Vérifiez la signature du script d'installation de l'agent Amazon Inspector Classic sur les systèmes d'exploitation Linux

Cette rubrique décrit le processus recommandée pour vérifier la validité du script d'installation de l'agent Amazon Inspector Classic pour les systèmes d'exploitation Linux.

Lorsque vous téléchargez une application à partir d'internet, nous vous recommandons d'authentifier l'identité de l'éditeur du logiciel et de vérifier que l'application n'a pas été modifiée ou corrompue depuis sa publication. Cela vous évitera d'installer une version de l'application contenant un virus ou tout autre code malveillant.

Si, après l'exécution de la procédure décrite dans cette rubrique, vous déterminez que le logiciel de l'agent Amazon Inspector Classic a été modifié ou corrompu, n'exécutez PAS le fichier d'installation. Contactez plutôt AWS Support.

Les fichiers d'agent Amazon Inspector Classic pour les systèmes d'exploitation Linux sont signés à l'aideGnuPG d'une mise en œuvre Open Source de la norme Pretty Good Privacy (OpenPGP) pour les signatures numériques sécurisées. GnuPG(également connu sous le nom deGPG) permet l'authentification et la vérification de l'intégrité par le biais d'une signature numérique. Amazon EC2

publie une clé publique et des signatures que vous pouvez utiliser pour vérifier les outils CLI Amazon EC2 téléchargés. Pour plus d'informations sur PGP et GnuPG (GPG), consultez http://www.gnupg.org.

La première étape consiste à établir une approbation avec l'éditeur du logiciel. Téléchargez la clé publique de l'éditeur du logiciel, vérifiez que le propriétaire de cette clé publique est bien celui qu'il prétend être, puis ajoutez la clé publique à votre porte-clés. Votre porte-clés est un ensemble de clés publiques connues. Après avoir établi l'authenticité de la clé publique, vous pouvez l'utiliser pour vérifier la signature de l'application.

Rubriques

Installation des outils GPG

Si votre système d'exploitation est Linux ou Unix, les outils GPG sont probablement déjà installés. Pour tester si les outils sont installés sur votre système, tapez gpg à partir d'une invite de commande. Si les outils GPG sont installés, une invite de commande GPG s'affiche. Si les outils GPG ne sont pas installés, vous voyez une erreur indiquant que la commande est introuvable. Vous pouvez installer le package GnuPG à partir d'un référentiel.

Pour installer les outils GPG sur un système Linux basé sur Debian

- Depuis un terminal, exécutez la commande suivante : apt-get install gnupg.

Pour installer les outils GPG sur un système Linux basé sur Red Hat

- Depuis un terminal, exécutez la commande suivante : yum install gnupg.

Authentification et importation de la clé publique

L'étape suivante consiste à authentifier la clé publique d'Amazon Inspector Classic et à l'ajouter en tant que clé de confiance à votreGPG porte-clés.

Pour authentifier et importer la clé publique Amazon Inspector Classic

1. Obtenez une copie de notre clé publique GPG en effectuant l'une des actions suivantes :

- Téléchargez-la à partir du site https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg.
- Copiez la clé à partir du texte suivant et collez-la dans un fichier nommé `inspector.gpg`. Veillez à inclure tout ce qui suit :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. À l'invite de commande, dans le répertoire où vous avez enregistré inspector.gpg, exécutez la commande suivante pour importer la clé publique d'Amazon Inspector Classic dans votre porte-clés :

```
gpg --import inspector.gpg
```

La commande renvoie des résultats semblables à ce qui suit :

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                   gpg: Total number processed: 1
                   gpg:               imported: 1  (RSA: 1)
```

Notez la valeur de la clé ; vous en aurez besoin lors de l'étape suivante. Dans l'exemple précédent, la valeur de la clé est `58360418`.

3. Vérifiez l'empreinte en exécutant la commande suivante, en remplaçant key-value (valeur clé) par la valeur de l'étape précédente :

```
gpg --fingerprint key-value
```

Cette commande renvoie un résultat semblable à ce qui suit :

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836
 0418
                uid                  Amazon Inspector <inspector@amazon.com>
```

De plus, la chaîne de l'empreinte doit être identique à `DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418`, comme illustré dans l'exemple précédent. Comparez l'empreinte de la clé renvoyée à celle publiée sur cette page. Elles doivent correspondre. Si elles ne correspondent pas, n'installez pas le script d'installation de l'agent Amazon Inspector Classic et contactez Support AWS.

Vérification de la signature du package

Après avoir installé les`GPG` outils, authentifié et importé la clé publique d'Amazon Inspector Classic et vérifié que la clé publique d'est approuvée, vous êtes prêt à vérifier la signature du script d'installation d'.

Pour vérifier la signature du script d'installation

1. À l'invite de commande, exécutez la commande suivante pour télécharger le fichier signature du script d'installation :

```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
```

2. Vérifiez la signature en exécutant la commande suivante à l'invite de commande dans le répertoire où vous avez enregistré`install.sig` et le fichier d'installation d'Amazon Inspector Classic. Ces deux fichiers doivent être présents.

   ```
   gpg --verify ./install.sig
   ```

   Le résultat doit ressembler à ce qui suit :

   ```
   gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
   gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
   ```

   Si le résultat contient l'expression`Good signature from "Amazon Inspector <inspector@amazon.com>"`, cela signifie que la signature a été vérifiée et vous pouvez continuer à exécuter le script d'installation d'Amazon Inspector Classic.

   Si le résultat inclut l'expression `BAD signature`, vérifiez si vous avez effectué la procédure correctement. Si vous continuez à obtenir cette réponse, n'exécutez pas le fichier d'installation que vous avez précédemment téléchargé, et contactez AWS Support.

Voici les informations détaillées sur les avertissements que vous pouvez voir :

- AVERTISSEMENT : Cette clé n'est pas certifiée par une signature fiable ! Rien n'indique que la signature appartient au propriétaire. Ce message fait référence à votre niveau de confiance personnel dans la conviction que vous possédez une clé publique authentique pour Amazon Inspector Classic. Dans un monde idéal, vous visiteriez un bureau AWS et vous recevriez la clé en personne. Cependant, vous la téléchargez le plus souvent à partir d'un site Web. Dans le cas présent, le site Web est un site AWS.
- gpg: no ultimately trusted keys found. Cela signifie que la clé spécifique n'est pas « approuvée en dernier lieu » par vous-même (ou par d'autres personnes de confiance).

Pour plus d'informations, consultez http://www.gnupg.org.

(Facultatif) Vérifiez la signature du script d'installation de l'agent Amazon Inspector Classic sur les systèmes d'exploitation Windows

Cette rubrique décrit celle recommandée pour vérifier la validité du script d'installation de l'agent Amazon Inspector Classic pour les systèmes d'exploitation Windows.

Lorsque vous téléchargez une application à partir d'internet, nous vous recommandons d'authentifier l'identité de l'éditeur du logiciel et de vérifier que l'application n'a pas été modifiée ou corrompue depuis sa publication. Cela vous évitera d'installer une version de l'application contenant un virus ou tout autre code malveillant.

Si, après l'exécution de la procédure décrite dans cette rubrique, vous déterminez que le logiciel de l'agent Amazon Inspector Classic a été modifié ou corrompu, n'exécutez PAS le fichier d'installation. Contactez plutôt AWS Support.

Pour vérifier la validité du script d'installation de l'agent téléchargé sur les systèmes d'exploitation Windows, vous devez vous assurer que l'empreinte de son certificat de signataire Amazon Services LLC est égale à cette valeur :

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

Pour vérifier cette valeur, exécutez la procédure suivante :

1. Cliquez avec le bouton droit sur le fichier `AWSAgentInstall.exe` téléchargé et ouvrez la fenêtre Properties (Propriétés).
2. Choisissez l'onglet Signatures numériques.
3. Dans la liste des signatures, choisissez Amazon Web Services, Inc., puis Détails.
4. Choisissez l'onglet General (Général), s'il n'est pas déjà sélectionné, puis View Certificate (Afficher le certificat).
5. Sélectionnez l'onglet Détails, puis sélectionnez All (Tous) dans la liste déroulante Show (Afficher), si cette option n'est pas déjà sélectionnée.
6. Faites défiler l'écran vers le bas jusqu'au champ Thumbprint (Empreinte), puis choisissez Thumbprint (Empreinte). Cela affichera la valeur complète de l'empreinte dans la fenêtre inférieure.

    - Si la valeur de l'empreinte affichée dans la fenêtre inférieure est identique à la valeur suivante :

      E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

le script d'installation de l'agent que vous avez téléchargé est authentique et peut être installé en toute sécurité.

- Si la valeur de l'empreinte affichée dans la fenêtre de détails inférieure n'est pas identique à la valeur ci-dessus, n'exécutez pas `AWSAgentInstall.exe`.

Cibles d'évaluation Amazon Inspector Classic

Vous pouvez utiliser Amazon Inspector Classic pour évaluer si votreAWScibles d'évaluation (vos collections deAWS) ont des problèmes de sécurité potentiels que vous devez résoudre.

> **Important**
>
> À l'heure actuelle, vos objectifs d'évaluation ne peuvent contenir que des instances EC2 qui s'exécutent sur certains systèmes d'exploitation pris en charge. Pour de plus amples informations sur les systèmes d'exploitation et les régions AWS pris en charge, veuillez consulter the section called “Systèmes d'exploitation et régions pris en charge”.

> **Note**
>
> Pour plus d'informations sur le lancement des instances EC2, consultez leDocumentation Amazon Elastic Compute Cloud.

Rubriques

Balisage des ressources pour créer un objectif d'évaluation

Afin de créer un objectif d'évaluation à faire évaluer par Amazon Inspector Classic, vous devez commencer par baliser les instances EC2 que vous souhaitez inclure dans votre objectif. Les balises sont des mots ou des expressions qui jouent le rôle de métadonnées pour identifier et organiser vos instances et autres.AWSAWS. Amazon Inspector Classic utilise les balises que vous créez pour identifier les instances qui appartiennent à votre objectif.

Chaque balise AWS est composée d'une paire clé-valeur de votre choix. Par exemple, vous pouvez choisir de nommer votre clé « Nom » et votre valeur « MyFirstInstance ». Après avoir balisé vos

instances, vous devez utiliser la console Amazon Inspector Classic pour ajouter ces instances à votre objectif d'évaluation. Il n'est pas nécessaire que les instances correspondent à plus d'une paire clé-valeur de balise.

Lorsque vous balisez vos instances EC2 pour créer des objectifs d'évaluation, vous pouvez créer vos propres clés de balise personnalisées ou utiliser des clés de balises créées par d'autres utilisateurs de la même.AWS. Vous pouvez également utiliser les clés de balise automatiquement créées par AWS. Par exemple,AWScrée automatiquement unNomclé de balise pour les instances EC2 que vous lancez.

Vous pouvez ajouter des balises aux instances EC2 lorsque vous les créez, ou vous pouvez ajouter, modifier ou supprimer ces balises une par une sur la page de la console de chaque instance EC2. Vous pouvez également ajouter des balises à plusieurs instances EC2 simultanément à l'aide de Tag Editor.

Pour plus d'informations, consultez Tag Editor. Pour plus d'informations sur le balisage des instances EC2, consultez Ressources et balises.

Limites d'objectif d'évaluation Amazon Inspector Classic

Vous pouvez créer jusqu'à 50 objectifs d'évaluation par compte AWS. Pour plus d'informations, consultez Limites de service Amazon Inspector Classic.

Création d'un objectif d'évaluation

Vous pouvez utiliser la console Amazon Inspector Classic pour créer des objectifs d'évaluation.

Pour créer un objectif d'évaluation

1. Connectez-vous à la consoleAWS Management Consoleet ouvrez la console Amazon Inspector Classic à l'adressehttps://console.aws.amazon.com/inspector/.
2. Dans le volet de navigation, choisissez Objectifs d'évaluation, puis Create.
3. Dans Nom, saisissez un nom pour votre objectif d'évaluation.
4. Effectuez l'une des actions suivantes :

   - Afin d'inclure toutes les instances EC2 dans cetAWSdans cet objectif d'évaluation, sélectionnez l'Toutes les instances.

> **Note**
>
> La limite du nombre maximal d'agents pouvant être inclus dans l'exécution d'une évaluation s'applique lorsque vous utilisez cette option. Pour plus d'informations, consultez Limites de service Amazon Inspector Classic.

- Afin de choisir les instances EC2 que vous souhaitez inclure dans cet objectif d'évaluation, pourUtiliser les balises, saisissez les noms clés de la balises et les paires clé-valeur.

5. (Facultatif) Lorsque vous créez une cible, vous pouvez sélectionner l'Installation des agentspour installer l'agent sur toutes les instances EC2 de cette cible. Pour utiliser cette option, l'agent SSM doit être installé sur vos instances EC2 et celles-ci doivent disposer d'un rôle IAM qui autorise la fonctionnalité Exécuter la commande. L'agent SSM est installé par défaut sur les instances Amazon EC2 Windows et sur les instances Amazon Linux. Amazon EC2 Systems Manager a besoin d'un rôle IAM pour les instances EC2 qui traiteront les commandes et d'un rôle distinct pour les utilisateurs qui exécutent les commandes. Pour plus d'informations, consultez Installation et configuration de l'agent SSM et Configuration de rôles de sécurité pour System Manager.

> **Important**
>
> Si un agent s'exécute déjà sur une instance EC2, cette option remplace l'agent en cours d'exécution sur l'instance par la dernière version de l'agent.

> **Note**
>
> Pour vos objectifs d'évaluation existants, vous pouvez choisir le Bouton Installer les agents avec Exécuter la commandepour installer l'agent sur toutes les instances EC2 de cette cible.

> **Note**
>
> Vous pouvez également installer l'agent sur plusieurs instances EC2 (sur des instances Linux et Windows avec la même commande) à distance à l'aide de la fonctionnalité Exécuter la commande de Systems Manager. Pour plus d'informations, consultez

Installation d'Amazon Inspector Agent sur plusieurs instances EC2 à l'aide de la fonctionnalité Exécuter la commande de Systems Manager.

6. Choisissez Save (Enregistrer).

> **Note**
>
> Vous pouvez utiliser le pluginAperçu de la ciblesur la consoleObjectifs d'évaluationpour passer en revue toutes les instances EC2 incluses dans l'objectif d'évaluation. Pour chaque instance EC2, vous pouvez consulter le nom d'hôte, l'ID d'instance, l'adresse IP et, le cas échéant, l'état de l'agent. Le statut de l'agent peut comporter les valeurs suivantes : EN BONNE SANTÉ,MAUVAIS POUR LA SANTÉ, etINCONNU. Amazon Inspector Classic affiche unINCONNUlorsqu'il n'est pas en mesure de déterminer si un agent s'exécute sur l'instance EC2.

Suppression d'un objectif d'évaluation

Utilisez la procédure suivante pour supprimer un objectif d'évaluation.

Pour supprimer un objectif d'évaluation

- Sur la page Assessment targets (Objectifs d'évaluation), choisissez l'objectif à supprimer, puis choisissez Delete (Supprimer). Lorsque vous êtes invité à confirmer l'opération, choisissez Oui.

  > **Important**
  >
  > Lorsque vous supprimez un objectif d'évaluation, tous les modèles d'évaluation, toutes les exécutions d'évaluation, tous les résultats et toutes les versions des rapports associés à l'objectif sont également supprimés.

Vous pouvez également supprimer un objectif d'évaluation à l'aide de l'API `DeleteAssessmentTarget`.

Règles, packages et règles Amazon Inspector Classic

Vous pouvez utiliser Amazon Inspector Classic pour évaluer vos objectifs d'évaluation (collections de ressources AWS) afin de détecter d'éventuels problèmes de sécurité et vulnérabilités. Amazon Inspector Classic compare le comportement et la configuration de sécurité des cibles d'évaluation aux packages de règles de sécurité sélectionnés. Dans le contexte d'Amazon Inspector Classic, une règle est un contrôle de sécurité effectué par Amazon Inspector Classic pendant le cycle d'évaluation.

Dans Amazon Inspector Classic, les règles sont regroupées dans des packages de règles distincts par catégorie, sévérité ou prix. Cela vous permet de choisir les types d'analyse que vous pouvez effectuer. Par exemple, Amazon Inspector Classic propose un grand nombre de règles que vous pouvez utiliser pour évaluer vos applications. Mais vous souhaiterez peut-être inclure un plus petit sous-ensemble de règles disponibles afin de cibler des sujets de préoccupation particuliers ou de découvrir des problèmes de sécurité spécifiques. Les entreprises dotées de grands services informatiques souhaiteront peut-être déterminer si leurs applications sont exposées à une menace de sécurité. D'autres pourront vouloir se concentrer uniquement sur les problèmes ayant un niveau de gravité élevé.

Niveaux de gravité des règles dans Amazon Inspector Classic

Un niveau de gravité est attribué à chaque règle Amazon Inspector Classic. Cela réduit le besoin de prioriser une règle par rapport à une autre dans votre analyse. Cela peut également vous aider à déterminer votre réponse lorsqu'une règle met en évidence un problème potentiel.

Les niveaux High (élevé), Medium (moyen) et Low (faible) indiquent tous un problème de sécurité pouvant mettre en péril la confidentialité, l'intégrité et la disponibilité des informations incluses dans votre objectif d'évaluation. Les niveaux se distinguent en fonction de la probabilité que le problème aboutisse à un compromis et de l'urgence de le résoudre.

Le niveau Informational (information) met simplement en évidence un détail de la configuration de la sécurité de votre objectif d'évaluation.

Voici les méthodes recommandées pour résoudre les problèmes en fonction de leur gravité :

- Élevé — Les problèmes très graves sont extrêmement urgents. Amazon Inspector Classic vous recommande de traiter ce problème de sécurité comme une urgence et de mettre en œuvre une solution immédiate.
- Moyennement grave — Les problèmes de gravité moyenne sont assez urgents. Amazon Inspector Classic vous recommande de résoudre ce problème dès que possible, par exemple lors de votre prochaine mise à jour de service.
- Faible — Les problèmes de faible gravité sont moins urgents. Amazon Inspector Classic vous recommande de résoudre ce problème dans le cadre de l'une de vos futures mises à jour de service.
- Informatif — Ces questions sont purement informatives. En fonction de vos objectifs professionnels et de ceux de votre organisation, vous pouvez soit simplement prendre note de cette information, soit l'utiliser pour améliorer la sécurité de votre objectif d'évaluation.

Packages de règles dans Amazon Inspector Classic

Une évaluation Amazon Inspector peut utiliser n'importe quelle combinaison d'ensembles de règles suivants :

Évaluations de réseaux :

- Joignabilité de réseau

Évaluations d'hôtes :

- Vulnérabilités et expositions courantes
- Évaluations Center for Internet Security (CIS)
- Bonnes pratiques de sécurité pour Amazon Inspector Classic

Joignabilité de réseau

Les règles du package Network Reachability analysent les configurations de votre réseau afin de détecter les failles de sécurité de vos instances EC2. Les résultats qu'Amazon Inspector génère apprennent également à limiter l'accès qui n'est pas sécurisé.

Le package de règles d'accessibilité réseau utilise les dernières technologies issues de l'initiative AWS Provable Security.

Les résultats générés par ces règles montrent si vos connexions sont accessibles depuis Internet via une passerelle Internet (y compris les instances derrière des Équilibreurs de charge d'application ou classiques), une connexion d'appairage de VPC ou une connexion VPN via une passerelle virtuelle. Ces résultats mettent également en évidence les configurations de réseau qui permettent un accès potentiellement malveillant, telles que les groupes de sécurité mal gérés, les listes de contrôle d'accès (ACL), les IGW, et ainsi de suite.

Ces règles permettent d'automatiser la surveillance de vos réseaux AWS et d'identifier les endroits où l'accès réseau à vos instances EC2 est susceptible d'être mal configuré. En incluant ce package dans votre exécution d'évaluation, vous pouvez mettre en œuvre des contrôles de sécurité de réseau détaillés sans avoir à installer les analyseurs et envoyer des paquets qui sont complexes et coûteux à gérer, notamment à travers des connexions d'appairage de VPC et des réseaux privés virtuels.

> **Important**
>
> Un agent Amazon Inspector Classic n'est pas nécessaire pour évaluer vos instances EC2 avec ce package de règles. Toutefois, un agent installé peut fournir des informations sur la présence d'un processus à l'écoute sur les ports. N'installez pas d'agent sur un système d'exploitation non pris en charge par Amazon Inspector Classic. Si un agent est présent sur une instance qui exécute un système d'exploitation non pris en charge, le package de règles de Joignabilité de réseau ne fonctionnera pas sur cette instance.

Pour plus d'informations, consultez Ensembles de règles Amazon Inspector Classic pour les systèmes d'exploitation pris en charge.

Configurations analysées

Les règles de Joignabilité de réseau analysent la configuration des entités suivantes pour des vulnérabilités :

- Instances Amazon EC2
- Application Load Balancers
- Direct Connect
- Elastic Load Balancers
- Interfaces réseau Elastic
- Passerelles Internet (IGW)

- Listes de contrôle d'accès réseau (ACL)
- Tables de routage
- Groupes de sécurité (SG)
- Sous-réseaux
- Virtual Private Clouds (VPC)
- Passerelles privées virtuelles (VGW)
- Connexions d'appairage de VPC

Chemins de joignabilité

Les règles de Joignabilité de réseau vérifient les chemins de joignabilité suivants, qui correspondent aux façons dont vos connexions sont accessibles de l'extérieur de votre VPC :

- **`Internet`** - Passerelles Internet (y compris les Équilibreurs de charge d'application et les Équilibreurs de charge classiques)
- **`PeeredVPC`** - Connexions d'appairage de VPC
- **`VGW`** - Passerelles privées virtuelles

Types de résultats

Une évaluation qui comprend l'ensemble de règles de Joignabilité de réseau peut renvoyer les types suivants de résultats pour chaque chemin de joignabilité :

- `RecognizedPort`
- `UnrecognizedPortWithListener`
- `NetworkExposure`

`RecognizedPort`

Un port qui est généralement utilisé pour un service bien connu est accessible. Si un agent est présent sur l'instance EC2 cible, le résultat généré indiquera également s'il existe un processus d'écoute actif sur le port. Les résultats de ce type sont indiqués en fonction de la gravité d'un impact de sécurité du service bien connu :

- **`RecognizedPortWithListener`**— Un port reconnu est accessible de l'extérieur depuis l'Internet public via un composant réseau spécifique, et un processus est en cours d'écoute sur le port.
- **`RecognizedPortNoListener`**— Un port est accessible de l'extérieur depuis l'Internet public via un composant réseau spécifique, et aucun processus n'écoute le port.
- **`RecognizedPortNoAgent`**— Un port est accessible de l'extérieur depuis l'Internet public via un composant réseau spécifique. La présence d'un processus d'écoute sur le port ne peut pas être déterminée sans l'installation d'agent sur l'instance cible.

Le tableau suivant présente une liste des ports reconnus :

Service	Ports TCP	Ports UDP
SMB	445	445
NetBIOS	137, 139	137, 138
LDAP	389	389
LDAP via TLS	636	
Catalogue global LDAP	3268	
Catalogue global LDAP via TLS	3269	
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752
RPC	111, 135, 530	111, 135, 530
WINS	1512, 42	1512, 42
DHCP	67, 68, 546, 547	67, 68, 546, 547
Syslog	601	514
Services d'impression	515	

Service	Ports TCP	Ports UDP
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017, 27018, 27019, 28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521, 1630	
Elasticsearch	9300, 9200	
HTTP	80	80
HTTPS	443	443

`UnrecogizedPortWithListener`

Un port qui n'est pas répertorié dans le tableau précédent est accessible et dispose d'un processus d'écoute actif. Les résultats de ce type contenant des informations sur les processus d'écoute, ils ne peuvent être générés que lorsqu'un agent Amazon Inspector est installé sur l'instance EC2 cible. Les résultats de ce type sont indiqués à faible gravité.

`NetworkExposure`

Les résultats de ce type présentent des informations agrégées sur les ports accessibles sur votre instance EC2. Pour chaque combinaison d'interfaces réseau élastiques et de groupes de sécurité sur une instance EC2, ces résultats indiquent l'ensemble accessible de plages de ports TCP et UDP. Les résultats de ce type disposent d'une sévérité Informative.

Vulnérabilités et expositions courantes

Les règles de ce package permettent de vérifier si les instances EC2 de vos cibles d'évaluation sont exposées à des vulnérabilités et à des expositions (CVE) courantes. Les attaques peuvent exploiter les vulnérabilités non patchées pour compromettre la confidentialité, l'intégrité ou la disponibilité de votre service ou de vos données. Le système CVE fournit une méthode de référence pour détecter les vulnérabilités de sécurité et expositions publiquement connues des informations. Pour plus d'informations, consultez https://cve.mitre.org/.

Si un CVE spécifique apparaît dans un résultat produit par une évaluation Amazon Inspector Classic, vous pouvez rechercher l'ID du CVE sur https://cve.mitre.org/ (par exemple,**CVE-2009-0021**). Les résultats de recherche peuvent fournir des informations détaillées sur cette CVE, sa gravité, et la façon de l'atténuer.

Pour le package de règles CVE (Common Vulnerabilities & Exploits), Amazon Inspector a mappé le score de base CVSS et les niveaux de gravité ALAS fournis :

Gravité d'Amazon Inspector	Score de base CVSS	Sévérité ALAS (si le CVSS n'est pas noté)
Élevée	>= 5	Critique ou important
Medium	< 5 and >= 2,1	Medium
Faible	< 2.1 and >= 0,8	Faible
Informationnel	< 0,8	N/A

Les règles incluses dans ce package vous aident à déterminer si vos instances EC2 sont exposées aux CVE dans les listes régionales suivantes :

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- UE (Irlande)
- UE (Francfort)

- UE (Londres)
- UE (Stockholm)
- Asie-Pacifique (Tokyo)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Sydney)
- AWS GovCloud West (États-Unis)
- AWS GovCloud East (États-Unis)

Le package de règles CVE est mis à jour régulièrement ; cette liste inclut les CVE qui sont incluses dans les exécutions d'évaluation qui ont lieu au moment où elle est récupérée.

Pour plus d'informations, voir Ensembles de règles Amazon Inspector Classic pour les systèmes d'exploitation pris en charge.

Évaluations Center for Internet Security (CIS)

Le programme CIS Security Benchmarks fournit les meilleures pratiques sectorielles bien définies, impartiales et consensuelles pour aider les entreprises à évaluer et à améliorer leur sécurité. AWS est une société membre de CIS Security Benchmarks. Pour obtenir la liste des certifications Amazon Inspector Classic, consultez la page Amazon Web Services sur le site Web du CIS.

Amazon Inspector Classic fournit actuellement les packages de règles certifiés CIS suivants pour aider à établir des postures de configuration sécurisées pour les systèmes d'exploitation suivants :

Amazon Linux

- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1`
- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2`
- `CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1`
- `CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2`
- `CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1`

CentOS Linux

- `CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server`

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

Utilisation de Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)

- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

Si un benchmark CIS spécifique apparaît dans un résultat produit par une évaluation Amazon Inspector Classic, vous pouvez télécharger une description PDF détaillée du benchmark sur https://benchmarks.cisecurity.org/ (inscription gratuite requise). Le document d'évaluation fournit des informations détaillées sur cette évaluation CIS, la gravité du problème et la manière de l'atténuer.

Pour plus d'informations, voir Ensembles de règles Amazon Inspector Classic pour les systèmes d'exploitation pris en charge.

Bonnes pratiques de sécurité pour Amazon Inspector Classic

Utilisez les règles Amazon Inspector Classic pour déterminer si vos systèmes sont configurés de manière sécurisée.

> **Important**
>
> À l'heure actuelle, vous pouvez inclure dans vos objectifs d'évaluation des instances EC2 exécutant les systèmes d'exploitation Linux ou Windows.
> Lors d'une exécution d'évaluation, les règles décrites dans cette section génèrent des résultats.seulementpour les instances EC2 exécutant des systèmes d'exploitation Linux.
> Les règles ne génèrent pas de résultats pour les instances EC2 qui exécutent des systèmes d'exploitation Windows.

Pour plus d'informations, consultez Ensembles de règles Amazon Inspector Classic pour les systèmes d'exploitation pris en charge.

Rubriques

Désactivation de la connexion racine via SSH

Cette règle permet de déterminer si le démon SSH est configuré pour autoriser la connexion à votre instance EC2 en tant que racine.

Gravité

Moyenne

Résultat

Votre objectif d'évaluation comprend une instance EC2 qui est configurée pour autoriser les utilisateurs à se connecter à l'aide des informations d'identification du compte racine via SSH. Cela augmente la probabilité d'une attaque en force réussie.

Résolution

Nous vous recommandons de configurer votre instance EC2 pour empêcher les connexions de compte racine via SSH. Il est préférable de vous connecter en tant qu'utilisateur non-racine et d'utiliser `sudo` pour augmenter les privilèges si nécessaire. Pour désactiver les connexions de compte racine via SSH, réglez `PermitRootLogin` sur `no` dans le fichier `/etc/ssh/sshd_config`, puis redémarrez `sshd`.

Prise en charge de SSH version 2 uniquement

Cette règle permet de déterminer si vos instances EC2 sont configurées pour prendre en charge le protocole SSH version 1.

Gravité

Moyenne

Résultat

Votre objectif d'évaluation comprend une instance EC2 qui est configurée pour prendre en charge SSH-1, qui comporte des défauts de conception inhérents réduisant considérablement sa sécurité.

Résolution

Nous vous recommandons de configurer les instances EC2 de votre objectif d'évaluation pour qu'elles prennent en charge uniquement SSH-2 et ses versions ultérieures. Pour OpenSSH, vous pouvez aboutir à cela en définissant `Protocol 2` dans le fichier `/etc/ssh/sshd_config`. Pour plus d'informations, consultez `man sshd_config`.

Désactivation de l'authentification par mot de passe via SSH

Cette règle permet de déterminer si vos instances EC2 sont configurées pour prendre en charge l'authentification par mot de passe via le protocole SSH.

Gravité

Moyenne

Résultat

Votre objectif d'évaluation comprend une instance EC2 qui est configurée pour prendre en charge l'authentification par mot de passe via SSH. L'authentification par mot de passe est susceptible de faire l'objet d'attaques en force et doit donc être désactivée au profit de l'authentification basée sur des clés dans la mesure du possible.

Résolution

Nous vous recommandons de désactiver l'authentification par mot de passe via SSH dans vos instances EC2 et d'activer la prise en charge de l'authentification basée sur des clés à la

place. Cela réduit considérablement la probabilité d'une attaque en force réussie. Pour plus d'informations, consultez https://aws.amazon.com/articles/1233/. Si l'authentification par mot de passe est prise en charge, il est important de limiter l'accès au serveur SSH aux adresses IP autorisées.

Configuration de l'âge maximal des mots de passe

Cette règle permet de déterminer si l'âge maximal des mots de passe est configuré pour vos instances EC2.

Gravité

Moyenne

Résultat

Votre objectif d'évaluation comprend une instance EC2 pour laquelle l'âge maximal des mots de passe n'est pas configuré.

Résolution

Si vous utilisez des mots de passe, nous vous recommandons de configurer l'âge maximal des mots de passe pour toutes les instances EC2 de votre objectif d'évaluation. Cela impose aux utilisateurs de modifier régulièrement leurs mots de passe et cela réduit les risques d'attaque réussie de découverte du mot de passe. Afin de résoudre ce problème pour les utilisateurs existants, utilisez la commande chage. Afin de configurer l'âge maximal des mots de passe pour tous les futurs utilisateurs, modifiez le champ `PASS_MAX_DAYS` du fichier `/etc/login.defs`.

Configuration de la longueur minimale des mots de passe

Cette règle permet de déterminer si la longueur minimale des mots de passe est configurée pour vos instances EC2.

Gravité

Moyenne

Résultat

Votre objectif d'évaluation comprend une instance EC2 pour laquelle la longueur minimale des mots de passe n'est pas configurée.

Résolution

Si vous utilisez des mots de passe, nous vous recommandons de configurer la longueur minimale des mots de passe pour toutes les instances EC2 de votre objectif d'évaluation. L'application d'une longueur minimale des mots de passe réduit le risque d'attaque réussie de découverte du mot de passe. Pour ce faire, utilisez l'option suivante du.`pwquality.conf`dans le fichier: `minlen`. Pour plus d'informations, consultez.https://linux.die.net/man/5/pwquality.conf.

Si`pwquality.conf`n'est pas disponible sur votre instance, vous pouvez définir la valeur du.`minlen`à l'aide de l'option`pam_cracklib.so`module. Pour plus d'informations, consultez `man pam_cracklib`.

Le`minlen`Cette option doit être définie sur 14 ou plus.

Configuration de la complexité des mots de passe

Cette règle permet de déterminer si un mécanisme de complexité des mots de passe est configuré pour vos instances EC2.

Gravité

Moyenne

Résultat

Aucun mécanisme de complexité des mots de passe ni aucune restriction n'est configuré pour les instances EC2 de votre objectif d'évaluation. Cela permet aux utilisateurs de définir des mots de passe simples, ce qui augmente les risques que des utilisateurs non autorisés accèdent aux comptes et les utilisent à mauvais escient.

Résolution

Si vous utilisez des mots de passe, nous vous recommandons de configurer toutes les instances EC2 de votre objectif d'évaluation pour qu'elles exigent un certain niveau de complexité des mots de passe. Pour ce faire, vous pouvez utiliser les options suivantes dans le fichier `pwquality.conf` : `lcredit`, `ucredit`, `dcredit` et `ocredit`. Pour plus d'informations, consultez https://linux.die.net/man/5/pwquality.conf.

Si `pwquality.conf` n'est pas disponible sur votre instance, vous pouvez définir les options `lcredit`, `ucredit`, `dcredit` et `ocredit` à l'aide du module `pam_cracklib.so`. Pour plus d'informations, consultez `man pam_cracklib`.

La valeur attendue pour chacune de ces options est inférieure ou égale à -1, comme indiqué ci-dessous :

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

De plus, l'option `remember` doit être définie sur 12 ou plus. Pour plus d'informations, consultez `man pam_unix`.

Activation d'ASLR

Cette règle permet de déterminer si la randomisation du format d'espace d'adresse (ASLR) est activée sur les systèmes d'exploitation des instances EC2 de votre objectif d'évaluation.

Gravité

Moyenne

Résultat

L'ASLR n'est pas activée pour une instance EC2 de votre objectif d'évaluation.

Résolution

Pour améliorer la sécurité de votre objectif d'évaluation, nous vous recommandons d'activer l'ASLR sur les systèmes d'exploitation de toutes les instances EC2 de votre objectif en exécutant la commandeecho 2 | sudo tee /proc/sys/kernel/randomize_va_space.

Activer la DEP

Cette règle permet de déterminer si la prévention de l'exécution des données (DEP) est activée sur les systèmes d'exploitation des instances EC2 de votre objectif d'évaluation.

> **Note**
>
> Cette règle n'est pas prise en charge pour les instances EC2 dotées de processeurs ARM.

Gravité

Moyenne

Résultat

La DEP n'est pas activée pour une instance EC2 de votre objectif d'évaluation.

Résolution

Nous vous recommandons d'activer la DEP sur les systèmes d'exploitation de toutes les instances EC2 de votre objectif d'évaluation. L'activation de la DEP protège vos instances contre les risques de sécurité à l'aide des techniques de dépassement de mémoire tampon.

Configuration des autorisations pour les répertoires système

Cette règle vérifie les autorisations sur les répertoires système qui contiennent des fichiers binaires et des informations de configuration du système. Il vérifie que seul l'utilisateur racine (un utilisateur qui se connecte à l'aide des informations d'identification du compte racine) dispose des autorisations d'écriture sur ces répertoires.

Gravité

Élevée

Résultat

Une instance EC2 de votre objectif d'évaluation contient un répertoire système qui est accessible en écriture par les utilisateurs non-racine.

Résolution

Afin d'améliorer la sécurité de votre objectif d'évaluation et d'empêcher l'escalade des privilèges par des utilisateurs locaux malveillants, configurez tous les répertoires système de toutes les instances EC2 de votre cible de telle manière qu'ils ne soient accessibles en écriture que par les utilisateurs qui se connectent à l'aide des informations d'identification du compte racine.

Modèles d'évaluation et cycles d'évaluation Amazon Inspector Classic

Amazon Inspector Classic vous aide à découvrir les problèmes de sécurité potentiels en utilisant des règles de sécurité pour analyser vos AWS ressources. Amazon Inspector Classic surveille et collecte les données comportementales (télémétrie) relatives à vos ressources. Les données incluent des informations sur l'utilisation de canaux sécurisés, le trafic réseau entre les processus en cours d'exécution et les détails de la communication avec AWS les services. Ensuite, Amazon Inspector Classic analyse et compare les données par rapport à un ensemble de packages de règles de sécurité. Enfin, Amazon Inspector Classic produit une liste de résultats qui identifient les problèmes de sécurité potentiels de différents niveaux de gravité.

Pour commencer, vous devez créer un objectif d'évaluation (un ensemble de AWS ressources que vous souhaitez qu'Amazon Inspector Classic analyse). Ensuite, vous créez un modèle d'évaluation (un plan que vous utilisez pour configurer votre évaluation). Vous utilisez le modèle pour lancer une exécution d'évaluation, c'est-à-dire le processus de surveillance et d'analyse qui génère un ensemble de résultats.

Rubriques

Modèles d'évaluation Amazon Inspector Classic

Un modèle d'évaluation vous permet de spécifier la configuration de vos exécutions d'évaluation, notamment les éléments suivants :

- Packages de règles utilisés par Amazon Inspector Classic pour évaluer votre objectif d'évaluation

- Durée de l'évaluation : vous pouvez définir la durée d'une évaluation entre 3 minutes et 24 heures. Nous vous recommandons de définir la durée des exécutions d'évaluation sur 1 heure.
- Rubriques Amazon SNS auxquelles Amazon Inspector Classic envoie des notifications concernant l'état et les résultats de votre cycle d'évaluation
- Attributs Amazon Inspector Classic (paires clé-valeur) que vous pouvez attribuer aux résultats générés par le cycle d'évaluation utilisant ce modèle d'évaluation

Une fois qu'Amazon Inspector Classic a créé le modèle d'évaluation, vous pouvez le baliser comme n'importe quelle autre AWS ressource. Pour plus d'informations, consultez Tag Editor. Le balisage des modèles d'évaluation vous permet de les organiser et d'assurer une meilleure surveillance de votre stratégie de sécurité. Par exemple, Amazon Inspector Classic propose un grand nombre de règles par rapport auxquelles vous pouvez évaluer vos objectifs d'évaluation. Vous souhaiterez peut-être inclure divers sous-ensembles de règles disponibles dans vos modèles d'évaluation afin de cibler des zones de préoccupation particulières ou de découvrir des problèmes de sécurité spécifiques. Le balisage des modèles d'évaluation vous permet de les localiser et de les exécuter rapidement à tout moment en fonction de vos objectifs et de votre stratégie de sécurité.

> **Important**
>
> Une fois que vous avez créé un modèle d'évaluation, vous ne pouvez plus le modifier.

Limites des modèles d'évaluation Amazon Inspector Classic

Vous pouvez créer jusqu'à 500 modèles d'évaluation pour chaque AWS compte.

Pour plus d'informations, consultez Limites de service Amazon Inspector Classic.

Création d'un modèle d'évaluation

Pour créer un modèle d'évaluation

1. Connectez-vous à la console Amazon Inspector Classic AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/inspector/.
2. Dans le volet de navigation, choisissez Modèles d'évaluation, puis Créer.
3. Dans Nom, saisissez un nom pour votre modèle d'évaluation.

4. Dans Nom de l'objectif, choisissez un objectif d'évaluation à analyser.

> **Note**
>
> Lorsque vous créez un modèle d'évaluation, vous pouvez utiliser le bouton Prévisualiser la cible sur la page Modèles d'évaluation pour passer en revue toutes les instances EC2 incluses dans la cible d'évaluation. Pour chaque instance EC2, vous pouvez consulter le nom d'hôte, l'ID de l'instance, l'adresse IP et, le cas échéant, le statut de l'agent. Le statut de l'agent peut prendre les valeurs suivantes : SAIN, MALSAIN et INCONNU. Amazon Inspector Classic affiche le statut INCONNU lorsqu'il ne parvient pas à déterminer si un agent est en cours d'exécution sur l'instance EC2.
> Vous pouvez également utiliser le bouton Preview Target sur la page Modèles d'évaluation pour vérifier les instances EC2 qui constituent des objectifs d'évaluation inclus dans vos modèles précédemment créés.

5. Dans Packages de règles, choisissez un ou plusieurs packages de règles à inclure dans votre modèle d'évaluation.
6. Pour Durée, spécifiez la durée de votre modèle d'évaluation.
7. (Facultatif) Pour les rubriques SNS, spécifiez une rubrique SNS à laquelle vous souhaitez qu'Amazon Inspector Classic envoie des notifications concernant l'état et les résultats des évaluations. Amazon Inspector Classic peut envoyer des notifications SNS concernant les événements suivants :

   - Une exécution d'évaluation a commencé
   - Une exécution d'évaluation est terminée
   - Le statut d'une exécution d'évaluation a changé
   - Un résultat a été généré

   Pour plus d'informations sur la configuration d'une rubrique SNS, consultez Configuration d'une rubrique SNS pour les notifications Amazon Inspector Classic.
8. (Facultatif) Pour Balise, saisissez les valeurs souhaitées dans les champs Clé et Valeur. Vous pouvez ajouter plusieurs balises au modèle d'évaluation.
9. (Facultatif) Pour les attributs ajoutés aux résultats, entrez les valeurs de clé et de valeur. Amazon Inspector Classic applique les attributs à tous les résultats générés par le modèle d'évaluation. Vous pouvez ajouter plusieurs attributs au modèle d'évaluation. Pour plus d'informations sur les résultats et le balisage des résultats, consultez Résultats d'Amazon Inspector Classic.

10. (Facultatif) Pour configurer un calendrier pour vos exécutions d'évaluation à l'aide de ce modèle, sélectionnez la case Set up recurring assessment runs once every <number_of_days>, starting now (Configurer des exécutions d'évaluation récurrentes une fois tous les <nombre de jours> à partir de maintenant) et spécifiez le modèle de récurrence (nombre de jours) à l'aide des flèches vers le haut et vers le bas.

> **Note**
>
> Lorsque vous cochez cette case, Amazon Inspector Classic crée automatiquement une règle Amazon CloudWatch Events pour le calendrier des cycles d'évaluation que vous configurez. Amazon Inspector Classic crée ensuite automatiquement un rôle IAM nomméAWS_InspectorEvents_Invoke_Assessment_Template. Ce rôle permet à CloudWatch Events d'effectuer des appels d'API vers les ressources Amazon Inspector Classic. Pour plus d'informations, consultez Qu'est-ce qu'Amazon CloudWatch Events ? et en utilisant des politiques basées sur les ressources pour CloudWatch les événements.

> **Note**
>
> Vous pouvez également configurer des exécutions d'évaluation automatiques via une fonction AWS Lambda . Pour plus d'informations, consultez La configuration de l'évaluation automatique passe par une fonction Lambda.

11. Choisissez Créer et exécuter ou Créer.

Suppression d'un modèle d'évaluation

Pour supprimer un modèle d'évaluation, utilisez la procédure suivante.

Pour supprimer un modèle d'évaluation

- Sur la page Assessment Templates (Modèles d'évaluation), choisissez le modèle à supprimer, puis choisissez Delete (Supprimer). Lorsque vous êtes invité à confirmer l'opération, choisissez Yes (Oui).

> **Important**
>
> Lorsque vous supprimez un modèle d'évaluation, tous les modèles d'évaluation, toutes les exécutions d'évaluation, tous les résultats et toutes les versions des rapports associés à ce modèle sont également supprimés.

Vous pouvez également supprimer un modèle d'évaluation à l'aide de l'API `DeleteAssessmentTemplate`.

Exécutions d'évaluation

Après avoir créé un modèle d'évaluation, vous pouvez l'utiliser pour lancer des exécutions d'évaluation. Vous pouvez démarrer plusieurs essais en utilisant le même modèle tant que vous respectez la limite de points fixée pour chaque AWS compte. Pour plus d'informations, consultez Limites des cycles d'évaluation Amazon Inspector Classic .

Si vous utilisez la console Amazon Inspector Classic, vous devez démarrer la première exécution de votre nouveau modèle d'évaluation depuis la page Modèles d'évaluation. Après avoir lancé l'exécution, vous pouvez utiliser la page Exécutions d'évaluation pour surveiller sa progression. Utilisez les boutons Exécuter, Annuler et Supprimer pour démarrer, annuler ou supprimer une exécution. Vous pouvez également afficher les détails de l'exécution, dont l'ARN de l'exécution, les packages de règles sélectionnés pour celle-ci, les balises et attributs que vous avez appliqués à cette exécution, et bien plus encore.

Pour les exécutions suivantes du modèle d'évaluation, vous pouvez utiliser les boutons Exécuter, Annuler et Supprimer de la page Modèles d'exécution ou de la page Exécutions d'évaluation.

Suppression d'une exécution d'évaluation

Pour supprimer une exécution d'évaluation, utilisez la procédure suivante.

Pour supprimer une exécution

- Sur la page Assessment runs (Exécutions d'évaluation), choisissez l'exécution à supprimer, puis choisissez Delete (Supprimer). Lorsque vous êtes invité à confirmer l'opération, choisissez Yes (Oui).

> **Important**
>
> Lorsque vous supprimez une exécution, tous les résultats et toutes les versions du rapport de cette exécution sont également supprimés.

Vous pouvez aussi supprimer une exécution en utilisant l'API `DeleteAssessmentRun`.

Limites des cycles d'évaluation Amazon Inspector Classic

Vous pouvez créer jusqu'à 50 000 cycles d'évaluation pour chaque AWS compte.

Vous pouvez avoir plusieurs exécutions en même temps tant que les cibles utilisées pour les exécutions ne contiennent pas d'instances EC2 qui se chevauchent.

Pour plus d'informations, consultez Limites de service Amazon Inspector Classic.

La configuration de l'évaluation automatique passe par une fonction Lambda

Si vous souhaitez configurer un calendrier récurrent pour votre évaluation, vous pouvez configurer votre modèle d'évaluation pour qu'il s'exécute automatiquement en créant une fonction Lambda à l'aide de la AWS Lambda console. Pour plus d'informations, consultez Fonctions Lambda.

Pour configurer des cycles d'évaluation automatiques à l'aide de la AWS Lambda console, effectuez la procédure suivante.

Pour configurer des exécutions automatiques via une fonction Lambda

1. Connectez-vous à la AWS Management ConsoleAWS Lambda console et ouvrez-la.
2. Dans le volet de navigation, choisissez Dashboard ou Functions, puis choisissez Create a Lambda Function.
3. Sur la page Create function (Créer une fonction), choisissez Browse serverless app repository (Parcourir le référentiel d'applications sans serveur), puis saisissez **`inspector`** dans le champ de recherche.
4. Choisissez le modèle inspector-scheduled-run.

5. Sur la page Révision, configuration et déploiement, configurez un calendrier récurrent pour les exécutions automatisées en spécifiant un CloudWatch événement qui déclenche votre fonction. Pour ce faire, saisissez un nom de règle et une description, puis choisissez une expression de planification. L'expression de planification détermine la fréquence à laquelle se produit l'exécution, par exemple, toutes les 15 minutes ou une fois par jour. Pour plus d'informations sur les CloudWatch événements et les concepts, consultez Qu'est-ce qu'Amazon CloudWatch Events ?

   Si vous cochez la case Enable trigger (Activer le déclencheur), l'exécution d'évaluation commence dès que vous avez fini de créer votre fonction. Les exécutions automatiques suivantes respecteront le modèle de récurrence spécifié dans le champ Schedule expression (Programmer l'expression). Si vous ne cochez pas la case Enable trigger lors de la création de la fonction, vous pouvez modifier la fonction ultérieurement pour activer ce déclencheur.

6. Sur la page Configure function, spécifiez les éléments suivants :

   - Pour Nom, saisissez le nom de votre fonction.
   - (Facultatif) Pour Description, saisissez une description qui vous aidera à identifier votre fonction ultérieurement.
   - Pour l'exécution, conservez la valeur par défaut de**`Node.js 8.10`**. AWS Lambda prend en charge le inspector-scheduled-runplan uniquement pour le temps **`Node.js 8.10`** d'exécution.
   - Indiquez le modèle d'évaluation que vous souhaitez exécuter automatiquement à l'aide de cette fonction. Pour ce faire, vous devez fournir la valeur de la variable d'environnement appelée assessmentTemplateArn.
   - Pour le gestionnaire, conservez la valeur par défaut de **`index.handler`**.
   - Définissez les autorisations pour votre fonction à l'aide du champ Rôle. Pour plus d'informations, consultez Modèle d'autorisations AWS Lambda.

     Pour exécuter cette fonction, vous avez besoin d'un rôle IAM qui permet de AWS Lambda démarrer les exécutions et d'écrire des messages de journal concernant les exécutions, y compris les erreurs éventuelles, dans Amazon CloudWatch Logs. AWS Lambda assume ce rôle pour chaque exécution automatique récurrente. Par exemple, vous pouvez associer le modèle de politique suivant à ce rôle IAM :

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

```
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

7. Passez en revue vos sélections, puis choisissez Create function.

Configuration d'une rubrique SNS pour les notifications Amazon Inspector Classic

Amazon Simple Notification Service (Amazon SNS) est un service Web qui envoie des messages aux points de terminaison ou aux clients abonnés. Vous pouvez utiliser Amazon SNS pour configurer les notifications pour Amazon Inspector Classic.

Pour configurer une rubrique SNS pour les notifications

1. Créez une rubrique SNS. Consultez Didacticiel : Création d'une rubrique Amazon SNS. Lorsque vous créez la rubrique, développez la section Access policy - optional (Stratégie d'accès - facultatif). Ensuite, procédez de la façon suivante pour autoriser l'évaluation à envoyer des messages dans la rubrique :

   a. Pour Choose method (Choisir une méthode), choisissez Basic (De base).

   b. Pour Définir qui peut publier des messages sur le sujet, choisissez Uniquement les AWS comptes spécifiés, puis entrez l'ARN du compte dans la région dans laquelle vous créez le sujet :

      - `US East (Ohio)` - arn:aws:iam::646659390643:root
      - `US East (N. Virginia)`- arn:aws:iam::316112463485:root
      - `US West (N. California)` - arn:aws:iam::166987590008:root
      - `US West (Oregon)` - arn:aws:iam::758058086616:root
      - `Asia Pacific (Mumbai)` - arn:aws:iam::162588757376:root

- `Asia Pacific (Seoul)` - arn:aws:iam::526946625049:root
- `Asia Pacific (Sydney)` - arn:aws:iam::454640832652:root
- `Asia Pacific (Tokyo)` - arn:aws:iam::406045910587:root
- `Europe (Frankfurt)` - arn:aws:iam::537503971621:root
- `Europe (Ireland)` - arn:aws:iam::357557129151:root
- `Europe (London)` - arn:aws:iam::146838936955:root
- `Europe (Stockholm)` - arn:aws:iam::453420244670:root
- `AWS GovCloud (US-East)`- arn ::iam : :206278770380:root aws-us-gov
- `AWS GovCloud (US-West)`- arn ::iam : :850862329162 : root aws-us-gov

c. Pour Définir qui peut s'abonner à cette rubrique, choisissez Uniquement les AWS comptes spécifiés, puis entrez l'ARN du compte dans la région dans laquelle vous créez la rubrique.

d. Pour éviter que l'Inspecteur ne soit utilisé comme un adjoint confus, comme indiqué dans la section Problème d'adjoint confus du guide de l'utilisateur de l'IAM, procédez comme suit :

i. Choisir Advanced (Avancé). Cela vous dirigera vers l'éditeur JSON.

ii. Ajoutez la condition suivante :

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:inspector:*:*:*"
   }
 }
```

e. (Facultatif) Pour plus d'informations sur aws : SourceAccount et aws :SourceArn, consultez la section Clés contextuelles des conditions globales dans le guide de l'utilisateur IAM.

f. Mettez à jour les autres paramètres pour la rubrique si nécessaire, puis choisissez Create topic (Créer la rubrique).

2. (Facultatif) Pour créer une rubrique SNS chiffrée, consultez la section Chiffrement au repos dans le guide du développeur SNS.

3. Pour éviter que l'Inspector ne soit utilisé comme un adjoint confus pour votre clé KMS, suivez les étapes supplémentaires ci-dessous :

a. Accédez à votre clé CMK dans la console KMS.

b. Choisissez Modifier.

c. Ajoutez la condition suivante :

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
 }
```

4. Créez un abonnement à la rubrique que vous avez créée. Pour plus d'informations, consultez Didacticiel : Abonnement d'un point de terminaison à une rubrique Amazon SNS.
5. Pour vérifier que l'abonnement est configuré correctement, publiez un message dans la rubrique. Pour plus d'informations, consultez Didacticiel : Publication d'un message dans une rubrique Amazon SNS.

Résultats d'Amazon Inspector Classic

Les résultats sont des problèmes de sécurité potentiels découverts par Amazon Inspector Classic lors de l'évaluation de votre objectif d'évaluation. Les résultats sont affichés sur la console Amazon Inspector Classic ou via l'API. Les résultats contiennent une description détaillée des problèmes de sécurité, ainsi que des recommandations pour les résoudre.

Une fois qu'Amazon Inspector a généré les résultats, vous pouvez les suivre en leur attribuant des attributs Amazon Inspector Classic. Ces attributs sont des paires clé-valeur.

Le suivi des résultats à l'aide d'attributs peut s'avérer très utile pour gérer le flux de travail de votre stratégie de sécurité. Par exemple, une fois que vous avez créé et exécuté une évaluation, elle génère une liste de résultats présentant divers niveaux de gravité, d'urgence et d'intérêt, en fonction de votre approche et de vos objectifs de sécurité. Vous souhaiterez peut-être suivre immédiatement les recommandations d'un résultat pour résoudre un problème de sécurité potentiellement urgent. Ou bien vous souhaiterez peut-être différer la résolution d'un autre résultat jusqu'à la prochaine mise à jour du service. Par exemple, pour suivre un résultat à résoudre immédiatement, vous pouvez créer et lui affecter un attribut ayant la paire clé-valeur **`Status`** / **`Urgent`**. Vous pouvez également utiliser des attributs pour distribuer la charge de travail de la résolution des problèmes de sécurité potentiels. Par exemple, pour charger Bob (qui est un ingénieur sécurité de votre équipe) de la tâche de résolution d'un résultat, vous pouvez affecter à ce résultat un attribut ayant la paire clé-valeur **`Assigned Engineer`** / **`Bob`**.

Utilisation des résultats

Effectuez la procédure suivante pour tous les résultats générés par Amazon Inspector Classic.

Pour trouver et analyser les résultats et leur affecter des attributs

1. Connectez-vous à la console Amazon Inspector Classic AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/inspector/.
2. Après avoir effectué une évaluation, accédez à la page Résultats de la console Amazon Inspector Classic pour consulter vos résultats.

   Vous pouvez également consulter vos résultats dans la section Résultats notables de la page Tableau de bord de la console Amazon Inspector Classic.

> **Note**
>
> Vous ne pouvez pas consulter les résultats générés par une exécution d'évaluation alors qu'elle est toujours en cours. Cependant, vous pouvez afficher un sous-ensemble de résultats si vous arrêtez l'évaluation avant la fin de son exécution. Dans un environnement de production, nous vous recommandons de laisser chaque exécution d'évaluation se terminer jusqu'au bout afin qu'elle puisse produire un ensemble complet de résultats.

3. Pour afficher les détails d'un résultat spécifique, sélectionnez le widget Développer en regard de ce résultat. Les détails du résultat incluent les éléments suivants :

   - Nom de la cible d'évaluation qui inclut l'instance EC2 où ce résultat a été enregistré.
   - Nom du modèle d'évaluation qui a été utilisé pour produire ce résultat.
   - Heure de début de l'exécution d'évaluation.
   - Heure de fin de l'exécution d'évaluation.
   - Statut de l'exécution d'évaluation.
   - Nom de l'ensemble de règles qui inclut la règle qui a déclenché ce résultat.
   - Nom du résultat.
   - Gravité du résultat.
   - Informations sur la gravité native du Common Vulnerability Scoring System (Système de notation de vulnérabilité courante - CVSS). Ceux-ci comprennent des métriques de vecteur CVSS et de score CVSS (y compris CVSS versions 2.0 et 3.0) pour les résultats générés par les règles de l'ensemble de règles Vulnérabilités et expositions courantes. Pour plus de détails sur le CVSS, consultez https://www.first.org/cvss/.
   - Informations de gravité natives fournies par le Center for Internet Security (CIS). Ceux-ci comprennent la métrique de pondération CIS pour les résultats générés par les règles de l'ensemble de Références CIS. Pour plus d'informations sur la métrique de pondération CIS, consultez https://www.cisecurity.org/.
   - Description du résultat.
   - Étapes recommandées que vous pouvez compléter pour résoudre le problème de sécurité potentiel décrit par le résultat.

4. Pour affecter des attributs à un résultat, choisissez un résultat, puis Ajouter/Modifier des attributs.

Vous pouvez également affecter des attributs aux résultats lorsque vous créez un modèle d'évaluation. Pour ce faire, vous configurez le nouveau modèle pour affecter automatiquement des attributs à tous les résultats générés par l'exécution d'évaluation. Vous pouvez utiliser les champs Clé et Valeur du champ Tags for findings from this assessment (Balises pour les résultats de cette évaluation). Pour plus d'informations, consultez Modèles d'évaluation et cycles d'évaluation Amazon Inspector Classic.

5. Pour exporter des résultats dans une feuille de calcul, cliquez sur la flèche vers le bas dans le coin supérieur droit de la page Résultats. Dans la boîte de dialogue, choisissez Exporter toutes les colonnes ou Exporter les colonnes visibles.

   Notez que dans le contenu exporté, toutes les valeurs datetime sont des horodatages epoch.

6. Pour filtrer vos résultats actuels, entrez une seule chaîne sur laquelle vous souhaitez filtrer, telle qu'un ID d'instance ou un numéro CVE, dans la barre de filtre située au-dessus du tableau des résultats. Pour afficher ou masquer des colonnes d'informations supplémentaires, cliquez sur l'icône des paramètres dans le coin supérieur droit de la page Résultats.

7. Pour supprimer les résultats, accédez à la page Assessment runs (Exécutions d'évaluation) et sélectionnez l'exécution qui a entraîné les résultats que vous souhaitez supprimer. Ensuite, choisissez Supprimer. Lorsque vous êtes invité à confirmer l'opération, choisissez Yes (Oui).

   > **Important**
   >
   > Vous ne pouvez pas supprimer des résultats individuels dans Amazon Inspector Classic. Lorsque vous supprimez une exécution d'évaluation, tous les résultats et toutes les versions du rapport de cette exécution sont également supprimés.

   Vous pouvez également supprimer une évaluation exécutée à l'aide de l'DeleteAssessmentRunAPI.

Rapports d'évaluation

Un Amazon Inspector ClassicRapport d'évaluationest un document qui détaille les éléments testés lors de l'exécution d'évaluation, ainsi que les résultats de l'évaluation. Vous pouvez stocker les rapports, les partager avec votre équipe les mesures correctives nécessaires, ou les utiliser pour augmenter vos données d'audit de conformité. Vous pouvez générer un rapport pour l'exécution d'une évaluation après l'exécution a réussi.

> **Note**
>
> Vous pouvez générer des rapports uniquement pour les exécutions d'évaluation qui se sont déroulées après le 25 avril 2017, c'est-à-dire à partir de la date de disponibilité des rapports d'évaluation dans Amazon Inspector Classic.

Vous pouvez afficher les types de rapports d'évaluation suivants :

- Rapport sur les résultats— ce rapport contient les informations suivantes :
  - Synthèse de l'évaluation
  - Instances EC2 évaluées lors de l'exécution d'évaluation
  - Packages de règles inclus dans l'exécution d'évaluation
  - Informations détaillées sur chaque résultat, y compris toutes les instances EC2 contenant le résultat
- Rapport complet— ce rapport contient toutes les informations incluses dans un rapport de résultats, ainsi que la liste des règles appliquées à toutes les instances de l'objectif d'évaluation.

Pour générer un rapport d'évaluation

1. Dans la page Exécutions d'évaluations, recherchez l'exécution pour laquelle vous souhaitez générer un rapport. Assurez-vous que son état est défini sur Analyse terminée.
2. Choisissez l'icône de rapports sous la colonne Rapports de cette exécution d'évaluation.

> **Important**
>
> L'icône de rapport est présent dans la colonne Rapports uniquement pour les exécutions d'évaluation effectuées le 25 avril 2017 ou après. C'est à ce moment que des rapports d'évaluation dans Amazon Inspector Classic sont devenus disponibles dans.

3. Dans la boîte de dialogue Rapport d'évaluation, sélectionnez le type de rapport que vous souhaitez afficher (soit un rapport de Résultats ou Complet) et le format du rapport (HTML ou PDF). Choisissez ensuite de Générer le rapport.

Vous pouvez également générer des rapports d'évaluation via l'API GetAssessmentReport.

Pour supprimer un rapport d'évaluation, utilisez la procédure suivante.

Pour supprimer un rapport

- Sur la page Assessment runs (Exécutions d'évaluation), choisissez l'exécution sur laquelle le rapport que vous souhaitez supprimer est basé, puis choisissez Delete (Supprimer). Lorsque vous êtes invité à confirmer l'opération, choisissez Oui.

  > **Important**
  >
  > Vous ne pouvez pas supprimer des rapports individuels dans Amazon Inspector Classic. Lorsque vous supprimez une exécution d'évaluation, toutes les versions du rapport de cette exécution et tous les résultats sont également supprimés.

  Vous pouvez également supprimer une exécution d'évaluation à l'aide de l'API DeleteAssessmentRun.

Exclusions dans Amazon Inspector Classic

Les exclusions sont un résultat des exécutions d'évaluation Amazon Inspector Classic. Les exclusions montrent lesquelles de vos vérifications de sécurité ne peuvent pas être effectuées et la manière de résoudre les erreurs. Ces problèmes peuvent être provoqués par exemple par l'absence d'un agent sur les instances EC2 de la cible spécifiée, par l'utilisation d'un système d'exploitation non pris en charge, ou par des erreurs inattendues.

Vous pouvez consulter les exclusions sur la page Assessment runs (Exécutions d'évaluation) de la console. Pour plus d'informations, consultez Affichage des exclusions après évaluation.

Pour éviter de subir des problèmes inutilesAWSfrais, Amazon Inspector Classic vous permet d'afficher un aperçu des exclusions avant d'exécuter une évaluation. Vous pouvez consulter un aperçu des exclusions sur la page Assessment templates (Modèles d'évaluation) de la console. Pour plus d'informations, consultez Aperçu des exclusions.

> **Note**
>
> Vous pouvez générer des exclusions après l'évaluation uniquement pour les exécutions qui se produisent après le 25 juin 2018. C'est alors que les exclusions dans Amazon Inspector Classic sont devenues disponibles. Toutefois, les aperçus des exclusions sont disponibles pour tous les modèles d'évaluation, quelle que soit leur date .

Rubriques

Types d'exclusion

Amazon Inspector Classic peut produire les types d'exclusion d'évaluation suivants.

Type d'exclusion	Description	Recommandation
Aucune instance dans l'objectif	Il n'y a aucune instance EC2 comportant les balises spécifiées dans l'objectif d'évaluation.	Vérifiez que les balises de votre objectif d'évaluation correspondent aux balises de votre instance EC2 cible.
L'agent est déjà en cours d'exécution	Une exécution d'évaluation est déjà en cours sur l'instance EC2 cible.	Patientez jusqu'à la fin de l'exécution d'évaluation actuelle sur l'instance EC2 cible.
Agent introuvable	Aucun agent Amazon Inspector Classic n'a été trouvé sur l'instance EC2 cible.	Installez ou réinstallez un agent Amazon Inspector Classic sur l'instance EC2 cible. Pour plus

Type d'exclusion	Description	Recommandation
		d'informations, consultez Installation des agents Amazon Inspector Classic.
L'agent est défectueux	L'agent Amazon Inspector Classic sur l'instance EC2 cible est dans un état non sain.	Vérifiez l'état de l'agent Amazon Inspector Classic sur cette instance et adoptez les mesures nécessaires. Pour plus d'informations, consultez Inspector Agents (Agents d'inspection).

Type d'exclusion	Description	Recommandation
Version de système d'exploitation non prise en charg	Le système d'exploitation de l'instance EC2 cible n'est pas pris en charge pour les évaluations Amazon Inspector Classic.	Supprimez l'instance EC2 cible de la cible d'évaluation, ou créez une cible qui ne comprend pas cette instance. Pour obtenir une liste des systèmes d'exploitation pris en charge, consultez Systèmes d'exploitation et régions pris en charge par Amazon Inspector Classic.

Type d'exclusion	Description	Recommandation
Packa de règles obsol	Le modèle d'évaluation comprend un package de règles obsolètes.	Créez un modèle d'évaluation sans l'ensemble de règles obsolètes et utilisez-le pour les exécutions d'évaluation futures.

Type d'exclusion	Description	Recommandation
Packa de règles non prises en charg par le systèr d'expl ation	Le système d'exploitation de l'instance EC2 cible n'est pas pris en charge par un package de règles inclus dans le modèle d'évaluation.	Créez d'un modèle d'évaluation sans les packages de règles en conflit ou supprimez l'instance EC2 cible à partir du modèle d'évaluation. Pour obtenir une liste de la prise en charge des packages de règles par système d'exploitation, consultez Disponibilité des packages de règles sur les

Type d'exclusion	Description	Recommandation
		systèmes d'exploitation pris en charge.
Erreur d'évaluation des règles pour une seule instan	Une erreur interne a provoqué l'échec de l'évaluation des règles pour cette instance.	Essayez d'exécuter à nouveau votre évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Type d'exclusion	Description	Recommandation
Erreur d'évaluation des règles	Une erreur interne a provoqué l'échec de l'évaluation des règles pour votre évaluation.	Essayez d'exécuter à nouveau l'évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Type d'exclusion	Description	Recommandation
Erreur de Joignabilité de réseau — interne	Une erreur interne a entraîné un échec d'évaluation de Joignabilité du réseau sur les contrôles pour les ports accessibles depuis Internet. Vous pourrez obtenir des résultats pour d'autres types de Joignabilité de réseau.	Essayez d'exécuter à nouveau l'évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Type d'exclusion	Description	Recommandation
Erreur d'accessibilité réseau — Internet via un Application Load Balan	Une erreur interne a entraîné un échec d'évaluation de Joignabilité du réseau sur les contrôles pour les ports accessibles depuis Internet via un Application Load Balancer. Vous pourrez obtenir des résultats pour d'autres types de Joignabilité de réseau.	Essayez d'exécuter à nouveau l'évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Type d'exclusion	Description	Recommandation
Erreur de Joignabilité de réseau via un équilibreur de charge Elastic Load Balan	Une erreur interne a entraîné un échec d'évaluation de Joignabilité du réseau sur les contrôles pour les ports accessibles depuis Internet via un équilibreur de charge Elastic Load Balancing. Vous pourrez obtenir des résultats pour d'autres types de Joignabilité de réseau.	Essayez d'exécuter à nouveau l'évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Type d'exclusion	Description	Recommandation
Erreur de Joignabilité de réseau — VPN	Une erreur interne a entraîné un échec d'évaluation de Joignabilité du réseau sur les contrôles pour les ports accessibles depuis le VPN. Vous pourrez obtenir des résultats pour d'autres types de Joignabilité de réseau.	Essayez d'exécuter à nouveau l'évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Type d'exclusion	Description	Recommandation
Erreur de Joignabilité de réseau — AWS Direct Conne	Une erreur interne a entraîné un échec d'évaluation de Joignabilité du réseau sur les contrôles pour les ports accessibles via AWS Direct Connect. Vous pourrez obtenir des résultats pour d'autres types de Joignabilité de réseau.	Essayez d'exécuter à nouveau l'évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Type d'exclusion	Description	Recommandation
Erreur de Joignabilité de réseau — appairage de VPC	Une erreur interne a entraîné un échec d'évaluation de Joignabilité du réseau sur les contrôles pour les ports accessibles depuis le VPC appairé. Vous pourrez obtenir des résultats pour d'autres types de Joignabilité de réseau.	Essayez d'exécuter à nouveau l'évaluation. Contactez le support technique si l'exclusion persiste lorsque vous relancez l'évaluation.

Aperçu des exclusions

Amazon Inspector Classic vous permet d'afficher un aperçu des exclusions potentielles avant d'exécuter une évaluation.

Pour afficher un aperçu des exclusions d'évaluation

1. Connectez-vous à la consoleAWS Management Consoleet ouvrez la console Amazon Inspector Classic à l'adressehttps://console.aws.amazon.com/inspector/.
2. Dans le volet de navigation, choisissez Assessment templates (Modèles d'évaluation).
3. Développez un modèle et choisissez Preview exclusions (Afficher un aperçu des exclusions) dans la section Assessment templates (Modèles d'évaluation).
4. Vérifiez les descriptions de toutes les exclusions détectées et les recommandations destinées à les résoudre.

   Vous pouvez également répertorier et décrire les exclusions à l'aide des opérations `ListExclusions` et `DescribeExclusions`.

Affichage des exclusions après évaluation

Après l'exécution d'une évaluation, vous pouvez afficher des détails de toute exclusion.

Pour afficher les détails relatifs aux exclusions

1. Connectez-vous à la consoleAWS Management Consoleet ouvrez la console Amazon Inspector Classic à l'adressehttps://console.aws.amazon.com/inspector/.
2. Dans le volet de navigation, choisissez Assessment runs (Exécutions d'évaluation).
3. Dans la colonne Exclusions, choisissez le lien actif qui est associé à une exécution d'évaluation.
4. Vérifiez les descriptions de toutes les exclusions détectées et les recommandations destinées à les résoudre.

   Vous pouvez également répertorier et décrire les exclusions à l'aide des opérations `ListExclusions` et `DescribeExclusions`.

Ensembles de règles Amazon Inspector Classic pour les systèmes d'exploitation pris en charge

Vous pouvez exécuter des ensembles de règles Amazon Inspector Classic sur les instances EC2 incluses dans vos objectifs d'évaluation. Le tableau suivant affiche la disponibilité des ensembles de règles pour les systèmes d'exploitation pris en charge.

Important

Vous pouvez effectuer une évaluation sans agent avec leJoignabilité de réseauEnsembles de règles sur n'importe quelle instance EC2, quel que soit le système d'exploitation.

Note

Pour plus d'informations sur les systèmes d'exploitation pris en charge, consultez Systèmes d'exploitation et régions pris en charge par Amazon Inspector Classic.

Systè d'exp ation pris en charg	Vulnérabi lités et expositio ns courantes	Evaluations CIS	Joignabilité de réseau	Bonnes pratiques de sécurité	Analyse du comportement d'exécution
Amaz Linux	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Amaz Linux 2018.	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Amaz Linux 2017.	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète

Systè d'exp ation pris en charg	Vulnérabi lités et expositio ns courantes	Evaluations CIS	Joignabilité de réseau	Bonnes pratiques de sécurité	Analyse du comportement d'exécution
Amaz Linux 2017.	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Amaz Linux 2016.	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Amaz Linux 2016.	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Amaz Linux 2015.	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Amaz Linux 2015.	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Amaz Linux 2014.	Pris en charge		Pris en charge	Pris en charge	
Amaz Linux 2014.	Pris en charge		Pris en charge	Pris en charge	
Amaz Linux 2013.	Pris en charge		Pris en charge	Pris en charge	

Systè d'exp ation pris en charg	Vulnérabi lités et expositio ns courantes	Evaluations CIS	Joignabilité de réseau	Bonnes pratiques de sécurité	Analyse du comportement d'exécution
Amaz Linux 2013.	Pris en charge		Pris en charge	Pris en charge	
Amaz Linux 2012.	Pris en charge		Pris en charge	Pris en charge	
Amaz Linux 2012.	Pris en charge		Pris en charge	Pris en charge	
Ubun 20.04 LTS	Pris en charge		Pris en charge	Pris en charge	
Ubun 18.04 LTS	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Ubun 16.04 LTS	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Ubun 14.04 LTS	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète

Systè d'exp ation pris en charg	Vulnérabi lités et expositio ns courantes	Evaluations CIS	Joignabilité de réseau	Bonnes pratiques de sécurité	Analyse du comportement d'exécution
Debia 10.x, 9.0 - 9.5, 8.0 - 8.7	Pris en charge		Pris en charge	Pris en charge	
RHEL 8.x	Pris en charge		Pris en charge	Pris en charge	
RHEL 7.6 - 7.x	Pris en charge	Pris en charge	Pris en charge	Pris en charge	
RHEL 6.2 - 6.9, 7.2 - 7.5	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Cent(7.6 - 7.X	Pris en charge	Pris en charge	Pris en charge	Pris en charge	

Systè d'exp ation pris en charg	Vulnérabi lités et expositio ns courantes	Evaluations CIS	Joignabilité de réseau	Bonnes pratiques de sécurité	Analyse du comportement d'exécution
Cent(6.2 - 6.9, 7.2 - 7.5	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Obsolète
Wind(	Pris en charge		Pris en charge		
Wind(Serve 2016 Base	Pris en charge	Pris en charge	Pris en charge		Obsolète
Wind(	Pris en charge	Pris en charge	Pris en charge		Obsolète
Wind(Serve	Pris en charge	Pris en charge	Pris en charge		Obsolète
Wind(	Pris en charge	Pris en charge	Pris en charge		Obsolète

Journalisation des appels d'API Amazon Inspector Classic avecAWS CloudTrail

Amazon Inspector Classic est intégré àAWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou unAWSdans Amazon Inspector Classic. CloudTrail capture tous les appels d'API pour Amazon Inspector Classic en tant qu'événements, y compris les appels de la console Amazon Inspector Classic et les appels de code à des opérations d'API Amazon Inspector Classic. Si vous créez un journal d'activité, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon S3, y compris des événements pour Amazon Inspector Classic. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents sur 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 Classic, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur de la demande et la date de la demande, ainsi que d'autres informations.

Pour en savoir plus sur CloudTrail, consultez le AWS CloudTrailGuide de l'utilisateur . Pour obtenir la liste complète des opérations d'API Amazon Inspector Classic, consultezActionsdans leRéférence de l'API Amazon Inspector Classic.

Informations relatives à Amazon Inspector Classic dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Quand une activité a lieu dans Amazon Inspector Classic, celle-ci est enregistrée dans un événement CloudTrail avec d'autres événements CloudTrail avec d'autres événements.AWSévénements de service dansHistorique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour un registre permanent des événements de votreAWScompte, y compris les événements pour Amazon Inspector Classic, créez unsentier. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux vers Amazon S3 bucket. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception des fichiers journaux CloudTrail de plusieurs régions et Réception des fichiers journaux CloudTrail de plusieurs comptes

CloudTrail enregistre toutes les opérations Amazon Inspector Classic, y compris des opérations en lecture seule, telles que`ListAssessmentRunsetDescribeAssessmentTargets`, et des opérations de gestion, telles que`AddAttributesToFindingsetCreateAssessmentTemplate`.

> **Note**
>
> CloudTrail enregistre uniquement les informations de la demande des opérations en lecture seule Amazon Inspector Classic. Les informations de demande et de réponse sont consignées pour toutes les autres opérations Amazon Inspector Classic.

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été effectuée par un autre service AWS

Pour en saConsultez plus, consultez Elément userIdentity CloudTrail.

Présentation des entrées des fichiers journaux Amazon Inspector Classic

Un journal de suivi est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande émise par une source et comprend des informations sur l'action demandée, la date et l'heure de l'action, ainsi que

d'autres paramètres de la demande, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail qui illustre Amazon Inspector Classic.`CreateResourceGroup`fonctionnement :


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
```

```
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

Surveillance d'Amazon Inspector Classic à l'aide d'Amazon CloudWatch

Vous pouvez surveiller Amazon Inspector Classic à l'aide d'AmazonCloudWatch, qui collecte et traite les données brutes en métriques lisibles en temps quasi réel. Par défaut, Amazon Inspector Classic envoie des données métriques par périodes CloudWatch de 5 minutes. Vous pouvez utiliser l'API AWS Management ConsoleAWS CLI, l'API ou une API pour afficher les métriques envoyées à Amazon Inspector ClassicCloudWatch.

Pour plus d'informations sur AmazonCloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

CloudWatchMétriques Amazon Inspector Classic

L'espace de noms Amazon Inspector Classic inclut les métriques suivantes.

`AssessmentTargetARN` métriques :

Métrique	Description
`TotalMatchingAgents`	Nombre d'agents correspondant à cet objectif
`TotalHealthyAgents`	Nombre d'agents sains correspondant à cet objectif
`TotalAssessmentRuns`	Nombre d'exécutions d'évaluation pour cet objectif
`TotalAssessmentRun Findings`	Nombre de résultats pour cet objectif

`AssessmentTemplateARN` métriques :

Métrique	Description
`TotalMatchingAgents`	Nombre d'agents correspondant à ce modèle
`TotalHealthyAgents`	Nombre d'agents sains correspondant à ce modèle

Métrique	Description
`TotalAssessmentRuns`	Nombre d'exécutions d'évaluation pour ce modèle
`TotalAssessmentRunFindings`	Nombre de résultats pour ce modèle

Métriques Aggregate

Métrique	Description
`TotalAssessmentRuns`	Nombre d'exécutions d'évaluation dans ce compte AWS

Configuration d'Amazon Inspector Classic à l'aide deAWS CloudFormation

Pour des informations de référence concernant les ressources Amazon Inspector Classic prises en charge parAWS CloudFormation, consultez les rubriques suivantes :

- `AWS::Inspector::AssessmentTarget`
- `AWS::Inspector::AssessmentTemplate`
- `AWS::Inspector::ResourceGroup`

> **Important**
>
> Pour des listes des ARN des ensembles de règles Amazon Inspector Classic pris en chargeAWSRégions, voirARNS Amazon Inspector Classic pour les packages de règles.

Intégration à AWS Security Hub

AWS Security Hub fournit une vue complète de votre état de sécurité dans AWS et vous permet de vérifier votre environnement par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Security Hub collecte les données de sécurité des comptes et services AWS, et de produits de tierces parties pris en charge. Il vous aide aussi à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité prioritaires.

L'intégration d'Amazon Inspector avec Security Hub vous permet d'envoyer les résultats d'Amazon Inspector à Security Hub. Security Hub peut ensuite inclure ces résultats dans son analyse de votre posture de sécurité.

Table des matières

Comment Amazon Inspector envoie des résultats à Security Hub

Dans Security Hub, les problèmes de sécurité sont suivis en tant que résultats. Certains résultats proviennent de problèmes qui sont détectés par d'autres services AWS ou par des partenaires tiers. Security Hub utilise également un ensemble de règles pour détecter les problèmes de sécurité et générer des résultats.

Security Hub fournit des outils permettant de gérer les résultats provenant de toutes ces sources. Vous pouvez afficher et filtrer les listes de résultats et afficher les informations sur un résultat. Veuillez consulter Viewing findings (Affichage des résultats)dans le Guide de l'utilisateur AWS Security Hub. Vous pouvez également suivre le statut d'une analyse dans un résultat. Consultez Prendre des mesures à la suite des résultats dans le Guide de l'utilisateur AWS Security Hub.

Tous les résultats dans Security Hub utilisent un format JSON standard appelé AWS Security Finding Format (ASFF). Le format ASFF comprend des informations sur la source du problème, les ressources affectées et le statut actuel du résultat. VoirFormat ASFF (AWS Security Finding Format)dans leAWS Security HubGuide de l'utilisateur.

Amazon Inspector est l'un desAWSservices qui envoie des résultats à Security Hub.

Types de résultats envoyés par Amazon Inspector

Amazon Inspector envoie tous les résultats qu'il génère à Security Hub.

Amazon Inspector envoie les résultats à Security Hub dans leAWSFormat ASFF (Security Finding Format). Dans le format ASFF, le champ `Types` fournit le type de résultat. Les résultats d'Amazon Inspector peuvent avoir les valeurs suivantes pour`Types`.

- Vérification du logiciel et de configuration/Vulnérabilité/CVE
- Vérification du logiciel et de configuration/Bonne de sécurité AWS et accessibilité du réseau
- Contrôles logiciels et de configuration/Normes de l'industrie et de la règlementation/Benchmarks de renforcement de l'hôte CIS

Latence pour l'envoi des résultats

Lorsqu'Amazon Inspector crée un résultat, ce dernier est généralement envoyé à Security Hub dans les cinq minutes.

Réessayer lorsque Security Hub n'est pas disponible

Si Security Hub n'est pas disponible, Amazon Inspector essaie à nouveau d'envoyer les résultats jusqu'à ce qu'ils soient reçus.

Mise à jour des résultats existants dans Security Hub

Après avoir envoyé un résultat à Security Hub, Amazon Inspector met à jour ce résultat pour refléter d'autres observations de l'activité de recherche. Cela entraînera moins de résultats Amazon Inspector dans Security Hub que dans Amazon Inspector.

Résultat type d'Amazon Inspector

Amazon Inspector envoie des résultats à Security Hub dans leAWSFormat ASFF (Security Finding Format).

Voici un exemple de résultat type d'Amazon Inspector.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
reachable from the internet. You can install the Inspector agent on this instance
and re-run the assessment to check for any process listening on this port. The
instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
```

```
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

Activation et configuration de l'intégration

Pour utiliser l'intégration avec Security Hub, vous devez activer Security Hub. Pour plus d'informations sur la façon d'activer Security Hub, veuillez consulter Configuration de Security Hub dans le Guide de l'utilisateur AWS Security Hub.

Lorsque vous activez à la fois Amazon Inspector et Security Hub, l'intégration est activée automatiquement. Amazon Inspector commence à envoyer les résultats à Security Hub.

Comment arrêter l'envoi des résultats

Pour arrêter l'envoi des résultats à Security Hub, vous pouvez utiliser la console Security Hub ou l'API.

VoirDésactivation et activation du flux de résultats d'une intégration (console)ouDésactivation du flux de résultats d'une intégration (API Security Hub, AWS CLI)dans leAWS Security HubGuide de l'utilisateur.

ARN Amazon Inspector Classic

Chaque type de ressource et package de règles est associé à un Amazon Resource Name (ARN) unique.

Table des matières

Ressources ARN pour Amazon Inspector Classic

Dans Amazon Inspector Classic, les ressources principales sont des groupes de ressources, des objectifs d'évaluation, des modèles d'exécutions d'évaluation et des résultats. Ces ressources ont des noms ARN (Amazon Resource Name) uniques qui leur sont associés, comme cela est illustré dans le tableau suivant.

Type de ressource	Format ARN
Groupe de ressources	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:resourcegroup/` *`ID`*
Objectif d'évaluation	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:target/`*`ID`*
Modèle d'évaluation	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:target/`*`ID`*`:template:` *`ID`*
Exécution d'évaluation	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:target/`*`ID`*`/template/` *`ID`*`/run/`*`ID`*
Résultat	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:target/`*`ID`*`/template/` *`ID`*`/run/`*`ID`*`/finding/` *`ID`*

ARNS Amazon Inspector Classic pour les packages de règles

Les tableaux suivants affichent tous les ARN pour les ensembles de règles Amazon Inspector Classic de toutes les régions prises en charge.

Rubriques

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Stockholm)

- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

USA Est (Ohio)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85`
Évaluation de la configuration de la sécurité du système d'exploitation CIS	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh`
Joignabilité de réseau	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30`
Bonnes pratiques de sécurité	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX`

USA Est (Virginie du Nord)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7`

Nom du package de règles	ARN
Évaluation de la configuration de la sécurité du système d'exploitation CIS	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8
Joignabilité de réseau	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd
Bonnes pratiques de sécurité	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q

USA Ouest (Californie du Nord)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa
Évaluation de la configuration de la sécurité du système d'exploitation CIS	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX
Joignabilité de réseau	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF

Nom du package de règles	ARN
Bonnes pratiques de sécurité	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-byoQRFYm`

USA Ouest (Oregon)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p`
Évaluation de la configuration de la sécurité du système d'exploitation CIS	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc`
Joignabilité de réseau	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl`
Bonnes pratiques de sécurité	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ`

Asie-Pacifique (Mumbai)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9dO`
Évaluation de la configuration de la sécurité du système d'exploitation CIS	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m`
Joignabilité de réseau	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1`
Bonnes pratiques de sécurité	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj`

Asie-Pacifique (Séoul)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	`arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc`
Évaluation de la configuration de la sécurité du système d'exploitation CIS	`arn:aws:inspector:ap-northeast-2:526`

Nom du package de règles	ARN
	946625049:rulespac kage/0-T9srhg1z
Joignabilité de réseau	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-s3OmLzhL
Bonnes pratiques de sécurité	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n

Asie-Pacifique (Sydney)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-D5TGAxiR
Évaluation de la configuration de la sécurité du système d'exploit ation CIS	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-Vkd2Vxjq
Joignabilité de réseau	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-FLcuV4Gz
Bonnes pratiques de sécurité	arn:aws:inspector: ap-southeast-2:454

Nom du package de règles	ARN
	640832652:rulespac kage/0-asL6HRgN

Asie-Pacifique (Tokyo)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-gHP9oWNT
Évaluation de la configuration de la sécurité du système d'exploit ation CIS	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-7WNjqgGu
Joignabilité de réseau	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-YI95DVd7
Bonnes pratiques de sécurité	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-bBUQnxMq

Europe (Francfort)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	arn:aws:inspector: eu-central-1:53750

Nom du package de règles	ARN
	3971621:rulespackage/0-wNqHa8M9
Évaluation de la configuration de la sécurité du système d'exploitation CIS	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-nZrAVuv8
Joignabilité de réseau	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
Bonnes pratiques de sécurité	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

Europe (Irlande)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
Évaluation de la configuration de la sécurité du système d'exploitation CIS	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
Joignabilité de réseau	arn:aws:inspector:eu-west-1:35755712

Nom du package de règles	ARN
	9151:rulespackage/0-SPzU33xe
Bonnes pratiques de sécurité	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SnojL3Z6

Europe (Londres)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
Évaluation de la configuration de la sécurité du système d'exploitation CIS	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
Joignabilité de réseau	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
Bonnes pratiques de sécurité	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

Europe (Stockholm)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd`
Évaluation de la configuration de la sécurité du système d'exploitation CIS	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f`
Joignabilité de réseau	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu`
Bonnes pratiques de sécurité	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf`

AWS GovCloud (US-East)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	`arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFu0b`
Évaluation de la configuration de la sécurité du système d'exploitation CIS	`arn:aws-us-gov:inspector:us-gov-east`

Nom du package de règles	ARN
	-1:206278770380:rulespackage/0-pTLCdIww
Bonnes pratiques de sécurité	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

AWS GovCloud (US-West)

Nom du package de règles	ARN
Vulnérabilités et expositions courantes	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
Évaluation de la configuration de la sécurité du système d'exploitation CIS	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc
Bonnes pratiques de sécurité	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G

Historique du document

Le tableau suivant décrit l'historique des publications de la documentation d'Amazon Inspector Classic après mai 2018.

Modification	Description	Date
Meilleures pratiques de sécurité mises à jour pour les mots de passe	Les exigences relatives aux meilleures pratiques de sécurité d'Amazon Inspector Classic concernant la longueur et la complexité des mots de passe des instances EC2 ont été mises à jour. Voir Configurer la longueur minimale du mot de passe et Configurer la complexité du mot de passe	8 mars 2021
Ajout du support pour les nouvelles versions du système d'exploitation	Amazon Inspector Classic prend désormais en charge les versions des systèmes d'exploitation suivantes : Ubuntu 20.4 LTS, Debian 10.x, RHEL 8.x et Windows Server 2019 Base.	15 octobre 2020
Informations de sécurité consolidées dans un nouveau chapitre sur la sécurité	Les informations de sécurité pour Amazon Inspector Classic, y compris les informations sur la gestion des identités et des accès, sont regroupées dans un chapitre sur la sécurité. Consultez la section Sécurité dans Amazon Inspector Classic.	7 avril 2020

Documentation mise à jour pour supprimer la prise en charge du package de règles d'analyse du comportement d'exécution.	Plusieurs rubriques ont été mises à jour pour supprimer des informations sur le package de règles d'analyse du comportement d'exécution qui n'est plus pris en charge.	5 septembre 2019
Support du système d'exploitation ajouté	Ajout de la prise en charge d'Amazon Inspector Classic pour CentOS 7.6. Pour plus d'informations, consultez les sections Systèmes d'exploitation et régions pris en charge par Amazon Inspector Classic et Disponibilité des packages de règles sur les systèmes d'exploitation pris en charge.	3 décembre 2018
Nouveau contenu	Ajout du package de règles d'accessibilité réseau Amazon Inspector Classic, qui permet aux utilisateurs d'exécuter des évaluations sans agent afin d'analyser la configuration du réseau pour détecter les vulnérabilités de sécurité. Pour plus d'informations, consultez la Network Reachability (Joignabilité de réseau).	9 novembre 2018

Support du système d'exploitation ajouté	Ajout de la prise en charge d'Amazon Inspector Classic pour RHEL 7.6. Pour plus d'informations, consultez les sections Systèmes d'exploitation et régions pris en charge par Amazon Inspector Classic et Disponibilité des packages de règles sur les systèmes d'exploitation pris en charge.	30 octobre 2018
Support du système d'exploitation ajouté	Prise en charge supplémentaire de divers systèmes d'exploitation pour le package de règles des évaluations CIS. Pour plus d'informations, consultez Références Center for Internet Security (CIS) et Disponibilité des packages de règles sur les systèmes d'exploitation pris en charge.	13 août 2018
Prise en charge de régions supplémentaires	Ajout de support de région pour `AWS GovCloud (US)`.	13 juin 2018

Le tableau suivant décrit l'historique des publications de la documentation d'Amazon Inspector Classic avant juin 2018.

Modification	Description	Date
Nouveau contenu	Ajout de la possibilité de cibler toutes les instances Amazon EC2 d'un compte. Pour plus d'informations, consultez Cibles d'évaluation Amazon Inspector Classic.	24 mai 2018

Modification	Description	Date
Ajout de la prise en charge de systèmes d'exploitation	Ajout du support Amazon Inspector Classic pour Amazon Linux 2018.03 et Ubuntu 18.04.	15 mai 2018
Nouveau contenu	Ajout de la possibilité de configurer des évaluations Amazon Inspector Classic récurrentes.	30 avril 2018
Nouveau contenu	Ajout de la possibilité d'install er un agent Amazon Inspector Classic via la console.	30 avril 2018
Ajout de la prise en charge de systèmes d'exploitation	Ajout de la prise en charge d'Amazon Inspector Classic pour Amazon Linux 2.	13 mars 2018
Ajout de la prise en charge de systèmes d'exploitation	Ajout du support d'évaluation Amazon Inspector Classic pour Windows Server 2016 Base.	20 février 2018
Prise en charge de régions supplémentaires	Ajout du support Amazon Inspector Classic pour la US `East (Ohio)` région.	7 février 2018
Nouveau contenu	Les évaluations Amazon Inspector Classic peuvent désormais être exécutées lorsque le module du noyau n'est pas disponible.	11 janvier 2018
Prise en charge de régions supplémentaires	Ajout du support Amazon Inspector Classic pour la EU `(Frankfurt)` région.	19 décembre 2017

Modification	Description	Date
Nouveau contenu	Ajout de la possibilité de vérifier l'état de santé des agents Amazon Inspector Classic à l'aide de l'API et de la console Amazon Inspector Classic.	15 décembre 2017
Nouveau contenu	Ajout des fonctions suivantes : • Utilisation du rôle lié à un service • L'AMI d'agent Amazon Inspector Classic est disponible AWS sur le Marketplace • AWS CloudFormation Modèles Amazon Inspector Classic	5 décembre 2017
Ajout de la prise en charge de systèmes d'exploitation	Ajout du support d'évaluation Amazon Inspector Classic pour CentOS 7.4.	9 novembre 2017
Ajout de la prise en charge de systèmes d'exploitation	Ajout du support d'évaluation Amazon Inspector Classic pour Amazon Linux 2017.09.	11 octobre 2017
Ajout de la prise en charge de systèmes d'exploitation	Ajout du support d'évaluation Amazon Inspector Classic pour RHEL 7.4.	20 février 2018
Ajout de l'éligibilité HIPAA	Amazon Inspector Classic est désormais éligible à la loi HIPAA.	31 juillet 2017

Modification	Description	Date
Nouveau contenu	Ajout de la possibilité de déclencher automatiquement l'évaluation de sécurité d'Amazon Inspector Classic avec Amazon CloudWatch Events.	27 juillet 2017
Prise en charge de régions supplémentaires	Ajout du support Amazon Inspector Classic pour la US `West (N. California)` région.	6 juin 2018
Ajout de la prise en charge de systèmes d'exploitation	Ajout du support d'évaluation Amazon Inspector Classic pour RHEL 6.2-6.9, RHEL 7.2-7.3, CentOS 6.9 et CentOS 7.2-7.3.	23 mai 2017
Ajout de la prise en charge de systèmes d'exploitation	Ajout du support d'évaluation Amazon Inspector Classic pour Amazon Linux 2017.03.	25 avril 2017
Nouveau contenu et ajout de la prise en charge de systèmes d'exploitation	Ajouté: • Support d'Amazon Inspector Classic pour Ubuntu 16.04. • Disponibilité du plan Lambda pour automatis er les opérations Amazon Inspector Classic.	5 janvier 2017
Nouvelle prise en charge de systèmes d'exploitation	Ajout de la prise en charge d'Amazon Inspector Classic pour Microsoft Windows.	26 août 2016

Modification	Description	Date
Prise en charge de régions supplémentaires	Ajout du support Amazon Inspector Classic pour la `Asia Pacific (Seoul)` région.	26 août 2016
Prise en charge de régions supplémentaires	Ajout du support Amazon Inspector Classic pour la `Asia Pacific (Mumbai)` région.	25 avril 2016
Prise en charge de régions supplémentaires	Ajout du support Amazon Inspector Classic pour la `Asia Pacific (Sydney)` région.	25 avril 2016
Lancement de service	Lancement du service Amazon Inspector Classic.	7 octobre 2015

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.