Benutzerhandbuch

Amazon Inspector

Amazon Inspector: Benutzerhandbuch

Table of Contents

Was ist Amazon Inspector?

Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre AWS Workloads kontinuierlich auf Softwareschwachstellen und unbeabsichtigte Netzwerkbedrohungen überprüft. Amazon Inspector erkennt und scannt automatisch laufende Amazon EC2 EC2-Instances, Container-Images in Amazon Elastic Container Registry (Amazon ECR) und AWS Lambda Funktionen auf bekannte Softwareschwachstellen und unbeabsichtigte Netzwerkgefährdung.

Amazon Inspector erstellt einen Befund, wenn es eine Softwareschwachstelle oder ein Problem mit der Netzwerkkonfiguration entdeckt. Ein Befund beschreibt die Sicherheitsanfälligkeit, identifiziert die betroffene Ressource, bewertet den Schweregrad der Sicherheitsanfälligkeit und gibt Hinweise zur Behebung. Sie können die Ergebnisse mit der Amazon Inspector Inspector-Konsole analysieren oder Ihre Ergebnisse über andere anzeigen und verarbeiten AWS-Services. Weitere Informationen finden Sie unter Die Ergebnisse in Amazon Inspector verstehen.

Themen

Funktionen von Amazon Inspector

Zentrales Verwalten mehrerer Amazon Inspector Inspector-Konten

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie Ihre Umgebung mithilfe von AWS Organizations über ein einziges Konto zentral verwalten. Mit diesem Ansatz können Sie ein Konto als delegiertes Administratorkonto für Amazon Inspector festlegen.

Amazon Inspector kann mit einem einzigen Klick für Ihr gesamtes Unternehmen aktiviert werden. Darüber hinaus können Sie die Aktivierung des Dienstes für future Mitglieder automatisieren, wann immer diese Ihrer Organisation beitreten. Das delegierte Administratorkonto von Amazon Inspector kann Ergebnisdaten und bestimmte Einstellungen für Mitglieder der Organisation verwalten. Dazu gehören die Anzeige aggregierter Ergebnisdetails für alle Mitgliedskonten, die Aktivierung oder Deaktivierung von Scans für Mitgliedskonten und die Überprüfung gescannter Ressourcen innerhalb der Organisation. AWS

Scannen Sie Ihre Umgebung kontinuierlich auf Sicherheitslücken und Netzwerkgefährdungen

Mit Amazon Inspector müssen Sie Bewertungsscans nicht manuell planen oder konfigurieren. Amazon Inspector erkennt automatisch Ihre in Frage kommenden Ressourcen und beginnt mit dem Scannen. Amazon Inspector bewertet Ihre Umgebung weiterhin während des gesamten Lebenszyklus Ihrer Ressourcen, indem es automatisch Ressourcen als Reaktion auf Änderungen, die zu einer neuen Sicherheitslücke führen könnten, erneut scannt, z. B.: Installation eines neuen Pakets in einer EC2-Instance, Installation eines Patches und wenn neue Common Vulnerabilities and Exposures (CVE), die sich auf die Ressource auswirken, veröffentlicht wird. Im Gegensatz zu herkömmlicher Sicherheitsscan-Software hat Amazon Inspector nur minimale Auswirkungen auf die Leistung Ihrer Flotte.

Wenn Sicherheitslücken oder offene Netzwerkpfade identifiziert werden, erstellt Amazon Inspector ein Ergebnis, das Sie untersuchen können. Das Ergebnis umfasst umfassende Informationen über die Sicherheitsanfälligkeit, die betroffene Ressource und Empfehlungen zur Behebung. Wenn Sie ein Ergebnis angemessen korrigieren, erkennt Amazon Inspector die Behebung automatisch und schließt das Ergebnis.

Beurteilen Sie Sicherheitslücken genau mit dem Amazon Inspector Risk Score

Amazon Inspector sammelt mithilfe von Scans Informationen über Ihre Umgebung und bietet Schweregrade, die speziell auf Ihre Umgebung zugeschnitten sind. Amazon Inspector untersucht die Sicherheitsmetriken, die den Basiswert der National Vulnerability Database (NVD) für eine Sicherheitslücke bilden, und passt sie an Ihre Computerumgebung an. Beispielsweise kann der Service den Amazon Inspector-Score eines Ergebnisses für eine Amazon EC2 EC2-Instance senken, wenn die Sicherheitsanfälligkeit über das Netzwerk ausgenutzt werden kann, aber von der Instance aus kein offener Netzwerkpfad zum Internet verfügbar ist. Diese Bewertung ist im CVSS-Format und ist eine Modifikation der von NVD bereitgestellten Basisbewertung des Common Vulnerability Scoring System (CVSS).

Identifizieren Sie wichtige Ergebnisse mit dem Amazon Inspector-Dashboard

Das Amazon Inspector-Dashboard bietet einen umfassenden Überblick über die Ergebnisse aus Ihrer gesamten Umgebung. Über das Dashboard können Sie auf die detaillierten Details eines Ergebnisses zugreifen. Das Dashboard enthält übersichtliche Informationen zur Scanabdeckung in Ihrer Umgebung, zu Ihren wichtigsten Ergebnissen und zu den Ressourcen, bei denen die meisten Ergebnisse vorliegen. Das Fenster zur risikobasierten Behebung im Amazon Inspector-Dashboard zeigt die Ergebnisse, die sich auf die größte Anzahl von Instances und Images auswirken. Dieses Fenster erleichtert es, die Ergebnisse mit den größten Auswirkungen auf Ihre Umgebung zu identifizieren, die Einzelheiten der Ergebnisse zu überprüfen und Lösungsvorschläge zu überprüfen.

Verwalten Sie Ihre Ergebnisse mithilfe anpassbarer Ansichten

Zusätzlich zum Dashboard bietet die Amazon Inspector Inspector-Konsole eine Ergebnisansicht. Diese Seite listet alle Ergebnisse für Ihre Umgebung auf und enthält Einzelheiten zu den einzelnen Ergebnissen. Sie können die Ergebnisse nach Kategorie oder Schwachstellentyp gruppiert anzeigen. In jeder Ansicht können Sie Ihre Ergebnisse mithilfe von Filtern weiter anpassen. Sie können Filter auch verwenden, um Unterdrückungsregeln zu erstellen, die unerwünschte Ergebnisse in Ihren Ansichten verbergen.

Sie können Filter und Unterdrückungsregeln verwenden, um Ergebnisberichte zu erstellen, in denen alle Ergebnisse oder eine benutzerdefinierte Auswahl von Ergebnissen angezeigt werden. Berichte können im CSV- oder JSON-Format generiert werden.

Überwachen und verarbeiten Sie Ergebnisse mit anderen Diensten und Systemen

Um die Integration mit anderen Diensten und Systemen zu unterstützen, veröffentlicht Amazon Inspector die Ergebnisse in Form von Befundereignissen auf Amazon EventBridge. EventBridge ist ein serverloser Eventbus-Service, der Ergebnisdaten an Ziele wie AWS Lambda Funktionen und Amazon Simple Notification Service (Amazon SNS) -Themen weiterleiten kann. Damit EventBridge können Sie die Ergebnisse im Rahmen Ihrer bestehenden Sicherheits- und Compliance-Workflows nahezu in Echtzeit überwachen und verarbeiten.

Wenn Sie aktiviert haben AWS Security Hub, veröffentlicht Amazon Inspector die Ergebnisse auch im Security Hub. Security Hub ist ein Service, der Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in Ihrer gesamten AWS Umgebung bietet und Ihnen hilft, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Mit Security Hub können Sie Ihre Ergebnisse im Rahmen einer umfassenderen Analyse der Sicherheitslage Ihres Unternehmens in einfacher überwachen und verarbeiten AWS.

Zugreifen auf Amazon Inspector

Amazon Inspector ist in den meisten Fällen verfügbar AWS-Regionen. Eine Liste der Regionen, in denen Amazon Inspector derzeit verfügbar ist, finden Sie unter Amazon Inspector Inspector-Endpunkte und Kontingente in der Amazon Web Services General Reference. Weitere Informationen AWS-Regionen dazu finden Sie unter Managing AWS-Regionen in der Amazon Web Services General Reference. In jeder Region können Sie auf folgende Weise mit Amazon Inspector arbeiten.

AWS Management-Konsole

Die AWS Management Console ist eine browserbasierte Oberfläche, mit der Sie AWS Ressourcen erstellen und verwalten können. Als Teil dieser Konsole bietet die Amazon Inspector Inspector-Konsole Zugriff auf Ihr Amazon Inspector Inspector-Konto und Ihre Ressourcen. Sie können Amazon Inspector Inspector-Aufgaben von der Amazon Inspector Inspector-Konsole aus ausführen.

AWS Befehlszeilentools

Mit AWS Befehlszeilentools können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um Amazon Inspector Inspector-Aufgaben auszuführen. Die Verwendung der Befehlszeile kann schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeilen-Tools können auch beim Erstellen von Skripts für -Aufgaben hilfreich sein.

AWS stellt zwei Gruppen von Befehlszeilentools bereit: das AWS Command Line Interface (AWS CLI) und das AWS Tools for PowerShell. Informationen zur Installation und Verwendung von finden Sie im AWS Command Line Interface User Guide. AWS CLI Informationen zur Installation und Verwendung der Tools für PowerShell finden Sie im AWS Tools for PowerShell Benutzerhandbuch.

AWS SDKs

AWS stellt SDKs bereit, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen, darunter Java, Go, Python, C++ und .NET. Die SDKs bieten bequemen, programmatischen Zugriff auf Amazon Inspector und andere. AWS-Services Sie übernehmen auch Aufgaben wie das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen. Informationen zur Installation und Verwendung der AWS SDKs finden Sie unter Tools to Build On. AWS

Amazon Inspector REST-API

Die Amazon Inspector REST-API bietet Ihnen umfassenden, programmatischen Zugriff auf Ihr Amazon Inspector Inspector-Konto und Ihre Ressourcen. Mit dieser API können Sie HTTPS-Anfragen direkt an Amazon Inspector senden. Im Gegensatz zu den AWS Befehlszeilentools und SDKs erfordert die Verwendung dieser API jedoch, dass Ihre Anwendung Details auf niedriger Ebene verarbeitet, wie z. B. die Generierung eines Hashs zum Signieren einer Anfrage.

Erste Schritte mit Amazon Inspector

Dieses Tutorial bietet eine praktische Einführung in Amazon Inspector.

Schritt 1 umfasst die Aktivierung von Amazon Inspector-Scans für ein eigenständiges Konto oder als delegierter Amazon Inspector-Administrator AWS Organizations in einer Umgebung mit mehreren Konten.

Schritt 2 behandelt das Verständnis der Ergebnisse von Amazon Inspector in der Konsole.

> **Note**
>
> In diesem Tutorial erledigen Sie Aufgaben in Ihrer aktuellen Version AWS-Region. Um Amazon Inspector in anderen Regionen einzurichten, müssen Sie diese Schritte in jeder dieser Regionen ausführen.

Themen

Bevor Sie beginnen

Amazon Inspector ist ein Schwachstellen-Management-Service, der Ihre Amazon EC2 EC2-Instances, Amazon ECR-Container-Images und AWS Lambda Funktionen kontinuierlich auf Softwareschwachstellen und unbeabsichtigte Netzwerkgefährdung überprüft.

Beachten Sie Folgendes, bevor Sie Amazon Inspector aktivieren:

- Amazon Inspector ist ein regionaler Service, und Daten werden dort gespeichert AWS-Region , wo Sie den Service nutzen. Alle Konfigurationsverfahren, die Sie in diesem Tutorial durchführen, müssen für jedes Verfahren wiederholt werden AWS-Region , das Sie mit Amazon Inspector überwachen möchten.
- Amazon Inspector bietet Ihnen die Flexibilität, Amazon EC2 EC2-Instance, Amazon ECR-Container-Image und AWS Lambda Funktionsscanning zu aktivieren. Sie können die Scanarten auf

der Kontoverwaltungsseite in der Amazon Inspector Inspector-Konsole oder mithilfe der Amazon Inspector Inspector-APIs verwalten.

- Amazon Inspector kann Common Vulnerabilities and Exposures (CVE) -Daten (Common Vulnerabilities and Exposures) für Ihre EC2-Instances nur bereitstellen, wenn der Amazon EC2 Systems Manager (SSM) -Agent installiert und aktiviert ist. Dieser Agent ist auf vielen EC2-Instances vorinstalliert, Sie müssen ihn jedoch möglicherweise manuell aktivieren. Unabhängig vom Status des SSM-Agenten werden alle Ihre EC2-Instances auf Netzwerkprobleme überprüft. Weitere Informationen zur Konfiguration von Scans für Amazon EC2 finden Sie unterAmazon EC2 EC2-Instances scannen. Amazon ECR und AWS Lambda Funktionsscanning erfordern keinen Agenten.
- Eine IAM-Benutzeridentität mit Administratorrechten AWS-Konto kann Amazon Inspector aktivieren. Aus Datenschutzgründen empfehlen wir Ihnen, Ihre Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. Auf diese Weise erhält jeder Benutzer nur die Berechtigungen, die für die Verwaltung von Amazon Inspector erforderlich sind. Informationen zu den für die Aktivierung von Amazon Inspector erforderlichen Berechtigungen finden Sie unterAWS verwaltete Richtlinie: AmazonInspector2FullAccess.
- Wenn Sie Amazon Inspector zum ersten Mal in einer beliebigen Region aktivieren, wird für Ihr Konto weltweit eine dienstbezogene Rolle mit dem Namen `AWSServiceRoleForAmazonInspector2` erstellt. Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es Amazon Inspector ermöglichen, Softwarepaketdetails zu sammeln und Amazon VPC-Konfigurationen zu analysieren, um Sicherheitslücken zu ermitteln. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Inspector. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden serviceverknüpfter Rollen.

Schritt 1: Amazon Inspector aktivieren

Der erste Schritt zur Verwendung von Amazon Inspector besteht darin, ihn für Sie zu aktivieren AWS-Konto. Nachdem Sie einen beliebigen Amazon Inspector-Scantyp aktiviert haben, beginnt Amazon Inspector sofort mit der Erkennung und dem Scannen aller infrage kommenden Ressourcen.

Wenn Sie Amazon Inspector für mehrere Konten innerhalb Ihrer Organisation über ein zentrales Administratorkonto verwalten möchten, müssen Sie einen delegierten Administrator für Amazon Inspector zuweisen. Wählen Sie eine der folgenden Optionen, um zu erfahren, wie Sie Amazon Inspector für Ihre Umgebung aktivieren.

Standalone account environment

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie Get Started.
3. Wählen Sie Amazon Inspector aktivieren.

Wenn Sie Amazon Inspector in einem eigenständigen Konto aktivieren, sind alle Scantypen standardmäßig aktiviert. Sie können aktivierte Scantypen über die Kontoverwaltungsseite in der Amazon Inspector Inspector-Konsole oder mithilfe der Amazon Inspector Inspector-APIs verwalten. Nach der Aktivierung erkennt Amazon Inspector automatisch alle geeigneten Ressourcen und beginnt mit dem Scannen. Überprüfen Sie die folgenden Informationen zum Scantyp, um zu erfahren, welche Ressourcen standardmäßig in Frage kommen:

Amazon EC2-Scannen

Um Common Vulnerabilities and Exposures (CVE) -Daten für Ihre EC2-Instance bereitzustellen, benötigt Amazon Inspector, dass der AWS Systems Manager (SSM) -Agent installiert und aktiviert ist. Dieser Agent ist auf vielen EC2-Instances vorinstalliert, Sie müssen ihn jedoch möglicherweise manuell aktivieren. Unabhängig vom Status des SSM-Agenten werden alle Ihre EC2-Instances auf Netzwerkprobleme überprüft. Weitere Informationen zur Konfiguration von Scans für Amazon EC2 finden Sie unterScannen von Amazon EC2 EC2-Instances mit Amazon Inspector.

Amazon ECR-Scannen

Wenn Sie das Amazon ECR-Scannen aktivieren, konvertiert Amazon Inspector alle Container-Repositorys in Ihrer privaten Registrierung, die für das standardmäßige Standard-Scannen von Amazon ECR konfiguriert sind, in das erweiterte Scannen mit kontinuierlichem Scannen. Sie können diese Einstellung auch optional so konfigurieren, dass nur bei Push gescannt wird oder dass ausgewählte Repositorys anhand von Einschlussregeln gescannt werden. Alle Bilder, die innerhalb der letzten 30 Tage übertragen wurden, sind für das Scannen auf Lebenszeit geplant. Diese Amazon ECR-Scaneinstellung kann jederzeit geändert werden. Weitere Informationen zur Konfiguration von Scans für Amazon ECR finden Sie unterScannen von Amazon ECR-Container-Bildern mit Amazon Inspector.

AWS Lambda Funktion Scannen

Wenn Sie den AWS Lambda Funktionsscan aktivieren, erkennt Amazon Inspector die Lambda-Funktionen in Ihrem Konto und beginnt sofort damit, sie auf Sicherheitslücken zu scannen. Amazon Inspector scannt neue Lambda-Funktionen und -Layer, wenn sie bereitgestellt werden, und scannt sie erneut, wenn sie aktualisiert werden oder wenn neue Common Vulnerabilities and Exposures (CVEs) veröffentlicht werden. Amazon Inspector bietet zwei verschiedene Stufen des Lambda-Funktionsscannens. Wenn Sie Amazon Inspector zum ersten Mal aktivieren, ist standardmäßig der Lambda-Standardscan aktiviert, der Paketabhängigkeiten in Ihren Funktionen scannt. Sie können zusätzlich das Lambda-Code-Scanning aktivieren, um den Entwicklercode in Ihren Funktionen auf Code-Schwachstellen zu scannen. Weitere Hinweise zur Konfiguration des Lambda-Funktionsscannens finden Sie unterAWS Lambda Scanfunktionen mit Amazon Inspector.

Multi-account environment

> **Important**
>
> Um diese Schritte ausführen zu können, müssen Sie derselben Organisation angehören wie alle Konten, die Sie verwalten möchten, und Zugriff auf das AWS Organizations Verwaltungskonto haben, um innerhalb Ihrer Organisation einen Administrator für Amazon Inspector zu delegieren. Für die Delegierung eines Administrators sind möglicherweise zusätzliche Berechtigungen erforderlich. Weitere Informationen finden Sie unter Erforderliche Berechtigungen zum designieren eines delegierten Administrators.
>
> > **Note**
> >
> > Um Amazon Inspector programmatisch für mehrere Konten in mehreren Regionen zu aktivieren, können Sie ein von Amazon Inspector entwickeltes Shell-Skript verwenden. Weitere Informationen zur Verwendung dieses Skripts finden Sie unter inspector2 - on. enablement-with-cli GitHub

Delegieren eines Administrators für Amazon Inspector

1. Melden Sie sich beim AWS Organizations Verwaltungskonto an.

2. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
3. Geben Sie im Bereich Delegierter Administrator die zwölfstellige ID desjenigen ein AWS-Konto , den Sie als delegierten Amazon Inspector-Administrator für die Organisation festlegen möchten. Wählen Sie dann Delegieren. Wählen Sie dann im Bestätigungsfenster erneut Delegieren aus.

> **Note**
>
> Amazon Inspector wird für Ihr Konto aktiviert, wenn Sie einen Administrator delegieren.

Mitgliedskonten hinzufügen

Als delegierter Administrator können Sie das Scannen für jedes Mitglied aktivieren, das dem Verwaltungskonto der Organizations zugeordnet ist. Dieser Workflow aktiviert alle Scanarten für alle Mitgliedskonten. Mitglieder können Amazon Inspector jedoch auch für ihre eigenen Konten aktivieren, oder Scans für einen Service können vom delegierten Administrator selektiv aktiviert werden. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

1. Melden Sie sich beim delegierten Administratorkonto an.
2. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
3. Wählen Sie im Navigationsbereich Account Management aus. In der Tabelle Konten werden alle Mitgliedskonten angezeigt, die dem Verwaltungskonto der Organizations zugeordnet sind.
4. Auf der Seite Kontoverwaltung können Sie im oberen Banner die Option Scannen für alle Konten aktivieren auswählen, um EC2-Instances, ECR-Container-Images und die AWS Lambda Funktion Scannen für alle Konten in Ihrer Organisation zu aktivieren. Alternativ können Sie die Konten, die Sie als Mitglieder hinzufügen möchten, auswählen, indem Sie sie in der Tabelle Konten auswählen. Wählen Sie dann im Menü Aktivieren die Option Alle Scans aus.
5. (Optional) Aktivieren Sie die Funktion Inspector automatisch für neue Mitgliedskonten aktivieren und wählen Sie die zu berücksichtigenden Scantypen aus, um diese Scans für alle neuen Mitgliedskonten zu aktivieren, die Ihrer Organisation hinzugefügt werden.

Amazon Inspector bietet derzeit Scans für EC2-Instances, ECR-Container-Images und AWS Lambda Funktionen. Nachdem Sie Amazon Inspector aktiviert haben, werden automatisch alle infrage kommenden Ressourcen erkannt und gescannt. Überprüfen Sie die folgenden Informationen zum Scantyp, um zu erfahren, welche Ressourcen standardmäßig in Frage kommen:

Amazon EC2-Scannen

Um CVE-Schwachstellendaten für Ihre EC2-Instances bereitzustellen, benötigt Amazon Inspector, dass der AWS Systems Manager (SSM) -Agent installiert und aktiviert ist. Dieser Agent ist auf vielen EC2-Instances vorinstalliert, Sie müssen ihn jedoch möglicherweise manuell aktivieren. Unabhängig vom Status des SSM-Agenten werden alle Ihre EC2-Instances auf Netzwerkprobleme überprüft. Weitere Informationen zur Konfiguration von Scans für Amazon EC2 finden Sie unterScannen von Amazon EC2 EC2-Instances mit Amazon Inspector.

Amazon ECR-Scannen

Wenn Sie das Amazon ECR-Scannen aktivieren, konvertiert Amazon Inspector alle Container-Repositorys in Ihrer privaten Registrierung, die für das standardmäßige Standard-Scannen von Amazon ECR konfiguriert sind, in das erweiterte Scannen mit kontinuierlichem Scannen. Sie können diese Einstellung auch optional so konfigurieren, dass nur bei Push gescannt wird oder dass ausgewählte Repositorys anhand von Einschlussregeln gescannt werden. Für alle Bilder, die innerhalb der letzten 30 Tage übertragen wurden, ist das Scannen auf Lebenszeit geplant. Diese Amazon ECR-Scaneinstellung kann vom delegierten Administrator jederzeit geändert werden. Weitere Informationen zur Konfiguration von Scans für Amazon ECR finden Sie unterScannen von Amazon ECR-Container-Bildern mit Amazon Inspector.

AWS Lambda Funktion Scannen

Wenn Sie den AWS Lambda Funktionsscan aktivieren, erkennt Amazon Inspector die Lambda-Funktionen in Ihrem Konto und beginnt sofort damit, sie auf Sicherheitslücken zu scannen. Amazon Inspector scannt neue Lambda-Funktionen und -Layer, wenn sie bereitgestellt werden, und scannt sie erneut, wenn sie aktualisiert werden oder wenn neue Common Vulnerabilities and Exposures (CVEs) veröffentlicht werden. Weitere Hinweise zur Konfiguration des Lambda-Funktionsscannens finden Sie unterAWS Lambda Scanfunktionen mit Amazon Inspector.

Schritt 2: Ergebnisse von Amazon Inspector anzeigen

Sie können die Ergebnisse für Ihre Umgebung in der Amazon Inspector Inspector-Konsole oder über die API anzeigen. Alle Ergebnisse werden auch an Amazon weitergeleitet EventBridge und AWS Security Hub (falls aktiviert). Darüber hinaus werden die Ergebnisse von Container-Images an Amazon ECR übertragen.

Die Amazon Inspector Inspector-Konsole bietet verschiedene Anzeigeformate für Ihre Ergebnisse. Das Amazon Inspector-Dashboard bietet Ihnen einen allgemeinen Überblick über die Risiken für Ihre Umgebung, während Sie in der Tabelle Ergebnisse die Details eines bestimmten Ergebnisses einsehen können.

In diesem Schritt untersuchen Sie anhand der Tabelle Ergebnisse und des Dashboards Ergebnisse die Details eines Ergebnisses. Informationen zum Amazon Inspector-Dashboard finden Sie unterDas Dashboard verstehen.

So zeigen Sie Details zu den Ergebnissen für Ihre Umgebung in der Amazon Inspector Inspector-Konsole an:

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Dashboard aus. Sie können einen der Links im Dashboard auswählen, um zu einer Seite in der Amazon Inspector Inspector-Konsole mit weiteren Details zu diesem Artikel zu gelangen.
3. Wählen Sie im Navigationsbereich Findings aus.
4. Standardmäßig wird die Registerkarte Alle Ergebnisse angezeigt, auf der alle Ergebnisse der EC2-Instance, des ECR-Container-Images und der AWS Lambda Funktionen für Ihre Umgebung angezeigt werden.
5. Wählen Sie in der Ergebnisliste in der Titelspalte einen Namen für das Ergebnis aus, um den Detailbereich für dieses Ergebnis zu öffnen. Alle Ergebnisse verfügen über eine Registerkarte mit den Ergebnisdetails. Sie können auf folgende Weise mit der Registerkarte „Details zum Befund“ interagieren:
   - Weitere Informationen zu der Sicherheitsanfälligkeit finden Sie unter dem Link im Abschnitt Details zur Sicherheitsanfälligkeit, um die Dokumentation zu dieser Sicherheitsanfälligkeit zu öffnen.

- Um Ihre Ressource genauer zu untersuchen, folgen Sie dem Link Ressourcen-ID im Abschnitt Betroffene Ressource, um die Servicekonsole für die betroffene Ressource zu öffnen.

Zu den Ergebnissen von Paketen mit Sicherheitslücken gibt es auch eine Registerkarte „Inspector Score“ und „Vulnerability Intelligence“, in der erklärt wird, wie der Amazon Inspector-Score für diese Entdeckung berechnet wurde, und es werden Informationen zu den allgemeinen Sicherheitslücken und Exploits (CVE) bereitgestellt, die mit dem Befund verknüpft sind. Weitere Informationen zu den Suchtypen finden Sie unter. Typen in Amazon Inspector finden

Das Amazon Inspector-Dashboard verstehen

Das Amazon Inspector-Dashboard bietet eine Momentaufnahme der aggregierten Statistiken für Ihre AWS Ressourcen in der aktuellen AWS Region. Diese Statistiken enthalten wichtige Kennzahlen zur Ressourcenabdeckung und zu aktiven Sicherheitslücken. Das Dashboard zeigt auch Gruppen von aggregierten Ergebnisdaten für Ihr Konto an, z. B. Amazon Elastic Compute Cloud (Amazon EC2) - Instances, Amazon Elastic Container Registry (Amazon ECR) und AWS Lambda Funktionen mit den wichtigsten Ergebnissen. Für eine eingehendere Analyse können Sie sich die unterstützenden Daten für Dashboard-Elemente ansehen.

Wenn es sich bei Ihrem Konto um das delegierte Administratorkonto von Amazon Inspector für eine Organisation handelt, enthält das Dashboard Kontoabdeckung, aggregierte Statistiken und Ergebnisdaten für alle Konten in Ihrer Organisation, einschließlich Ihres eigenen Kontos.

Anzeige des Dashboards

Das Dashboard zeigt einen Überblick über die Abdeckung Ihrer Umgebung und wichtige Ergebnisse.

So zeigen Sie das Dashboard an:

1. Öffnen Sie die Amazon Inspector Inspector-Konsole https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Sie können auf folgende Weise mit dem Dashboard interagieren:
   - Das Dashboard wird automatisch alle fünf Minuten aktualisiert. Sie können die Daten jedoch manuell aktualisieren, indem Sie das Aktualisierungssymbol in der oberen rechten Ecke der Seite auswählen.
   - Um die unterstützenden Daten für ein Element im Dashboard anzuzeigen, wählen Sie das Element aus.
   - Wenn Sie als delegierter Administrator von Amazon Inspector mehrere Konten über AWS Organisationen verwalten, zeigt das Dashboard aggregierte Statistiken für Ihre Mitgliedskonten an. Um das Dashboard zu filtern und nur Daten für ein bestimmtes Konto anzuzeigen, geben Sie die Konto-ID in das Feld Konto ein.

Dashboard-Komponenten verstehen und Daten interpretieren

Jeder Abschnitt des Amazon Inspector-Dashboards bietet Einblicke in wichtige Kennzahlen oder aktive Ergebnisdaten, die Ihnen helfen können, die aktuelle Sicherheitslage Ihrer AWS Ressourcen zu verstehen AWS-Region.

Abdeckung der Umwelt

Der Abschnitt Umweltberichterstattung enthält Statistiken über die von Amazon Inspector gescannten Ressourcen. In diesem Abschnitt können Sie die Anzahl und den Prozentsatz der Amazon EC2-Instances, Amazon ECR-Bilder und AWS Lambda Funktionen sehen, die von Amazon Inspector gescannt wurden. Wenn Sie AWS Organizations als delegierter Administrator von Amazon Inspector mehrere Konten verwalten, werden Ihnen auch die Gesamtzahl der Organisationskonten, die Anzahl mit aktiviertem Amazon Inspector und der daraus resultierende Deckungsprozentsatz für die Organisation angezeigt. In diesem Abschnitt können Sie auch feststellen, welche Ressourcen nicht von Amazon Inspector abgedeckt werden. Diese Ressourcen können Sicherheitslücken enthalten, die ausgenutzt werden könnten, um Ihr Unternehmen zu gefährden. Weitere Details finden Sie unter Bewertung der Abdeckung Ihrer AWS Umgebung durch Amazon Inspector.

Wenn Sie eine Deckungsgruppe auswählen, gelangen Sie zur Kontoverwaltungsseite für die von Ihnen gewählte Gruppierung. Auf der Kontoverwaltungsseite finden Sie Details darüber, welche Konten, Amazon EC2 EC2-Instances und Amazon ECR-Repositorys von Amazon Inspector abgedeckt werden.

Die folgenden Deckungsgruppen sind verfügbar:

- Account
- Instances
- Container-Repositorien
- Container-Images
- Lambda

Kritische Ergebnisse

Der Abschnitt Kritische Ergebnisse enthält eine Anzahl der kritischen Sicherheitslücken in Ihrer Umgebung und eine Gesamtzahl aller Ergebnisse in Ihrer Umgebung. In diesem Abschnitt werden die Zahlen pro Ressource und Bewertungstyp angezeigt. Weitere Informationen zu kritischen

Ergebnissen und dazu, wie Amazon Inspector die Kritikalität bestimmt, finden Sie unterDie Ergebnisse in Amazon Inspector verstehen.

Wenn Sie eine kritische Ergebnisgruppe auswählen, gelangen Sie zur Seite Alle Ergebnisse und wendet automatisch Filter an, um alle kritischen Ergebnisse anzuzeigen, die der von Ihnen ausgewählten Gruppierung entsprechen.

Die folgenden Gruppen kritischer Ergebnisse sind verfügbar:

- Ergebnisse von ECR-Container-Bildern
- Ergebnisse von Amazon EC2
- Ergebnisse zur Erreichbarkeit des Netzwerks
- AWS Lambda Ergebnisse zur Funktion

Risikobasierte Abhilfemaßnahmen

Im Abschnitt Risikobasierte Problembehebungen werden die fünf Softwarepakete mit den wichtigsten Sicherheitslücken aufgeführt, von denen die meisten Ressourcen in Ihrer Umgebung betroffen sind. Durch die Behebung dieser Pakete kann die Anzahl kritischer Risiken für Ihre Umgebung erheblich reduziert werden. Wählen Sie den Namen des Softwarepakets, um die zugehörigen Sicherheitslücken und die betroffenen Ressourcen zu sehen.

Konten mit den wichtigsten Ergebnissen

Im Abschnitt Konten mit den kritischsten Ergebnissen werden die fünf AWS Konten in Ihrer Umgebung mit den kritischsten Ergebnissen sowie die Gesamtzahl der Ergebnisse für dieses Konto angezeigt. Dieser Abschnitt ist nur vom delegierten Administratorkonto aus sichtbar, wenn Amazon Inspector für das Scannen mehrerer Konten mit konfiguriert ist. AWS Organizations Diese Ansicht hilft delegierten Administratoren zu verstehen, welche Konten innerhalb des Unternehmens möglicherweise am stärksten gefährdet sind.

Wählen Sie Konto-ID, um weitere Informationen über das betroffene Mitgliedskonto zu erhalten.

Amazon ECR-Repositorys mit den wichtigsten Ergebnissen

Im Abschnitt Elastic Container Registry (ECR) -Repositorien mit den wichtigsten Ergebnissen werden die fünf Amazon ECR-Repositorys in Ihrer Umgebung mit den kritischsten Container-Image-Ergebnissen angezeigt. In der Ansicht werden der Repository-Name, die AWS Konto-ID, das Erstellungsdatum des Repositorys, die Anzahl der kritischen Sicherheitslücken und die Gesamtzahl der Sicherheitslücken angezeigt. Anhand dieser Ansicht können Sie ermitteln, welche Repositorys möglicherweise am stärksten gefährdet sind.

Wählen Sie den Repository-Namen, um weitere Informationen über das betroffene Repository zu erhalten.

Container-Images mit den wichtigsten Ergebnissen

Im Abschnitt Container-Images mit den kritischsten Ergebnissen werden die fünf Container-Images in Ihrer Umgebung mit den kritischsten Ergebnissen angezeigt. In der Ansicht werden Image-Tag-Daten, Repository-Name, Image-Digest, AWS Konto-ID, Anzahl kritischer Sicherheitslücken und Gesamtzahl der Sicherheitslücken angezeigt. Anhand dieser Ansicht können Anwendungsbesitzer erkennen, welche Container-Images möglicherweise neu erstellt und neu gestartet werden müssen.

Wählen Sie Container-Image, um weitere Informationen über das betroffene Container-Image zu erhalten.

Fälle mit den kritischsten Ergebnissen

Der Abschnitt Instances mit den kritischsten Ergebnissen zeigt die fünf Amazon EC2 EC2-Instances mit den kritischsten Ergebnissen. Die Ansicht zeigt die Instanz-ID, die AWS Konto-ID, die Amazon Machine Image (AMI) -ID, die Anzahl kritischer Sicherheitslücken und die Gesamtzahl der Sicherheitslücken. Diese Ansicht hilft Infrastrukturbesitzern dabei, zu erkennen, welche Instances möglicherweise gepatcht werden müssen.

Wählen Sie Instance-ID, um weitere Informationen über die betroffene Amazon EC2 EC2-Instance zu erhalten.

Amazon Machine Images (AMI) mit den wichtigsten Ergebnissen

Im Abschnitt Amazon Machine Images (AMIs) mit den kritischsten Ergebnissen werden die fünf AMIs in Ihrer Umgebung mit den kritischsten Ergebnissen aufgeführt. Die Ansicht zeigt die AMI-ID, die AWS Konto-ID, die Anzahl der betroffenen EC2-Instances, die in der Umgebung ausgeführt werden, das AMI-Erstellungsdatum, die Betriebssystemplattform des AMI, die Anzahl der kritischen Sicherheitslücken und die Gesamtzahl der Sicherheitslücken. Anhand dieser Ansicht können Infrastrukturbesitzer ermitteln, welche AMIs möglicherweise neu erstellt werden müssen.

Wählen Sie Betroffene Instances aus, um weitere Informationen zu den Instances zu erhalten, die über das betroffene AMI gestartet wurden.

AWS Lambda Funktionen mit den kritischsten Ergebnissen

Im Abschnitt AWS Lambda Funktionen mit den kritischsten Ergebnissen werden die fünf wichtigsten Lambda-Funktionen in Ihrer Umgebung mit den kritischsten Ergebnissen angezeigt.

Die Ansicht zeigt den Namen der Lambda-Funktion, die AWS Konto-ID, die Laufzeitumgebung, die Anzahl kritischer Sicherheitslücken, die Anzahl der schwerwiegenden Sicherheitslücken und die Gesamtzahl der Sicherheitslücken. Diese Ansicht hilft Infrastrukturbesitzern dabei, zu erkennen, welche Lambda-Funktionen möglicherweise behoben werden müssen.

Wählen Sie Funktionsname, um weitere Informationen über die betroffene AWS Lambda Funktion zu erhalten.

Die Ergebnisse in Amazon Inspector verstehen

Ein Befund ist ein detaillierter Bericht über eine Sicherheitslücke, von der eine Ihrer AWS Ressourcen betroffen ist. Die Ergebnisse sind nach erkannten Sicherheitslücken benannt und enthalten Bewertungen des Schweregrads, Informationen zu den betroffenen Ressourcen und Details, in denen beschrieben wird, wie die gemeldeten Sicherheitslücken behoben werden können.

Amazon Inspector generiert ein Ergebnis, wenn es eine Sicherheitslücke in einer Amazon EC2 EC2-Instance, einem Container-Image in einem Amazon ECR-Repository oder einer AWS Lambda Funktion entdeckt. Amazon Inspector scannt kontinuierlich Ihre Computerumgebung und speichert all Ihre aktiven Ergebnisse, bis Sie sie korrigieren.

Wenn Sie ein Ergebnis korrigieren, wird das Ergebnis automatisch geschlossen und Amazon Inspector löscht das Ergebnis nach 7 Tagen. Wenn Sie eine Ressource löschen, löscht Amazon Inspector alle mit der Ressource verknüpften Ergebnisse nach 30 Tagen.

Wenn Sie Amazon Inspector deaktivieren, werden die Ergebnisse nach 24 Stunden entfernt. Wenn AWS Ihr Konto gesperrt wird, werden die Ergebnisse nach 90 Tagen entfernt.

Die Ergebnisse werden in einen der folgenden Staaten eingeteilt:

Aktiv

Amazon Inspector identifiziert Ergebnisse, die nicht behoben wurden, als aktiv.

Unterdrückt

Amazon Inspector identifiziert Ergebnisse, die einer oder mehreren Unterdrückungsregeln unterliegen, als unterdrückt. Unterdrückte Ergebnisse finden Sie in der Liste Unterdrückte Ergebnisse. Weitere Informationen finden Sie unter Unterdrückung der Ergebnisse von Amazon Inspector mit Unterdrückungsregeln.

Closed (Abgeschlossen)

Nachdem Sie eine Sicherheitslücke behoben haben, erkennt Amazon Inspector diese automatisch und ändert den Status der Entdeckung in „Geschlossen“. Geschlossene Ergebnisse werden nach 7 Tagen gelöscht.

Themen

- Typen in Amazon Inspector finden
- Suchen und Anzeigen der Ergebnisse von Amazon Inspector
- Amazon Inspector findet Einzelheiten
- Amazon Inspector-Score und Schwachstelleninformationen
- Schweregrade der Ergebnisse von Amazon Inspector

Typen in Amazon Inspector finden

Amazon Inspector generiert Ergebnisse für Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Container-Images in Amazon Elastic Container Registry (Amazon ECR) -Repositorys und Funktionen. AWS Lambda Amazon Inspector kann die folgenden Arten von Ergebnissen generieren.

Sicherheitslücke im Package

Package von Ergebnissen zu Sicherheitslücken in Paketen werden Softwarepakete in Ihrer AWS Umgebung identifiziert, die Common Vulnerabilities and Exposures (CVEs) ausgesetzt sind. Angreifer können diese ungepatchten Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten zu gefährden oder auf andere Systeme zuzugreifen. Das CVE-System ist eine Referenzmethode für öffentlich bekannte Sicherheitslücken und -risiken im Bereich der Informationssicherheit. Weitere Informationen finden Sie unter https://www.cve.org/.

CVE-Erkennungen für Linux werden Amazon Inspector innerhalb von 24 Stunden nach Veröffentlichung durch die Sicherheitsempfehlungen der Anbieter hinzugefügt. CVE-Erkennungen für Windows werden innerhalb von 48 Stunden nach ihrer Veröffentlichung durch Microsoft zu Amazon Inspector hinzugefügt. Sie können den verwendenSuche in der Amazon Inspector Inspector-Schwachstellendatenbank, um zu sehen, ob eine CVE-Erkennung unterstützt wird.

Amazon Inspector kann Ergebnisse zu Sicherheitslücken in Paketen für EC2-Instances, ECR-Container-Images und Lambda-Funktionen generieren. Die Ergebnisse der Sicherheitslücken von Paketen enthalten zusätzliche Details, die für diesen Befundtyp einzigartig sind, nämlich den Inspector-Score und die Schwachstelleninformationen.

Sicherheitslücke im Code

Durch die Entdeckung von Sicherheitslücken im Code werden Zeilen in Ihrem Code identifiziert, die Angreifer ausnutzen könnten. Zu den Sicherheitslücken im Code gehören Injektionsfehler, Datenlecks, schwache Kryptografie oder fehlende Verschlüsselung in Ihrem Code.

Amazon Inspector bewertet Ihren Anwendungscode für Lambda-Funktionen mithilfe von automatisiertem Denken und maschinellem Lernen, das Ihren Anwendungscode auf allgemeine Sicherheitsbestimmungen hin analysiert. Es identifiziert Richtlinienverstöße und Sicherheitslücken auf der Grundlage interner Detektoren, die in Zusammenarbeit mit Amazon entwickelt wurden CodeGuru. Eine Liste möglicher Erkennungen finden Sie unter CodeGuru Detector Library.

> **Important**
>
> Das Codescanning von Amazon Inspector erfasst Codefragmente, um erkannte Sicherheitslücken hervorzuheben. Diese Schnipsel können hartcodierte Anmeldeinformationen oder andere vertrauliche Materialien im Klartext enthalten.

Amazon Inspector kann Ergebnisse zu Code-Schwachstellen für Lambda-Funktionen generieren, wenn Sie diese Scannen von Lambda-Code mit Amazon Inspector aktiviert haben.

Codefragmente, die im Zusammenhang mit einer Code-Schwachstelle erkannt wurden, werden vom Service gespeichert. CodeGuru Standardmäßig wird zur Verschlüsselung Ihres Codes ein AWS eigener Schlüssel verwendet, der von gesteuert CodeGuru wird. Sie können jedoch Ihren eigenen, vom Kunden verwalteten Schlüssel für die Verschlüsselung über die Amazon Inspector API verwenden. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand für den Code in Ihren Ergebnissen.

Erreichbarkeit über das Netzwerk

Die Ergebnisse der Netzwerkerreichbarkeit deuten darauf hin, dass es in Ihrer Umgebung offene Netzwerkpfade zu Amazon EC2 EC2-Instances gibt. Diese Ergebnisse treten auf, wenn Ihre TCP- und UDP-Ports von den VPC-Edges aus erreichbar sind, z. B. ein Internet-Gateway (einschließlich Instances hinter Application Load Balancers oder Classic Load Balancers), eine VPC-Peering-Verbindung oder ein VPN über ein virtuelles Gateway. Diese Ergebnisse heben Netzwerkkonfigurationen hervor, die möglicherweise zu freizügig sind, wie z. B. schlecht verwaltete Sicherheitsgruppen, Zugriffskontrolllisten oder Internet-Gateways, oder die potenziell böswilligen Zugriff ermöglichen.

Amazon Inspector generiert nur Ergebnisse zur Netzwerkerreichbarkeit für Amazon EC2 EC2-Instances. Amazon Inspector führt alle 24 Stunden Scans durch, um die Erreichbarkeit des Netzwerks zu ermitteln.

Amazon Inspector bewertet beim Scannen nach Netzwerkpfaden die folgenden Konfigurationen:

- Amazon EC2-Instances
- AWS Lambda Funktionen
- Application Load Balancer
- Direct Connect
- Elastic Load Balancers
- Elastic-Network-Schnittstellen
- Internet-Gateways
- Listen zur Netzwerkzugriffskontrolle
- Routing-Tabellen
- Sicherheitsgruppen
- Subnets
- Virtuelle private Clouds
- Virtuelle private Gateways
- VPC-Endpunkte
- VPC-Gateway-Endpunkte
- VPC-Peering-Verbindungen
- VPN-Verbindungen

Suchen und Anzeigen der Ergebnisse von Amazon Inspector

Die Verfahren in diesem Abschnitt beschreiben, wie Sie Ergebnisse in Amazon Inspector über die Amazon Inspector Inspector-Konsole und API suchen und anzeigen können. Die Einzelheiten der Suche variieren je nach Art der Entdeckung, Art der Sicherheitslücke und den betroffenen Ressourcen. Weitere Informationen finden Sie unter Amazon Inspector findet Einzelheiten.

Console

Um die Ergebnisse in der Konsole anzuzeigen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Findings aus. Sie werden zu einem Bildschirm mit den Ergebnissen weitergeleitet, auf dem Sie alle Ihre Ergebnisse einsehen können. In der Tabelle

Ergebnisse können Sie ein Ergebnis auswählen, indem Sie in der Titelspalte den Namen des Ergebnisses auswählen.

3. (Optional) Sie können auch Ergebnisse anzeigen, die nach Kategorien gruppiert sind. Wählen Sie im Navigationsbereich Ergebnisse und dann eine der folgenden Kategorien aus:

   - Nach Sicherheitslücke
   - Nach Instanz

     > **Note**
     >
     > Ergebnisse, die nach Instanzen gruppiert sind, enthalten keine Informationen zur Netzwerkverfügbarkeit.

   - Nach Container-Image
   - Nach dem Container-Repository
   - Nach Lambda-Funktion

API

Führen Sie den ListFindingsAPI-Vorgang aus. In der Anfrage können Sie angeben `filterCriteria`, dass bestimmte Ergebnisse zurückgegeben werden sollen.

Amazon Inspector findet Einzelheiten

In der Amazon Inspector Inspector-Konsole können Sie Details zu jedem Ergebnis einsehen. Die Einzelheiten zu den Ergebnissen variieren je nach Art des Befundes.

Um die Details zu einem Ergebnis anzuzeigen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home
2. Wählen Sie die Region aus, in der Sie sich die Ergebnisse ansehen möchten.
3. Wählen Sie im Navigationsbereich Findings aus, um die Ergebnisliste anzuzeigen
4. (Optional) Verwenden Sie die Filterleiste, um ein bestimmtes Ergebnis auszuwählen. Weitere Informationen finden Sie unter Filtern der Ergebnisse von Amazon Inspector.
5. Wählen Sie ein Ergebnis aus, um das zugehörige Detailfenster anzuzeigen.

Der Bereich mit den Ergebnisdetails enthält die grundlegenden Erkennungsmerkmale des Ergebnisses. Dazu gehören der Titel des Befundes sowie eine grundlegende Beschreibung der identifizierten Sicherheitslücke, Vorschläge zur Behebung und eine Bewertung des Schweregrads. Informationen zur Bewertung finden Sie unterSchweregrade der Ergebnisse von Amazon Inspector.

Die für ein Ergebnis verfügbaren Details variieren je nach Art des Ergebnisses und der betroffenen Ressource.

Alle Ergebnisse enthalten die AWS-Konto ID-Nummer, für die das Ergebnis identifiziert wurde, einen Schweregrad, einen Befundtyp, das Datum, an dem das Ergebnis erstellt wurde, und einen Abschnitt „Betroffene Ressource“ mit Details zu dieser Ressource.

Der Typ des Ergebnisses bestimmt, welche Informationen zur Behebung und zur Schwachstellenanalyse für den Befund verfügbar sind. Je nach Art des Ergebnisses sind unterschiedliche Ergebnisdetails verfügbar.

Sicherheitslücke im Package

Ergebnisse zu Sicherheitslücken in Paketen sind für EC2-Instances, ECR-Container-Images und Lambda-Funktionen verfügbar. Weitere Informationen finden Sie unter Sicherheitslücke im Package.

Zu den Ergebnissen der Paketschwachstelle gehören auchAmazon Inspector-Score und Schwachstelleninformationen.

Dieser Befundtyp enthält die folgenden Details:

- Fix verfügbar — Zeigt an, ob die Sicherheitsanfälligkeit in einer neueren Version der betroffenen Pakete behoben wurde. Hat einen der folgenden Werte:
  - `YES`, was bedeutet, dass alle betroffenen Pakete eine feste Version haben.
  - `NO`, was bedeutet, dass keine betroffenen Pakete eine feste Version haben.
  - `PARTIAL`, was bedeutet, dass eines oder mehrere (aber nicht alle) der betroffenen Pakete eine feste Version haben.
- Exploit verfügbar — Zeigt an, dass es sich bei der Sicherheitsanfälligkeit um einen bekannten Exploit handelt.
  - `YES`, was bedeutet, dass es sich bei der in Ihrer Umgebung entdeckten Sicherheitslücke um einen bekannten Exploit handelt. Amazon Inspector hat keinen Einblick in die Verwendung von Exploits in einer Umgebung.
  - `NO`, was bedeutet, dass für diese Sicherheitsanfälligkeit kein Exploit bekannt ist.

- Betroffene Pakete — Listet jedes Paket auf, das bei der Entdeckung als gefährdet identifiziert wurde, sowie die Einzelheiten zu jedem Paket:
- Dateipfad — Die EBS-Volume-ID und die Partitionsnummer, die mit einem Ergebnis verknüpft sind. Dieses Feld ist in den Ergebnissen für EC2-Instances enthalten, die mit gescannt wurden. Scannen ohne Agenten
- Installierte Version//Behobene Version — Die Versionsnummer des aktuell installierten Pakets, für das eine Sicherheitslücke erkannt wurde. Vergleichen Sie die installierte Versionsnummer mit dem Wert nach dem Schrägstrich (/). Der zweite Wert ist die Versionsnummer des Pakets, das die entdeckte Sicherheitslücke behebt, wie sie in den Common Vulnerabilities and Exposures (CVEs) oder in der zugehörigen Empfehlung angegeben ist. Wenn die Sicherheitsanfälligkeit in mehreren Versionen behoben wurde, wird in diesem Feld die neueste Version aufgeführt, die den Fix enthält. Wenn ein Fix nicht verfügbar ist, ist dieser Wert`None available`.

  > **Note**
  >
  > Wenn ein Ergebnis erkannt wurde, bevor Amazon Inspector begann, dieses Feld in die Ergebnisse aufzunehmen, ist der Wert für dieses Feld leer. Möglicherweise ist jedoch ein Fix verfügbar.

- Paketmanager — Der Paketmanager, der zur Konfiguration dieses Pakets verwendet wurde.
- Problembehebung — Wenn ein Update über ein aktualisiertes Paket oder eine aktualisierte Programmierbibliothek verfügbar ist, enthält dieser Abschnitt die Befehle, die Sie ausführen können, um das Update durchzuführen. Sie können den bereitgestellten Befehl kopieren und in Ihrer Umgebung ausführen.

  > **Note**
  >
  > Die Befehle zur Problembehebung werden aus Datenfeeds von Anbietern bereitgestellt und können je nach Systemkonfiguration variieren. Genauere Hinweise finden Sie in den Referenzen oder in der Dokumentation zum Betriebssystem.

- Details zur Sicherheitslücke — bietet einen Link zur bevorzugten Quelle von Amazon Inspector für das im Ergebnis identifizierte CVE, z. B. National Vulnerability Database (NVD), REDHAT oder ein anderer Betriebssystemanbieter. Darüber hinaus finden Sie die Schweregrade für den Befund. Weitere Informationen zur Bewertung des Schweregrads finden Sie beispielsweise

unterSchweregrade der Ergebnisse von Amazon Inspector. Die folgenden Punktzahlen sind enthalten, einschließlich der jeweiligen Bewertungsvektoren:

- EPSS-Score
- Ergebnis des Inspector
- CVSS 3.1 von Amazon CVE
- CVSS 3.1 von NVD
- CVSS 2.0 von NVD (falls zutreffend, für ältere CVEs)

- Verwandte Sicherheitslücken — Spezifiziert weitere Sicherheitslücken im Zusammenhang mit der Entdeckung. In der Regel handelt es sich dabei um andere CVEs, die sich auf dieselbe Paketversion auswirken, oder um andere CVEs innerhalb derselben Gruppe wie die gefundene CVE, wie vom Hersteller festgelegt.

Sicherheitslücke im Code

Die Ergebnisse von Sicherheitslücken im Code sind nur für Lambda-Funktionen verfügbar. Weitere Informationen finden Sie unter Sicherheitslücke im Code. Dieser Erkennungstyp enthält die folgenden Details:

- Fix verfügbar — Für Sicherheitslücken im Code ist dieser Wert immer gültig`YES`.
- Name des Detektors — Der Name des CodeGuru Detektors, der zur Erkennung der Sicherheitslücke im Code verwendet wurde. Eine Liste möglicher Erkennungen finden Sie in der CodeGuru Detektorbibliothek.
- Melder-Tags — Die mit dem Detektor verknüpften CodeGuru Tags CodeGuru verwenden Tags, um Erkennungen zu kategorisieren.
- Relevante CWE — IDs der Common Weakness Enumeration (CWE), die mit der Sicherheitslücke im Code verknüpft sind.
- Dateipfad — Der Speicherort der Code-Sicherheitslücke.
- Ort der Sicherheitslücke — Für Sicherheitslücken beim Scannen von Lambda-Code zeigt dieses Feld die genauen Codezeilen an, in denen Amazon Inspector die Sicherheitsanfälligkeit gefunden hat.
- Vorgeschlagene Behebung — Hier wird vorgeschlagen, wie der Code bearbeitet werden kann, um das Problem zu beheben.

Erreichbarkeit über das Netzwerk

Ergebnisse zur Netzwerkerreichbarkeit sind nur für EC2-Instances verfügbar. Weitere Informationen finden Sie unter Erreichbarkeit über das Netzwerk. Dieser Ergebnistyp enthält die folgenden Details:

- Offener Portbereich — Der Portbereich, über den auf die EC2-Instance zugegriffen werden konnte.
- Offene Netzwerkpfade — Zeigt den offenen Zugriffspfad zur EC2-Instance an. Wählen Sie ein Element im Pfad aus, um weitere Informationen zu erhalten.
- Behebung — Empfiehlt eine Methode zum Schließen des offenen Netzwerkpfads.

Amazon Inspector-Score und Schwachstelleninformationen

Wenn Sie in der Amazon Inspector Inspector-Konsole einen Befund auswählen, können Sie sich den Inspector-Score ansehen. Auf der Registerkarte Vulnerability Intelligence werden die Bewertungsdetails für die Sicherheitslücke eines Pakets sowie Details zur Schwachstellenanalyse angezeigt. Diese Details sind nur für Sicherheitslücke im Package Ergebnisse verfügbar.

Amazon Inspector-Punktzahl

Der Amazon Inspector-Score ist ein kontextualisierter Score, den Amazon Inspector für jeden EC2-Instance-Fund erstellt. Der Amazon Inspector-Score wird bestimmt, indem die Basisinformationen des CVSS v3.1-Scores mit Informationen korreliert werden, die während der Scans aus Ihrer Computerumgebung gesammelt wurden, wie z. B. Ergebnisse zur Netzwerkerreichbarkeit und Daten zur Ausnutzbarkeit. Beispielsweise kann der Amazon Inspector-Score eines Ergebnisses niedriger sein als der Basiswert, wenn die Sicherheitsanfälligkeit über das Netzwerk ausgenutzt werden kann, Amazon Inspector jedoch feststellt, dass kein offener Netzwerkpfad zur anfälligen Instance über das Internet verfügbar ist.

Die Basisbewertung für ein Ergebnis ist die vom Anbieter bereitgestellte CVSS v3.1-Basisbewertung. RHEL-, Debian- oder Amazon-Hersteller-Basiswerte werden unterstützt. Für andere Anbieter oder für Fälle, in denen der Anbieter keine Bewertung angegeben hat, verwendet Amazon Inspector die Basisbewertung aus der National Vulnerability Database (NVD). Amazon Inspector verwendet den Common Vulnerability Scoring System Version 3.1 Calculator, um den Score zu berechnen. Sie können die Quelle der Basisbewertung eines einzelnen Ergebnisses in den Details des Ergebnisses unter den Schwachstellendetails als Quelle der Sicherheitslücke (oder packageVulnerabilityDetails.source in der Ergebnis-JSON) sehen

> **Note**
>
> Der Amazon Inspector Score ist für Linux-Instances, auf denen Ubuntu ausgeführt wird, nicht verfügbar. Das liegt daran, dass Ubuntu seinen eigenen Schweregrad für Sicherheitslücken definiert, der sich vom zugehörigen CVE-Schweregrad unterscheiden kann.

Einzelheiten zur Amazon Inspector-Punktzahl

Wenn Sie die Detailseite eines Befundes öffnen, können Sie die Registerkarte Inspector Score und Vulnerability Intelligence auswählen. Dieses Feld zeigt den Unterschied zwischen dem Basiswert und dem Inspector-Score. In diesem Abschnitt wird erklärt, wie Amazon Inspector den Schweregrad auf der Grundlage einer Kombination aus dem Amazon Inspector-Score und dem Hersteller-Score für das Softwarepaket zugewiesen hat. Wenn sich die Punktzahlen unterscheiden, wird in diesem Bereich erklärt, warum.

Im Abschnitt CVSS-Score-Metriken finden Sie eine Tabelle mit Vergleichen zwischen den CVSS-Basisscore-Metriken und dem Inspector-Score. Bei den verglichenen Kennzahlen handelt es sich um die Basiskennzahlen, die im CVSS-Spezifikationsdokument definiert sind, das von verwaltet wird. first.org Im Folgenden finden Sie eine Zusammenfassung der Basiskennzahlen:

Angriffsvektor

Der Kontext, in dem eine Sicherheitslücke ausgenutzt werden kann. Bei Ergebnissen von Amazon Inspector kann dies „Netzwerk“, „Angrenzendes Netzwerk“ oder „Lokal“ sein.

Komplexität des Angriffs

Dies beschreibt den Schwierigkeitsgrad, mit dem ein Angreifer konfrontiert sein wird, wenn er die Sicherheitsanfälligkeit ausnutzt. Eine niedrige Punktzahl bedeutet, dass der Angreifer nur wenige oder keine zusätzlichen Bedingungen erfüllen muss, um die Sicherheitsanfälligkeit auszunutzen. Eine hohe Punktzahl bedeutet, dass ein Angreifer erhebliche Anstrengungen unternehmen muss, um einen erfolgreichen Angriff mit dieser Sicherheitsanfälligkeit durchzuführen.

Privileg erforderlich

Dies beschreibt die Rechtestufe, die ein Angreifer benötigt, um eine Sicherheitslücke auszunutzen.

Interaktion mit dem Benutzer

Diese Metrik gibt an, ob für einen erfolgreichen Angriff unter Ausnutzung dieser Sicherheitsanfälligkeit ein menschlicher Benutzer erforderlich ist, der nicht der Angreifer ist.

Scope

Dies gibt an, ob sich eine Sicherheitsanfälligkeit in einer anfälligen Komponente auf Ressourcen in Komponenten auswirkt, die über den Sicherheitsbereich der anfälligen Komponente hinausgehen. Wenn dieser Wert Unverändert ist, sind die betroffene Ressource und die betroffene Ressource identisch. Wenn dieser Wert geändert ist, kann die anfällige Komponente ausgenutzt werden, um Ressourcen zu beeinträchtigen, die von verschiedenen Sicherheitsbehörden verwaltet werden.

Vertraulichkeit

Dabei wird das Ausmaß der Auswirkungen auf die Vertraulichkeit von Daten innerhalb einer Ressource gemessen, wenn die Sicherheitsanfälligkeit ausgenutzt wird. Dies reicht von „Keine“, bei der keine Vertraulichkeit verloren geht, bis hin zu „Hoch“, bei der alle Informationen innerhalb einer Ressource weitergegeben werden oder vertrauliche Informationen wie Passwörter oder Verschlüsselungsschlüssel preisgegeben werden können.

Integrität

Dabei wird das Ausmaß der Auswirkungen auf die Integrität der Daten innerhalb der betroffenen Ressource gemessen, wenn die Sicherheitsanfälligkeit ausgenutzt wird. Die Integrität ist gefährdet, wenn der Angreifer Dateien innerhalb der betroffenen Ressourcen verändert. Die Bewertung reicht von „Keine“, wobei der Angriff es einem Angreifer nicht ermöglicht, Informationen zu ändern, bis hin zu „Hoch“, bei dem die Sicherheitsanfälligkeit es einem Angreifer ermöglichen würde, einige oder alle Dateien zu ändern, oder die Dateien, die geändert werden könnten, schwerwiegende Folgen haben könnten.

Verfügbarkeit

Damit wird das Ausmaß der Auswirkungen auf die Verfügbarkeit der betroffenen Ressource gemessen, wenn die Sicherheitsanfälligkeit ausgenutzt wird. Die Bewertung reicht von „Keine“, wenn die Sicherheitsanfälligkeit die Verfügbarkeit überhaupt nicht beeinträchtigt, bis hin zu „Hoch“, bei dem der Angreifer bei Ausnutzung die Verfügbarkeit der Ressource vollständig verweigern oder dafür sorgen kann, dass ein Dienst nicht verfügbar ist.

Informationen zu Sicherheitslücken

In diesem Abschnitt werden die verfügbaren Informationen über das CVE von Amazon sowie branchenübliche Quellen für Sicherheitsinformationen wie Recorded Future und Cybersecurity and Infrastructure Security Agency (CISA) zusammengefasst.

> **Note**
>
> Intel von CISA, Amazon oder Recorded Future wird nicht für alle CVEs verfügbar sein.

Sie können die Informationen zu Sicherheitslücken in der Konsole oder mithilfe der BatchGetFindingDetailsAPI einsehen. Die folgenden Details sind in der Konsole verfügbar:

ATT&CK

In diesem Abschnitt werden die Taktiken, Techniken und Verfahren (TTPs) von MITRE im Zusammenhang mit dem CVE beschrieben. Die zugehörigen TTPs werden angezeigt. Wenn es mehr als zwei zutreffende TTPs gibt, können Sie den Link auswählen, um eine vollständige Liste anzuzeigen. Wenn Sie eine Taktik oder Technik auswählen, werden Informationen dazu auf der MITRE-Website geöffnet.

CISA

Dieser Abschnitt behandelt relevante Daten im Zusammenhang mit der Sicherheitsanfälligkeit. Das Datum, an dem die Cybersecurity and Infrastructure Security Agency (CISA) die Sicherheitslücke in den Katalog der bekannten Sicherheitslücken aufgenommen hat, basierend auf Hinweisen auf eine aktive Ausnutzung, und das Fälligkeitsdatum, an dem die CISA erwartet, dass die Systeme gepatcht werden. Diese Informationen stammen von CISA.

Bekannte Schadsoftware

In diesem Abschnitt sind bekannte Exploit-Kits und Tools aufgeführt, die diese Sicherheitsanfälligkeit ausnutzen.

Beweise

In diesem Abschnitt werden die kritischsten Sicherheitsereignisse im Zusammenhang mit dieser Sicherheitsanfälligkeit zusammengefasst. Wenn mehr als 3 Ereignisse dieselbe Kritikalitätsstufe haben, werden die drei jüngsten Ereignisse angezeigt.

Letztes Mal gemeldet

In diesem Abschnitt wird das Datum des letzten bekannten öffentlichen Exploits für diese Sicherheitsanfälligkeit angezeigt.

Schweregrade der Ergebnisse von Amazon Inspector

Wenn Amazon Inspector eine Schwachstellenfeststellung generiert, weist es der Entdeckung automatisch einen Schweregrad zu. Der Schweregrad einer Entdeckung spiegelt die Hauptmerkmale der Entdeckung wider und kann Ihnen daher bei der Bewertung und Priorisierung Ihrer Ergebnisse helfen. Der Schweregrad eines Ergebnisses impliziert nicht die Wichtigkeit oder Bedeutung, die eine betroffene Ressource für Ihr Unternehmen haben könnte, und gibt auch keinen Hinweis darauf.

Der Schweregrad eines Ergebnisses wird durch einen numerischen Wert bestimmt, der einem der folgenden Schweregrade entspricht: informativ, niedrig, mittel, hoch oder kritisch.

Die Methode, mit der Amazon Inspector den Schweregrad bestimmt, hängt vom Befundtyp ab. In den folgenden Abschnitten erfahren Sie mehr darüber, wie Amazon Inspector den Schweregrad für jeden Befundtyp bestimmt.

Schweregrad der Sicherheitslücke im Softwar

Amazon Inspector verwendet den NVD/CVSS-Score als Grundlage für die Bewertung des Schweregrads von Sicherheitslücken in Softwarepaketen. Der NVD/CVSS-Wert ist der vom NVD veröffentlichte und vom CVSS definierte Schweregrad der Sicherheitslücke. Der NVD/CVSS-Score setzt sich aus Sicherheitsmetriken wie der Komplexität des Angriffs, dem Reifegrad des Exploit-Codes und den erforderlichen Rechten zusammen. Amazon Inspector erstellt eine numerische Bewertung von 1 bis 10, die den Schweregrad der Sicherheitsanfälligkeit widerspiegelt. Amazon Inspector stuft dies als Basiswert ein, da er den Schweregrad einer Sicherheitslücke anhand ihrer intrinsischen Merkmale widerspiegelt, die im Laufe der Zeit konstant sind. Bei dieser Bewertung wird auch davon ausgegangen, dass die Auswirkungen im schlimmsten Fall auf verschiedene bereitgestellte Umgebungen angemessen sind. Der CVSS v3-Standard ordnet die CVSS-Scores den folgenden Schweregraden zu.

Ergebnis	Bewertung
0	Informativ

0,1—3,9	Niedrig
4,0—6,9	Mittelschwer
7,0—8,9	Hoch
9,0—10,0	Kritisch

Die gefundenen Sicherheitslücken in Paketen können auch den Schweregrad Untriaged haben. Das bedeutet, dass der Anbieter noch keinen Schwachstellen-Score für die entdeckte Sicherheitslücke festgelegt hat. In diesem Fall empfehlen wir, die Referenz-URLs für das Ergebnis zu verwenden, um die Sicherheitslücke zu untersuchen und entsprechend zu reagieren.

Zu den Ergebnissen der Paketschwachstellen gehören die folgenden Bewertungen und die zugehörigen Bewertungsvektoren als Teil der Ergebnisdetails:

- EPSS-Punktzahl
- Ergebnis des Inspector
- CVSS 3.1 von Amazon CVE
- CVSS 3.1 von NVD
- CVSS 2.0 von NVD (falls zutreffend)

Schweregrad der Sicherheitslücke

Für die Suche nach Sicherheitslücken im Code verwendet Amazon Inspector die Schweregrade, die von den CodeGuru Amazon-Detektoren definiert wurden, die den Befund generiert haben. Jedem Detektor wird mithilfe des CVSS v3-Bewertungssystems ein Schweregrad zugewiesen. Eine Erläuterung der CodeGuru verwendeten Schweregrade finden Sie unter Schweregraddefinitionen im CodeGuru Leitfaden. Eine Liste der Melder nach Schweregrad finden Sie, wenn Sie eine der folgenden unterstützten Programmiersprachen auswählen:

- Python-Detektoren nach Schweregrad
- Java-Detektoren nach Schweregrad

Schweregrad der Netzwerkerreichbarkeit

Amazon Inspector bestimmt den Schweregrad einer Sicherheitslücke im Netzwerk auf der Grundlage der offengelegten Services, Ports und Protokolle sowie der Art des offenen Pfads. In der folgenden Tabelle werden diese Schweregrade definiert. Der Wert in der Spalte Bewertung offener Pfade steht für offene Pfade von virtuellen Gateways, Peer-VPCs und Netzwerken. AWS Direct Connect Für alle anderen exponierten Dienste, Ports und Protokolle wurde der Schweregrad „Information“ eingestuft.

Service	TCP-Ports	UDP-Anschlüsse	Bewertung des Internetpfads	Pfadbewertung öffnen
DHCP	67, 68, 546, 547	67, 68, 546, 547	Mittelschwer	Informativ
Elasticsearch	9300, 9200	N/A	Mittelschwer	Informativ
FTP	21	21	Hoch	Mittelschwer
Global Catalog LDAP	3268	N/A	Mittelschwer	Informativ
Global Catalog LDAP über TLS	3269	N/A	Mittelschwer	Informativ
HTTP	80	80	Niedrig	Informativ
HTTPS	443	443	Niedrig	Informativ
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752	Mittelschwer	Informativ
LDAP	389	389	Mittelschwer	Informativ
LDAP über TLS	636	N/A	Mittelschwer	Informativ
MongoDB	27017, 27018, 27019, 28017	N/A	Mittelschwer	Informativ
MySQL	3306	N/A	Mittelschwer	Informativ
NetBIOS	137, 139	137, 138	Mittelschwer	Informativ

NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110	Mittelschwer	Informativ
Oracle	1521, 1630	N/A	Mittelschwer	Informativ
PostgreSQL	5432	N/A	Mittelschwer	Informativ
Druckdienste	515	N/A	Hoch	Mittelschwer
RDP	3389	3389	Mittelschwer	Niedrig
RPC	111, 135, 530	111, 135, 530	Mittelschwer	Informativ
SMB	445	445	Mittelschwer	Informativ
SSH	22	22	Mittelschwer	Niedrig
SQL Server	1433	1434	Mittelschwer	Informativ
Syslog	601	514	Mittelschwer	Informativ
Telnet	23	23	Hoch	Mittelschwer
WINS	1512, 42	1512, 42	Mittelschwer	Informativ

Ergebnisse in Amazon Inspector verwalten

Amazon Inspector bietet verschiedene Möglichkeiten, Ihre Ergebnisse zu sortieren, zu gruppieren und zu verwalten. Mit diesen Funktionen können Sie die Ergebnisse an Ihre Umgebung anpassen, Ergebnisse anhand verschiedener Ansichten zusammenfassen und sich auf Schwachstellen in Ihrer spezifischen AWS Umgebung konzentrieren.

Die Ergebnisse werden je nach Status in verschiedenen Ansichten angezeigt: aktiv, unterdrückt oder geschlossen. Standardmäßig werden in jeder Ansicht nur aktive Ergebnisse angezeigt. Ein aktives Ergebnis stellt ein potenzielles Sicherheitsproblem dar, das von Amazon Inspector erkannt wurde und auf eine Sicherheitslücke oder potenzielle Bedrohung hinweist. Unterdrückte Ergebnisse sind aktive Ergebnisse, die Sie mithilfe von Unterdrückungsregeln ausgeschlossen haben. Amazon Inspector setzt den Status eines Befundes automatisch auf „Geschlossen“, wenn es feststellt, dass das Ergebnis behoben wurde. Sie schließen Ergebnisse nicht manuell.

Sie können die Ergebnisse auch in einem Service anzeigen AWS Security Hub, der einen umfassenden Überblick über Ihren Sicherheitsstatus in Ihrer gesamten AWS Umgebung bietet. Weitere Informationen finden Sie unter Amazon Inspector Inspector-Integration mit AWS Security Hub. Die Ergebnisse von Container-Images sind auch in der Amazon ECR-Konsole verfügbar, und Sie können die Ergebnisse für alle Ressourcen mithilfe der AWS Command Line Interface (AWS CLI) oder API anzeigen.

Themen

Ergebnisse von Amazon Inspector anzeigen

Die Amazon Inspector Inspector-Konsole zeigt Ergebnisse in Registerkartenansichten an, die auf verwandten Gruppierungen basieren. Jede Ansicht enthält Informationen, die Ihnen helfen können, spezifische Sicherheitslücken zu analysieren, Ihre anfälligsten Ressourcen zu identifizieren und die

Gesamtauswirkung von Sicherheitslücken in Ihrer Umgebung einzuschätzen. Sie können zu einer anderen Ergebnisansicht wechseln, indem Sie im Navigationsbereich „Ergebnisse“ eine Option auswählen. Sie können auch in jeder Ansicht einen Filter erstellen, um sich auf bestimmte Arten von Ergebnissen zu konzentrieren. Weitere Informationen zur Verwendung von Filtern finden Sie unterFiltern der Ergebnisse von Amazon Inspector.

Die Ergebnisse können nach den folgenden Parametern gruppiert werden:

- Nach Sicherheitslücke — Listet die kritischsten Sicherheitslücken auf, die in Ihrer Umgebung entdeckt wurden. Wählen Sie in dieser Ansicht einen Titel der Sicherheitslücke aus, um einen Detailbereich mit zusätzlichen Informationen zu öffnen.
- Nach Konto — Listet Ihre Konten auf, Amazon Inspector scannt die Deckung in Prozent für jedes Konto und die Gesamtzahl der Ergebnisse mit kritischem und hohem Schweregrad für jedes Konto. Diese Gruppierung steht nur delegierten Administratoren zur Verfügung.
- Nach Instance — Listet die anfälligsten Amazon EC2 EC2-Instances in Ihrer Umgebung auf.
- Nach Container-Image — Listet die anfälligsten Amazon ECR-Container-Images in Ihrer Umgebung auf.
- Nach Container-Repository — Zeigt die Repositorys mit den meisten Sicherheitslücken an.
- Nach Lambda-Funktion — Zeigt die Lambda-Funktionen mit den meisten Sicherheitslücken an.
- Alle Ergebnisse — Zeigt eine vollständige Liste der Ergebnisse für Ihre Umgebung an. Dies ist die Standardansicht, wenn Sie zur Ergebnisseite navigieren. In dieser Ansicht können Sie nach aktiven, unterdrückten und geschlossenen Ergebnissen filtern.

Sie können Unterdrückungsregeln auf der Grundlage von Filtern erstellen, um Ergebnisse aus den Ergebnisansichten auszuschließen. Weitere Informationen finden Sie unter Unterdrückung der Ergebnisse von Amazon Inspector mit Unterdrückungsregeln.

Filtern der Ergebnisse von Amazon Inspector

Mit einem Ergebnisfilter können Sie nur die Ergebnisse anzeigen, die den von Ihnen angegebenen Kriterien entsprechen. Ergebnisse, die den Filterkriterien nicht entsprechen, werden aus Ihrer Ansicht ausgeschlossen. Sie können Suchfilter mit der Amazon Inspector Inspector-Konsole erstellen. Informationen zur Verwendung dieser Filter zur automatischen Unterdrückung vorhandener und future Ergebnisse finden Sie unterUnterdrückung der Ergebnisse von Amazon Inspector mit Unterdrückungsregeln.

Filter in der Amazon Inspector Inspector-Konsole erstellen

In jeder Ergebnisansicht können Sie die Filterfunktion verwenden, um Ergebnisse mit bestimmten Merkmalen zu finden. Filter werden entfernt, wenn Sie zu einer anderen Ansicht mit Registerkarten wechseln.

Ein Filter besteht aus einem Filterkriterium, das aus einem Filterattribut und einem Filterwert besteht. Ergebnisse, die Ihren Filterkriterien nicht entsprechen, werden von der Ergebnisliste ausgeschlossen. Um beispielsweise alle Ergebnisse zu sehen, die mit Ihrem Administratorkonto verknüpft sind, können Sie das AWS Konto-ID-Attribut auswählen und es mit dem Wert Ihrer zwölfstelligen AWS Konto-ID verknüpfen.

Einige Filterkriterien gelten für alle Ergebnisse, während andere nur für bestimmte Ressourcentypen oder nur für Suchtypen verfügbar sind.

Um einen Filter auf die Ergebnisansicht anzuwenden

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Findings aus. In der Standardansicht werden alle Ergebnisse mit dem Status Aktiv angezeigt.
3. Um Ergebnisse nach Kriterien zu filtern, wählen Sie die Filterleiste Hinzufügen aus, um eine Liste aller zutreffenden Filterkriterien für diese Ansicht anzuzeigen. Verschiedene Filterkriterien sind in verschiedenen Ansichten verfügbar.
4. Wählen Sie aus der Liste ein Kriterium aus, nach dem Sie filtern möchten.
5. Geben Sie im Kriterieneingabebereich die gewünschten Filterwerte ein, um dieses Kriterium zu definieren.
6. Wählen Sie Anwenden, um dieses Filterkriterium auf Ihre aktuellen Ergebnisse anzuwenden. Sie können weitere Filterkriterien hinzufügen, indem Sie erneut die Filtereingabeleiste auswählen.
7. (Optional) Um Ihre unterdrückten oder geschlossenen Ergebnisse anzuzeigen, wählen Sie in der Filterleiste Aktiv und dann Unterdrückt oder Geschlossen aus. Wählen Sie „Alle anzeigen“, um aktive, unterdrückte und geschlossene Ergebnisse in derselben Ansicht anzuzeigen.

Unterdrückung der Ergebnisse von Amazon Inspector mit Unterdrückungsregeln

Verwenden Sie Unterdrückungsregeln, um Ergebnisse auszuschließen, die den Kriterien entsprechen. Sie können beispielsweise eine Regel erstellen, die alle Ergebnisse mit niedrigen Sicherheitslücken unterdrückt, sodass Sie sich nur auf die Ergebnisse konzentrieren können, die am kritischsten sind.

> **Note**
>
> Unterdrückungsregeln werden nur verwendet, um Ihre Ergebnisliste zu filtern. Sie haben keine Auswirkungen auf die Ergebnisse und verhindern auch nicht, dass Amazon Inspector Ergebnisse generiert.

Wenn Amazon Inspector Ergebnisse generiert, die einer Unterdrückungsregel entsprechen, werden die Ergebnisse auf Unterdrückt gesetzt. Ergebnisse, die einer Unterdrückungsregel entsprechen, werden standardmäßig nicht in Ihrer Liste angezeigt.

Amazon Inspector speichert unterdrückte Ergebnisse, bis sie behoben sind. Amazon Inspector erkennt behobene Ergebnisse. Wenn Amazon Inspector ein behobenes Ergebnis erkennt, setzt es das Ergebnis auf „Geschlossen“ und speichert es für 7 Tage.

Unterdrückte Ergebnisse werden bei AWS Security Hub und Amazon EventBridge als Ereignisse veröffentlicht. Sie können unerwünschte Ergebnisse in Security Hub automatisch unterdrücken, indem Sie den Status der Ergebnisse mithilfe einer EventBridge Regel ändern. Weitere Informationen finden Sie unter So erstellen Sie Regeln für die automatische Unterdrückung in AWS Security Hub.

Sie können keine Unterdrückungsregel erstellen, die Ergebnisse schließt oder behebt. Sie können nur eine Unterdrückungsregel erstellen, um zu filtern, welche Ergebnisse in Ihrer Liste erscheinen. Sie können unterdrückte Ergebnisse jederzeit in der Amazon Inspector Inspector-Konsole einsehen.

> **Note**
>
> Mitgliedskonten in einer Organisation können keine Unterdrückungsregeln erstellen oder verwalten.

Eine Unterdrückungsregel erstellen

Sie können Unterdrückungsregeln erstellen, um die Liste der Ergebnisse zu filtern, die standardmäßig angezeigt werden. Sie können eine Unterdrückungsregel programmgesteuert erstellen, indem Sie die CreateFilterAPI verwenden und `SUPRESS` als Wert für angeben. `action`

> **Note**
>
> Nur eigenständige Konten und delegierte Amazon Inspector-Administratoren können Unterdrückungsregeln erstellen und verwalten. Mitgliedern einer Organisation wird im Navigationsbereich keine Option für Unterdrückungsregeln angezeigt.

Um eine Unterdrückungsregel zu erstellen (Konsole)

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich die Option Suppression Rules aus. Wählen Sie dann Create rule (Regel erstellen) aus.
3. Gehen Sie für jedes Kriterium wie folgt vor:
   - Wählen Sie die Filterleiste aus, um eine Liste mit Filterkriterien anzuzeigen, die Sie zu Ihrer Unterdrückungsregel hinzufügen können.
   - Wählen Sie die Filterkriterien für Ihre Unterdrückungsregel aus.
4. Wenn Sie mit dem Hinzufügen von Kriterien fertig sind, geben Sie einen Namen für die Regel und optional eine Beschreibung ein.
5. Wählen Sie Save rule (Regel speichern). Amazon Inspector wendet sofort die neue Unterdrückungsregel an und verbirgt alle Ergebnisse, die den Kriterien entsprechen.

Unterdrückte Ergebnisse anzeigen

Standardmäßig zeigt Amazon Inspector keine unterdrückten Ergebnisse in der Amazon Inspector Inspector-Konsole an. Sie können sich jedoch die Ergebnisse ansehen, die durch eine bestimmte Regel unterdrückt wurden.

Um unterdrückte Ergebnisse anzuzeigen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich die Option Unterdrückungsregeln aus.
3. Wählen Sie in der Liste der Unterdrückungsregeln den Titel der Regel aus.

Unterdrückungsregeln ändern

Sie können jederzeit Änderungen an den Unterdrückungsregeln vornehmen.

Um die Unterdrückungsregeln zu ändern

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home
2. Wählen Sie im Navigationsbereich die Option Unterdrückungsregeln aus.
3. Wählen Sie den Titel der Unterdrückungsregel aus, die Sie ändern möchten.
4. Nehmen Sie die gewünschten Änderungen vor und wählen Sie dann Speichern, um die Regel zu aktualisieren.

Löschen von Unterdrückungsregeln

Sie können Unterdrückungsregeln löschen. Wenn Sie eine Unterdrückungsregel löschen, beendet Amazon Inspector die Unterdrückung neuer und vorhandener Ergebnisse, die die Regelkriterien erfüllen und nicht durch andere Regeln unterdrückt werden.

Nachdem Sie eine Unterdrückungsregel gelöscht haben, haben neue und bestehende Ergebnisse, die die Kriterien der Regel erfüllen, den Status Aktiv. Das bedeutet, dass sie standardmäßig auf der Amazon Inspector Inspector-Konsole angezeigt werden. Darüber hinaus veröffentlicht Amazon Inspector diese Ergebnisse im EventBridge Rahmen von Veranstaltungen an AWS Security Hub und Amazon.

Um eine Unterdrückungsregel zu löschen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich die Option Unterdrückungsregeln aus.

3. Aktivieren Sie das Kontrollkästchen neben dem Titel der Unterdrückungsregel, die Sie löschen möchten.
4. Wählen Sie Löschen und bestätigen Sie dann Ihre Auswahl, um die Regel dauerhaft zu löschen.

Ergebnisberichte aus Amazon Inspector exportieren

Zusätzlich zum Senden von Ergebnissen an Amazon EventBridge und AWS Security Hub können Sie die Ergebnisse optional als Ergebnisbericht in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportieren. Ein Ergebnisbericht ist eine CSV- oder JSON-Datei, die die Details der Ergebnisse enthält, die Sie in den Bericht aufnehmen möchten. Er bietet eine detaillierte Momentaufnahme Ihrer Ergebnisse zu einem bestimmten Zeitpunkt. Für jedes Ergebnis enthält die Datei Details wie den Amazon-Ressourcennamen (ARN) der betroffenen Ressource, Datum und Uhrzeit der Erstellung des Ergebnisses, die zugehörige CVE-ID (Common Vulnerabilities and Exposures) sowie den Schweregrad, den Status und die Amazon Inspector- und CVSS-Werte des Ergebnisses.

Wenn Sie einen Ergebnisbericht konfigurieren, geben Sie zunächst an, welche Ergebnisse in den Bericht aufgenommen werden sollen. Standardmäßig enthält Amazon Inspector Daten für alle Ihre Ergebnisse in der aktuellen Version AWS-Region , die den Status Aktiv haben. Wenn Sie der delegierte Amazon Inspector-Administrator für eine Organisation sind, umfasst dies Ergebnisdaten für alle Mitgliedskonten in Ihrer Organisation.

Sie können einen Bericht optional anpassen, indem Sie die Daten filtern. Mithilfe von Filtern können Sie Daten für Ergebnisse mit bestimmten Merkmalen ein- oder ausschließen, z. B. alle kritischen Ergebnisse, die in einem bestimmten Zeitraum erstellt wurden, alle aktiven Ergebnisse für eine bestimmte Ressource oder alle kritischen Ergebnisse eines bestimmten Typs. Wenn Sie der Amazon Inspector-Administrator für eine Organisation sind, können Sie Filter verwenden, um einen Bericht zu erstellen, der Ergebnisse für eine bestimmte Person AWS-Konto in Ihrer Organisation enthält, z. B. alle kritischen Ergebnisse eines Kontos, die den Status Aktiv haben und für die eine Lösung verfügbar ist. Sie können den Bericht dann zur Behebung an den Kontoinhaber weitergeben.

> **Note**
>
> Wenn Sie einen Ergebnisbericht mithilfe der CreateFindingsReportAPI exportieren, werden Ihnen standardmäßig nur aktive Ergebnisse angezeigt. Um unterdrückte oder

geschlossene Ergebnisse zu sehen, müssen Sie `SUPPRESSED` oder `CLOSED` als Werte für die FindingStatus-Filterkriterien angeben.

Wenn Sie einen Ergebnisbericht exportieren, verschlüsselt Amazon Inspector die Daten mit einem Schlüssel AWS Key Management Service (AWS KMS), den Sie angeben, und fügt den Bericht einem S3-Bucket hinzu, den Sie ebenfalls angeben. Der Verschlüsselungsschlüssel muss ein vom Kunden verwalteter, AWS Key Management Service (AWS KMS) symmetrischer Verschlüsselungsschlüssel sein, der in der aktuellen Version enthalten ist. AWS-Region Darüber hinaus muss die Schlüsselrichtlinie Amazon Inspector die Verwendung des Schlüssels ermöglichen. Der S3-Bucket muss sich auch in der aktuellen Region befinden, und die Bucket-Richtlinie muss es Amazon Inspector ermöglichen, Objekte zum Bucket hinzuzufügen.

Nachdem Amazon Inspector die Verschlüsselung und Speicherung Ihres Berichts abgeschlossen hat, können Sie den Bericht aus dem von Ihnen angegebenen S3-Bucket herunterladen oder an einen anderen Speicherort verschieben. Alternativ können Sie den Bericht im selben S3-Bucket speichern und diesen Bucket als Repository für Ergebnisberichte verwenden, die Sie anschließend exportieren.

Dieses Thema führt Sie durch den Prozess, mit dem AWS Management Console Sie einen Ergebnisbericht exportieren können. Der Prozess besteht darin, zu überprüfen, ob Sie über die erforderlichen Berechtigungen verfügen, die benötigten Ressourcen zu konfigurieren und anschließend den Bericht zu konfigurieren und zu exportieren.

> **Note**
>
> Sie können jeweils nur einen Ergebnisbericht exportieren. Wenn gerade ein Export ausgeführt wird, warten Sie, bis der Export abgeschlossen ist, bevor Sie versuchen, einen weiteren Bericht zu exportieren.

Aufgaben

- Schritt 1: Überprüfen Sie Ihre Berechtigungen
- Schritt 2: Konfigurieren Sie einen S3-Bucket
- Schritt 3: Konfigurieren Sie eine AWS KMS key
- Schritt 4: Konfigurieren und exportieren Sie einen Ergebnisbericht
- Beheben Sie Exportfehler

Nachdem Sie einen Ergebnisbericht zum ersten Mal exportiert haben, können die Schritte 1—3 optional sein. Dies hängt in erster Linie davon ab, ob Sie denselben S3-Bucket und AWS KMS key für nachfolgende Berichte verwenden möchten.

Wenn Sie es vorziehen, einen Bericht nach den Schritten 1—3 programmgesteuert zu exportieren, verwenden Sie den CreateFindingsReportBetrieb der Amazon Inspector API.

Schritt 1: Überprüfen Sie Ihre Berechtigungen

Bevor Sie einen Ergebnisbericht aus Amazon Inspector exportieren, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um sowohl Ergebnisberichte zu exportieren als auch Ressourcen für die Verschlüsselung und Speicherung der Berichte zu konfigurieren. Um Ihre Berechtigungen zu überprüfen, verwenden Sie AWS Identity and Access Management (IAM), um die IAM-Richtlinien zu überprüfen, die mit Ihrer IAM-Identität verknüpft sind. Vergleichen Sie dann die Informationen in diesen Richtlinien mit der folgenden Liste von Aktionen, die Sie ausführen dürfen müssen, um einen Ergebnisbericht zu exportieren.

Amazon Inspector

Stellen Sie für Amazon Inspector sicher, dass Sie die folgenden Aktionen ausführen dürfen:

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

Diese Aktionen ermöglichen es Ihnen, Ergebnisdaten für Ihr Konto abzurufen und diese Daten in Ergebnisberichten zu exportieren.

Wenn Sie planen, umfangreiche Berichte programmgesteuert zu exportieren, können Sie auch überprüfen, ob Sie die folgenden Aktionen ausführen dürfen:`inspector2:GetFindingsReportStatus`, um den Status von Berichten zu überprüfen und`inspector2:CancelFindingsReport`, um laufende Exporte abzubrechen.

AWS KMS

Stellen Sie sicher AWS KMS, dass Sie die folgenden Aktionen ausführen dürfen:

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

Mit diesen Aktionen können Sie die Schlüsselrichtlinie für das abrufen und aktualisieren AWS KMS key , das Amazon Inspector zur Verschlüsselung Ihres Berichts verwenden soll.

Um die Amazon Inspector Inspector-Konsole zum Exportieren eines Berichts zu verwenden, stellen Sie außerdem sicher, dass Sie die folgenden AWS KMS Aktionen ausführen dürfen:

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

Diese Aktionen ermöglichen es Ihnen, Informationen über das AWS KMS keys für Ihr Konto abzurufen und anzuzeigen. Sie können dann einen dieser Schlüssel auswählen, um Ihren Bericht zu verschlüsseln.

Wenn Sie vorhaben, einen neuen KMS-Schlüssel für die Verschlüsselung Ihres Berichts zu erstellen, müssen Sie auch berechtigt sein, die `kms:CreateKey` Aktion auszuführen.

Amazon S3

Stellen Sie für Amazon S3 sicher, dass Sie die folgenden Aktionen ausführen dürfen:

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

Mit diesen Aktionen können Sie den S3-Bucket erstellen und konfigurieren, in dem Amazon Inspector Ihren Bericht speichern soll. Sie ermöglichen Ihnen auch das Hinzufügen und Löschen von Objekten aus dem Bucket.

Wenn Sie planen, Ihren Bericht mit der Amazon Inspector Inspector-Konsole zu exportieren, überprüfen Sie auch, ob Sie die `s3:ListAllMyBuckets` `s3:GetBucketLocation` Aktionen ausführen dürfen. Mit diesen Aktionen können Sie Informationen zu den S3-Buckets für Ihr Konto abrufen und anzeigen. Sie können dann einen dieser Buckets auswählen, um den Bericht zu speichern.

Wenn Sie eine oder mehrere der erforderlichen Aktionen nicht ausführen dürfen, bitten Sie Ihren AWS Administrator um Unterstützung, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2: Konfigurieren Sie einen S3-Bucket

Nachdem Sie Ihre Berechtigungen überprüft haben, können Sie den S3-Bucket konfigurieren, in dem Sie Ihren Ergebnisbericht speichern möchten. Dabei kann es sich um einen vorhandenen Bucket für Ihr eigenes Konto oder um einen vorhandenen Bucket handeln, der einem anderen gehört AWS-Konto und auf den Sie zugreifen dürfen. Wenn Sie Ihren Bericht in einem neuen Bucket speichern möchten, erstellen Sie den Bucket, bevor Sie fortfahren.

Der S3-Bucket muss sich im selben AWS-Region Verzeichnis befinden wie die Ergebnisdaten, die Sie exportieren möchten. Wenn Sie beispielsweise Amazon Inspector in der Region USA Ost (Nord-Virginia) verwenden und Ergebnisdaten für diese Region exportieren möchten, muss sich der Bucket auch in der Region USA Ost (Nord-Virginia) befinden.

Darüber hinaus muss die Richtlinie des Buckets Amazon Inspector das Hinzufügen von Objekten zum Bucket ermöglichen. In diesem Thema wird erklärt, wie die Bucket-Richtlinie aktualisiert wird, und es gibt ein Beispiel für die Anweisung, die der Richtlinie hinzugefügt werden soll. Ausführliche Informationen zum Hinzufügen und Aktualisieren von Bucket-Richtlinien finden Sie unter Verwenden von Bucket-Richtlinien im Amazon Simple Storage Service-Benutzerhandbuch.

Wenn Sie Ihren Bericht in einem S3-Bucket speichern möchten, der einem anderen Konto gehört, arbeiten Sie mit dem Besitzer des Buckets zusammen, um die Richtlinie des Buckets zu aktualisieren. Rufen Sie auch den URI für den Bucket ab. Sie müssen diesen URI eingeben, wenn Sie Ihren Bericht exportieren.

Um die Bucket-Richtlinie zu aktualisieren

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3.
2. Wählen Sie im Navigationsbereich die Option Buckets aus.
3. Wählen Sie den S3-Bucket aus, in dem Sie den Ergebnisbericht speichern möchten.
4. Wählen Sie die Registerkarte Berechtigungen.
5. Wählen Sie im Abschnitt Bucket-Richtlinie die Option Bearbeiten aus.
6. Kopieren Sie die folgende Beispielanweisung in Ihre Zwischenablage:

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

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

7. Fügen Sie im Bucket-Policy-Editor auf der Amazon S3 S3-Konsole die vorherige Anweisung in die Richtlinie ein, um sie der Richtlinie hinzuzufügen.

   Wenn Sie die Anweisung hinzufügen, stellen Sie sicher, dass die Syntax gültig ist. Bucket-Richtlinien verwenden das JSON-Format. Das bedeutet, dass Sie vor oder nach der Anweisung ein Komma hinzufügen müssen, je nachdem, wo Sie die Anweisung zur Richtlinie hinzufügen. Wenn Sie die Anweisung als letzte Anweisung hinzufügen, fügen Sie hinter der schließenden Klammer für die vorhergehende Anweisung ein Komma hinzu. Wenn Sie sie als erste Anweisung oder zwischen zwei vorhandenen Anweisungen hinzufügen, fügen Sie hinter der schließenden Klammer für die Anweisung ein Komma ein.

8. Aktualisieren Sie die Anweisung mit den richtigen Werten für Ihre Umgebung, wobei:

   - *DOC-EXAMPLE-BUCKET ist der Name des Buckets*.
   - *111122223333* ist die Konto-ID für Sie. AWS-Konto
   - *Region* ist die Region, AWS-Region in der Sie Amazon Inspector verwenden und Amazon Inspector erlauben möchten, Berichte zum Bucket hinzuzufügen. Zum Beispiel `us-east-1` für die Region USA Ost (Nord-Virginia).

> **Note**
>
> Wenn Sie Amazon Inspector in einem manuell aktivierten System verwenden AWS-Region, fügen Sie dem Wert für das `Service` Feld auch den entsprechenden Regionalcode hinzu. Dieses Feld gibt den Amazon Inspector Service Principal an. Wenn Sie beispielsweise Amazon Inspector in der Region Naher Osten (Bahrain) verwenden, die den Regionalcode hat`me-south-1`, `inspector2.amazonaws.com` ersetzen Sie ihn `inspector2.me-south-1.amazonaws.com` in der Anweisung durch.

Beachten Sie, dass die Beispielanweisung Bedingungen definiert, die zwei globale IAM-Bedingungsschlüssel verwenden:

- aws: SourceAccount — Diese Bedingung ermöglicht es Amazon Inspector, dem Bucket Berichte nur für Ihr Konto hinzuzufügen. Es verhindert, dass Amazon Inspector dem Bucket Berichte für andere Konten hinzufügt. Genauer gesagt gibt die Bedingung an, welches Konto den Bucket für die in der `aws:SourceArn` Bedingung angegebenen Ressourcen und Aktionen verwenden kann.

  Um Berichte für weitere Konten im Bucket zu speichern, fügen Sie dieser Bedingung die Konto-ID für jedes weitere Konto hinzu. Beispielsweise:

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

- aws: SourceArn — Diese Bedingung schränkt den Zugriff auf den Bucket basierend auf der Quelle der Objekte ein, die dem Bucket hinzugefügt werden. Sie verhindert, dass andere AWS-Services Objekte zum Bucket hinzufügen. Es verhindert auch, dass Amazon Inspector Objekte zum Bucket hinzufügt und gleichzeitig andere Aktionen für Ihr Konto ausführt. Genauer gesagt erlaubt die Bedingung Amazon Inspector, Objekte nur dann zum Bucket hinzuzufügen, wenn es sich bei den Objekten um Ergebnisberichte handelt, und nur, wenn diese Berichte von dem Konto und in der Region erstellt wurden, die in der Bedingung angegeben sind.

  Damit Amazon Inspector die angegebenen Aktionen für weitere Konten ausführen kann, fügen Sie Amazon Resource Names (ARNs) für jedes weitere Konto zu dieser Bedingung hinzu. Beispielsweise:

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

Die in den `aws:SourceArn` Bedingungen `aws:SourceAccount` und angegebenen Konten müssen übereinstimmen.

Beide Bedingungen verhindern, dass Amazon Inspector bei Transaktionen mit Amazon S3 als verwirrter Stellvertreter eingesetzt wird. Obwohl wir dies nicht empfehlen, können Sie diese Bedingungen aus der Bucket-Richtlinie entfernen.

9. Wenn Sie mit der Aktualisierung der Bucket-Richtlinie fertig sind, wählen Sie Änderungen speichern aus.

Schritt 3: Konfigurieren Sie eine AWS KMS key

Nachdem Sie Ihre Berechtigungen überprüft und den S3-Bucket konfiguriert haben, legen AWS KMS key Sie fest, welchen Code Amazon Inspector zur Verschlüsselung Ihres Ergebnisberichts verwenden soll. Bei dem Schlüssel muss es sich um einen vom Kunden verwalteten KMS-Schlüssel mit symmetrischer Verschlüsselung handeln. Darüber hinaus muss sich der Schlüssel in demselben AWS-Region S3-Bucket befinden, den Sie zum Speichern des Berichts konfiguriert haben.

Der Schlüssel kann ein vorhandener KMS-Schlüssel aus Ihrem eigenen Konto oder ein vorhandener KMS-Schlüssel sein, den ein anderes Konto besitzt. Wenn Sie einen neuen KMS-Schlüssel verwenden möchten, erstellen Sie den Schlüssel, bevor Sie fortfahren. Wenn Sie einen vorhandenen Schlüssel verwenden möchten, der einem anderen Konto gehört, rufen Sie den Amazon-Ressourcennamen (ARN) des Schlüssels ab. Sie müssen diesen ARN eingeben, wenn Sie Ihren Bericht aus Amazon Inspector exportieren. Informationen zum Erstellen und Überprüfen der Einstellungen für KMS-Schlüssel finden Sie unter Schlüssel verwalten im AWS Key Management Service Entwicklerhandbuch.

Nachdem Sie festgelegt haben, welchen KMS-Schlüssel Sie verwenden möchten, erteilen Sie Amazon Inspector die Erlaubnis, den Schlüssel zu verwenden. Andernfalls kann Amazon Inspector den Bericht nicht verschlüsseln und exportieren. Um Amazon Inspector die Erlaubnis zur Verwendung des Schlüssels zu erteilen, aktualisieren Sie die Schlüsselrichtlinie für den Schlüssel.

Ausführliche Informationen zu wichtigen Richtlinien und zur Verwaltung des Zugriffs auf KMS-Schlüssel finden Sie unter Wichtige Richtlinien AWS KMS im AWS Key Management Service Entwicklerhandbuch.

So aktualisieren Sie die Schlüsselrichtlinie

> **Note**
>
> Das folgende Verfahren dient der Aktualisierung eines vorhandenen Schlüssels, damit Amazon Inspector ihn verwenden kann. Falls Sie noch nicht über einen vorhandenen Schlüssel verfügen, finden Sie eine Anleitung https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html zur Erstellung eines Schlüssels.

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.
4. Wählen Sie den KMS-Schlüssel aus, den Sie zum Verschlüsseln des Berichts verwenden möchten. Der Schlüssel muss ein symmetrischer Verschlüsselungsschlüssel (SYMMETRIC_DEFAULT) sein.
5. Wählen Sie auf der Registerkarte Schlüsselrichtlinie die Option Bearbeiten aus. Wenn Sie keine wichtige Richtlinie mit der Schaltfläche Bearbeiten sehen, müssen Sie zuerst Zur Richtlinienansicht wechseln auswählen.
6. Kopieren Sie die folgende Beispielanweisung in Ihre Zwischenablage:

```
{
    "Sid": "Allow Amazon Inspector to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
```

```
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
        }
    }
}
```

7. Fügen Sie im Editor für Schlüsselrichtlinien auf der AWS KMS Konsole die vorherige Anweisung in die Schlüsselrichtlinie ein, um sie der Richtlinie hinzuzufügen.

   Stellen Sie beim Hinzufügen der Anweisung sicher, dass die Syntax gültig ist. Wichtige Richtlinien verwenden das JSON-Format. Das bedeutet, dass Sie vor oder nach der Anweisung ein Komma hinzufügen müssen, je nachdem, wo Sie die Anweisung zur Richtlinie hinzufügen. Wenn Sie die Anweisung als letzte Anweisung hinzufügen, fügen Sie hinter der schließenden Klammer für die vorhergehende Anweisung ein Komma hinzu. Wenn Sie sie als erste Anweisung oder zwischen zwei vorhandenen Anweisungen hinzufügen, fügen Sie hinter der schließenden Klammer für die Anweisung ein Komma ein.

8. Aktualisieren Sie die Anweisung mit den richtigen Werten für Ihre Umgebung, wobei:

   - *111122223333* ist die Konto-ID für Ihr. AWS-Konto
   - *Region* ist die Region, AWS-Region in der Sie Amazon Inspector erlauben möchten, Berichte mit dem Schlüssel zu verschlüsseln. Zum Beispiel `us-east-1` für die Region USA Ost (Nord-Virginia).

   > **Note**
   >
   > Wenn Sie Amazon Inspector in einem manuell aktivierten System verwenden AWS-Region, fügen Sie dem Wert für das `Service` Feld auch den entsprechenden Regionalcode hinzu. Wenn Sie beispielsweise Amazon Inspector in der Region Naher Osten (Bahrain) verwenden, `inspector2.amazonaws.com` ersetzen Sie es durch`inspector2.me-south-1.amazonaws.com`.

   Wie die Beispielanweisung für die Bucket-Richtlinie im vorherigen Schritt verwenden die `Condition` Felder in diesem Beispiel zwei globale IAM-Bedingungsschlüssel:

- aws: SourceAccount — Diese Bedingung ermöglicht es Amazon Inspector, die angegebenen Aktionen nur für Ihr Konto durchzuführen. Insbesondere bestimmt sie, welches Konto die angegebenen Aktionen für die in der `aws:SourceArn` Bedingung angegebenen Ressourcen und Aktionen ausführen kann.

  Damit Amazon Inspector die angegebenen Aktionen für weitere Konten ausführen kann, fügen Sie dieser Bedingung die Konto-ID für jedes weitere Konto hinzu. Beispielsweise:

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

- aws: SourceArn — Diese Bedingung verhindert, dass andere AWS-Services die angegebenen Aktionen ausführen. Außerdem wird verhindert, dass Amazon Inspector den Schlüssel verwendet, während andere Aktionen für Ihr Konto ausgeführt werden. Mit anderen Worten, es ermöglicht Amazon Inspector, S3-Objekte nur dann mit dem Schlüssel zu verschlüsseln, wenn es sich bei den Objekten um Ergebnisberichte handelt, und nur wenn diese Berichte von dem Konto und in der Region erstellt wurden, die in der Bedingung angegeben sind.

  Damit Amazon Inspector die angegebenen Aktionen für weitere Konten ausführen kann, fügen Sie dieser Bedingung ARNs für jedes weitere Konto hinzu. Beispielsweise:

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:us-east-1:111122223333:report/*",
      "arn:aws:inspector2:us-east-1:444455556666:report/*",
      "arn:aws:inspector2:us-east-1:123456789012:report/*"
  ]
  ```

  Die in den `aws:SourceArn` Bedingungen `aws:SourceAccount` und angegebenen Konten müssen übereinstimmen.

Diese Bedingungen verhindern, dass Amazon Inspector bei Transaktionen mit als verwirrter Stellvertreter eingesetzt wird AWS KMS. Wir empfehlen dies zwar nicht, Sie können diese Bedingungen jedoch aus der Erklärung entfernen.

9. Wenn Sie mit der Aktualisierung der wichtigsten Richtlinie fertig sind, wählen Sie Änderungen speichern.

Schritt 4: Konfigurieren und exportieren Sie einen Ergebnisbericht

Nachdem Sie Ihre Berechtigungen überprüft und Ressourcen zum Verschlüsseln und Speichern Ihres Ergebnisberichts konfiguriert haben, können Sie den Bericht konfigurieren und exportieren.

Um einen Ergebnisbericht zu konfigurieren und zu exportieren

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich unter Ergebnisse die Option Alle Ergebnisse aus.
3. (Optional) Fügen Sie mithilfe der Filterleiste über der Tabelle Ergebnisse Filterkriterien hinzu, die angeben, welche Ergebnisse in den Bericht aufgenommen werden sollen. Wenn Sie Kriterien hinzufügen, aktualisiert Amazon Inspector die Tabelle, sodass sie nur die Ergebnisse enthält, die den Kriterien entsprechen. Die Tabelle bietet eine Vorschau der Daten, die Ihr Bericht enthalten wird.

   > **Note**
   >
   > Wir empfehlen, dass Sie Filterkriterien hinzufügen. Wenn Sie dies nicht tun, enthält der Bericht Daten für alle Ihre aktuellen Ergebnisse AWS-Region , die den Status Aktiv haben. Wenn Sie der Amazon Inspector-Administrator für eine Organisation sind, umfasst dies Ergebnisdaten für alle Mitgliedskonten in Ihrer Organisation.
   > Wenn ein Bericht Daten für alle oder viele Ergebnisse enthält, kann es sehr lange dauern, den Bericht zu erstellen und zu exportieren, und Sie können jeweils nur einen Bericht exportieren.

4. Wählen Sie Ergebnisse exportieren aus.
5. Geben Sie im Abschnitt Exporteinstellungen für Exportdateityp ein Dateiformat für den Bericht an:

   - Um eine JavaScript Objektnotationsdatei (.json) zu erstellen, die die Daten enthält, wählen Sie JSON aus.

     Wenn Sie die JSON-Option wählen, enthält der Bericht alle Felder für jedes Ergebnis. Eine Liste möglicher JSON-Felder finden Sie unter Finding data type in der Amazon Inspector API-Referenz.
   - Um eine Datei mit kommagetrennten Werten (.csv) zu erstellen, die die Daten enthält, wählen Sie CSV.

Wenn Sie die CSV-Option wählen, enthält der Bericht nur eine Teilmenge der Felder für jedes Ergebnis, d. h. ungefähr 45 Felder, die die wichtigsten Attribute eines Ergebnisses angeben. Zu den Feldern gehören: Befundtyp, Titel, Schweregrad, Status, Beschreibung, Zuerst gesehen, Zuletzt gesehen, Korrektur verfügbar, AWS Konto-ID, Ressourcen-ID, Ressourcen-Tags und Problembehebung. Diese Felder ergänzen die Felder, in denen Bewertungsdetails und Referenz-URLs für jedes Ergebnis erfasst werden. Im Folgenden finden Sie ein Beispiel für die CSV-Header in einem Ergebnisbericht:

AWS Konto ID [illegible] gefunden [illegible] ID für Container [illegible] Package [illegible] Vektor [illegible] ID [illegible] des Anbieters [illegible]

6. Geben Sie unter Exportort für S3-URI den S3-Bucket an, in dem Sie den Bericht speichern möchten:

   - Um den Bericht in einem Bucket zu speichern, der Ihrem Konto gehört, wählen Sie Browse S3 aus. Amazon Inspector zeigt eine Tabelle der S3-Buckets für Ihr Konto an. Wählen Sie die Zeile für den gewünschten Bucket aus und klicken Sie dann auf Auswählen.

> Tip
>
> Um auch ein Amazon S3 S3-Pfadpräfix für den Bericht anzugeben, fügen Sie einen Schrägstrich (/) und das Präfix an den Wert im Feld S3-URI an. Amazon Inspector fügt dann das Präfix hinzu, wenn der Bericht dem Bucket hinzugefügt wird, und Amazon S3 generiert den durch das Präfix angegebenen Pfad.
> Wenn Sie beispielsweise Ihre AWS-Konto ID als Präfix verwenden möchten und Ihre Konto-ID 111122223333 lautet, fügen Sie sie an den Wert im Feld **`/111122223333`** S3-URI an.
> Ein Präfix ähnelt einem Verzeichnispfad innerhalb eines S3-Buckets. Es ermöglicht Ihnen, ähnliche Objekte in einem Bucket zu gruppieren, ähnlich wie Sie ähnliche Dateien zusammen in einem Ordner auf einem Dateisystem speichern könnten.
> Weitere Informationen finden Sie unter Organisieren von Objekten in der Amazon S3 S3-Konsole mithilfe von Ordnern im Amazon Simple Storage Service-Benutzerhandbuch.

- Um den Bericht in einem Bucket zu speichern, der einem anderen Konto gehört, geben Sie den URI für den Bucket ein — zum Beispiel**`s3://DOC-EXAMPLE_BUCKET`**, wobei DOC-EXAMPLE_BUCKET der Name des Buckets ist. Der Bucket-Besitzer kann diese Informationen für Sie in den Eigenschaften des Buckets finden.

7. Geben Sie für den KMS-Schlüssel den an AWS KMS key , den Sie zum Verschlüsseln des Berichts verwenden möchten:

   - Um einen Schlüssel aus Ihrem eigenen Konto zu verwenden, wählen Sie den Schlüssel aus der Liste aus. In der Liste werden vom Kunden verwaltete KMS-Schlüssel mit symmetrischer Verschlüsselung für Ihr Konto angezeigt.
   - Um einen Schlüssel zu verwenden, der einem anderen Konto gehört, geben Sie den Amazon-Ressourcennamen (ARN) des Schlüssels ein. Der Schlüsselinhaber kann diese Informationen für Sie in den Eigenschaften des Schlüssels finden. Weitere Informationen finden Sie unter Suchen der Schlüssel-ID und des Schlüssel-ARN im AWS Key Management Service Entwicklerhandbuch.

8. Wählen Sie Export aus.

Amazon Inspector generiert den Ergebnisbericht, verschlüsselt ihn mit dem von Ihnen angegebenen KMS-Schlüssel und fügt ihn dem von Ihnen angegebenen S3-Bucket hinzu. Abhängig von der Anzahl der Ergebnisse, die Sie in den Bericht aufnehmen möchten, kann dieser Vorgang mehrere Minuten oder Stunden dauern. Wenn der Export abgeschlossen ist, zeigt Amazon Inspector eine Meldung an, dass Ihr Ergebnisbericht erfolgreich exportiert wurde. Wählen Sie optional Bericht anzeigen in der Nachricht, um zu dem Bericht in Amazon S3 zu navigieren.

Beachten Sie, dass Sie jeweils nur einen Bericht exportieren können. Wenn gerade ein Export ausgeführt wird, warten Sie, bis der Export abgeschlossen ist, bevor Sie versuchen, einen weiteren Bericht zu exportieren.

Beheben Sie Exportfehler

Wenn beim Versuch, einen Ergebnisbericht zu exportieren, ein Fehler auftritt, zeigt Amazon Inspector eine Meldung an, in der der Fehler beschrieben wird. Sie können die Informationen in diesem Thema als Leitfaden verwenden, um mögliche Ursachen und Lösungen für den Fehler zu ermitteln.

Stellen Sie beispielsweise sicher, dass sich der S3-Bucket im aktuellen Bucket befindet AWS-Region und die Bucket-Richtlinie Amazon Inspector erlaubt, Objekte zum Bucket hinzuzufügen. Stellen Sie

außerdem sicher, dass der in der aktuellen Region aktiviert AWS KMS key ist, und stellen Sie sicher, dass die Schlüsselrichtlinie Amazon Inspector die Verwendung des Schlüssels ermöglicht.

Nachdem Sie den Fehler behoben haben, versuchen Sie erneut, den Bericht zu exportieren.

Der Fehler kann nicht mehrere Berichte haben

Wenn Sie versuchen, einen Bericht zu erstellen, Amazon Inspector jedoch bereits einen Bericht generiert, erhalten Sie eine Fehlermeldung mit der Angabe Grund: Es können nicht mehrere Berichte in Bearbeitung sein. Dieser Fehler tritt auf, weil Amazon Inspector jeweils nur einen Bericht für ein Konto erstellen kann.

Um den Fehler zu beheben, können Sie warten, bis der andere Bericht abgeschlossen ist, oder ihn stornieren, bevor Sie einen neuen Bericht anfordern.

Sie können den Status eines Berichts überprüfen, indem Sie den GetFindingsReportStatusVorgang verwenden. Dieser Vorgang gibt die Berichts-ID jedes Berichts zurück, der gerade generiert wird.

Bei Bedarf können Sie mithilfe der `GetFindingsReportStatus` Operation die vom Vorgang angegebene Berichts-ID verwenden, um einen Export abzubrechen, der CancelFindingsReportgerade ausgeführt wird.

Erstellen von benutzerdefinierten Antworten auf Ergebnisse von Amazon Inspector mit Amazon EventBridge

Amazon Inspector erstellt ein Ereignis EventBridge für Amazon für neu generierte Ergebnisse, neu aggregierte Ergebnisse und Änderungen im Stand der Ergebnisse. Alles andere als eine Änderung der `lastObservedAt` Felder `updatedAt` und veröffentlicht ein neues Ereignis. Das bedeutet, dass neue Ereignisse für ein Ergebnis generiert werden, wenn Sie beispielsweise eine Ressource neu starten oder die mit einer Ressource verknüpften Tags ändern. Die Ergebnis-ID im `id` Feld bleibt jedoch dieselbe. Ereignisse werden auf die bestmögliche Weise ausgegeben.

> **Note**
>
> Wenn es sich bei Ihrem Konto um einen von Amazon Inspector delegierten Administrator handelt, werden Ereignisse in Ihrem Konto zusätzlich zu dem Mitgliedskonto, von dem sie stammen, EventBridge veröffentlicht.

Wenn Sie EventBridge Ereignisse mit Amazon Inspector verwenden, können Sie Aufgaben automatisieren, um auf Sicherheitsprobleme zu reagieren, die durch die Ergebnisse von Amazon Inspector aufgedeckt wurden.

Amazon Inspector sendet Ereignisse an den Standard-Event-Bus in derselben Region. Das bedeutet, dass Sie für jede Region, in der Sie Amazon Inspector ausführen, Ereignisregeln konfigurieren müssen, um Ereignisse für diese Region zu sehen.

Um Benachrichtigungen über Ergebnisse von Amazon Inspector auf der Grundlage von EventBridge Ereignissen zu erhalten, müssen Sie eine EventBridge Regel und ein Ziel für Amazon Inspector erstellen. Diese Regel EventBridge ermöglicht das Senden von Benachrichtigungen über Ergebnisse, die Amazon Inspector generiert, an das in der Regel angegebene Ziel. Weitere Informationen finden Sie unter EventBridgeAmazon-Regeln im EventBridge Amazon-Benutzerhandbuch.

Schema des Ereignisses

Im Folgenden finden Sie ein Beispiel für das Amazon Inspector Inspector-Ereignisformat für ein EC2-Suchereignis. Ein Beispiel für ein Schema anderer Such- und Ereignistypen finden Sie unterEventBridge Schema.

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
```

```
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-image-
aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
```

```
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```


Eine EventBridge Regel erstellen, um Sie über Ergebnisse von Amazon Inspector zu informieren

Um die Sichtbarkeit der Ergebnisse von Amazon Inspector EventBridge zu erhöhen, können Sie automatische Suchwarnungen einrichten, die an einen Messaging-Hub gesendet werden. In diesem Thema erfahren Sie, wie Sie Benachrichtigungen `CRITICAL` und `HIGH` Schweregrade per E-Mail, Slack oder Amazon Chime senden. Sie erfahren, wie Sie ein Amazon Simple Notification Service-Thema einrichten und dieses Thema dann mit einer EventBridge Ereignisregel verbinden.

Schritt 1. Ein Amazon SNS SNS-Thema und einen Endpunkt einrichten

Um automatische Benachrichtigungen einzurichten, müssen Sie zunächst ein Thema in Amazon Simple Notification Service einrichten und einen Endpunkt hinzufügen. Weitere Informationen finden Sie im SNS-Handbuch.

Dieses Verfahren legt fest, wohin Sie Amazon Inspector Inspector-Ergebnisdaten senden möchten. Das SNS-Thema kann während oder nach der Erstellung der EventBridge Ereignisregel zu einer Ereignisregel hinzugefügt werden.

Email setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Themen und dann Thema erstellen aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard aus. Geben Sie als Nächstes einen Themennamen ein, z. **`Inspector_to_Email`** B. Weitere Angaben sind optional.
4. Wählen Sie Create Topic (Thema erstellen) aus. Dadurch wird ein neues Fenster mit Details zu Ihrem neuen Thema geöffnet.
5. Wählen Sie im Abschnitt Abonnements die Option Abonnement erstellen aus.
6. a. Wählen Sie im Menü Protocol (Protokoll) die Option Email (E-Mail) aus.

   b. Geben Sie im Feld Endpoint die E-Mail-Adresse ein, an die Sie Benachrichtigungen erhalten möchten.

   > **Note**
   >
   > Nach der Erstellung des Abonnements müssen Sie Ihr Abonnement über Ihren E-Mail-Client bestätigen.

   c. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Suchen Sie in Ihrem Posteingang nach einer Abonnementnachricht und wählen Sie Abonnement bestätigen.

Slack setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Themen und dann Thema erstellen aus.

3. Wählen Sie im Abschnitt Thema erstellen die Option Standard aus. Geben Sie als Nächstes einen Themennamen ein, z. **`Inspector_to_Slack`** B. Weitere Angaben sind optional. Wählen Sie Thema erstellen, um die Endpunkterstellung abzuschließen.

Einen AWS Chatbot Client konfigurieren

1. Navigieren Sie zur AWS Chatbot Konsole unterhttps://console.aws.amazon.com/chatbot/.
2. Wählen Sie im Bereich Konfigurierte Clients die Option Neuen Client konfigurieren aus.
3. Wähle Slack und dann zur Bestätigung Configure.

> **Note**
>
> Wenn du Slack auswählst, musst du die Zugriffsberechtigungen für deinen Channel bestätigen AWS Chatbot , indem du Zulassen auswählst.

4. Wählen Sie Neuen Kanal konfigurieren aus, um den Bereich mit den Konfigurationsdetails zu öffnen.

   a. Geben Sie einen Namen für den Kanal ein.

   b. Wähle für den Slack-Kanal den Kanal aus, den du verwenden möchtest.

   c. Kopiere in Slack die Kanal-ID des privaten Channels, indem du mit der rechten Maustaste auf den Kanalnamen klickst und Link kopieren auswählst.

   d. Füge im AWS Chatbot Fenster die AWS Management Console Kanal-ID, die du aus Slack kopiert hast, in das Feld Private Channel-ID ein.

   e. Wähle unter Berechtigungen aus, ob du eine IAM-Rolle mithilfe einer Vorlage erstellen möchtest, falls du noch keine Rolle hast.

   f. Wählen Sie für Richtlinienvorlagen die Option Benachrichtigungsberechtigungen aus. Dies ist die IAM-Richtlinienvorlage für AWS Chatbot. Diese Richtlinie bietet die erforderlichen Lese- und Listenberechtigungen für CloudWatch Alarme, Ereignisse und Protokolle sowie für Amazon SNS SNS-Themen.

   g. Wählen Sie für Channel-Guardrail-Richtlinien die Option 2. AmazonInspector ReadOnlyAccess

   h. Wählen Sie die Region aus, in der Sie zuvor Ihr SNS-Thema erstellt haben, und wählen Sie dann das Amazon SNS SNS-Thema aus, das Sie erstellt haben, um Benachrichtigungen an den Slack-Kanal zu senden.

5. Wählen Sie Konfigurieren.

Amazon Chime setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Themen aus und wählen Sie dann Thema erstellen aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard aus. Geben Sie als Nächstes einen Themennamen ein, z. **`Inspector_to_Chime`** B. Weitere Angaben sind optional. Wählen Sie Thema erstellen, um den Vorgang abzuschließen.

Einen AWS Chatbot Client konfigurieren

1. Navigieren Sie zur AWS Chatbot Konsole unterhttps://console.aws.amazon.com/chatbot/.
2. Wählen Sie im Bereich Konfigurierte Clients die Option Neuen Client konfigurieren.
3. Wählen Sie Chime und anschließend zur Bestätigung Configure.
4. Geben Sie im Bereich mit den Konfigurationsdetails einen Namen für den Kanal ein.
5. Öffnen Sie in Amazon Chime den gewünschten Chatroom.
   a. Wählen Sie das Zahnradsymbol rechts oben und danach Manage webhooks and bots aus.
   b. Wählen Sie URL kopieren, um die Webhook-URL in Ihre Zwischenablage zu kopieren.
6. Fügen Sie im AWS Chatbot Fenster die URL ein, die Sie kopiert haben, in das Feld Webhook-URL. AWS Management Console
7. Wählen Sie unter Berechtigungen aus, ob Sie eine IAM-Rolle mithilfe einer Vorlage erstellen möchten, falls Sie noch keine Rolle haben.
8. Wählen Sie für Richtlinienvorlagen die Option Benachrichtigungsberechtigungen aus. Dies ist die IAM-Richtlinienvorlage für AWS Chatbot. Es bietet die erforderlichen Lese- und Listenberechtigungen für CloudWatch Alarme, Ereignisse und Protokolle sowie für Amazon SNS SNS-Themen.
9. Wählen Sie die Region aus, in der Sie zuvor Ihr SNS-Thema erstellt haben, und wählen Sie dann das Amazon SNS SNS-Thema aus, das Sie erstellt haben, um Benachrichtigungen an den Amazon Chime Chime-Raum zu senden.

10. Wählen Sie Konfigurieren.

Schritt 2. Eine EventBridge Regel für Amazon Inspector Inspector-Ergebnisse erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Regeln und dann Regel erstellen aus.
3. Geben Sie einen Namen und optional eine Beschreibung für Ihre Regel ein.
4. Wählen Sie Regel mit einem Ereignismuster und dann Weiter aus.
5. Wählen Sie im Bereich „Ereignismuster“ die Option Benutzerdefinierte Muster (JSON-Editor) aus.
6. Fügen Sie den folgenden JSON-Code in den Editor ein.

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

> **Note**
>
> Dieses Muster sendet Benachrichtigungen für alle von Amazon Inspector festgestellten aktiven `CRITICAL` oder `HIGH` schwerwiegenden Ergebnisse.

   Wählen Sie Weiter, wenn Sie mit der Eingabe des Ereignismusters fertig sind.

7. Wählen Sie auf der Seite Ziele auswählen die Option AWS-Service. Wählen Sie dann für Zieltyp auswählen die Option SNS-Thema aus.
8. Wählen Sie unter Thema den Namen des SNS-Themas aus, das Sie in Schritt 1 erstellt haben. Wählen Sie anschließend Weiter.
9. Fügen Sie bei Bedarf optionale Tags hinzu und wählen Sie Weiter.
10. Überprüfen Sie Ihre Regel und wählen Sie dann Regel erstellen aus.

EventBridge für Amazon Inspector Inspector-Umgebungen mit mehreren Konten

Wenn Sie ein delegierter Administrator von Amazon Inspector sind, werden auf Ihrem Konto EventBridge Regeln angezeigt, die auf den entsprechenden Ergebnissen Ihrer Mitgliedskonten basieren. Wenn Sie EventBridge in Ihrem Administratorkonto Benachrichtigungen über Ergebnisse einrichten, wie im vorherigen Abschnitt beschrieben, erhalten Sie Benachrichtigungen über mehrere Konten. Mit anderen Worten, Sie werden über Ergebnisse und Ereignisse informiert, die von Ihren Mitgliedskonten generiert wurden, zusätzlich zu den Ergebnissen und Ereignissen, die von Ihrem eigenen Konto generiert wurden.

Sie können die JSON-Details `accountId` aus den Ergebnissen verwenden, um das Mitgliedskonto zu identifizieren, von dem das Amazon Inspector Inspector-Ergebnis stammt.

Exportieren von SBOMs mit Amazon Inspector

Sie können die Amazon Inspector Inspector-Konsole oder API verwenden, um Software Bill of Materials (SBOM) für Ihre Ressourcen zu generieren. Eine SBOM ist ein verschachteltes Inventar aller Open-Source-Softwarekomponenten und Drittanbieter-Softwarekomponenten Ihrer Codebasis. Amazon Inspector stellt SBOMs für einzelne Ressourcen in Ihrer Umgebung bereit. Aus Amazon Inspector exportierte SBOMs können Ihnen helfen, Einblick in Informationen über Ihr Softwareangebot zu gewinnen, wie z. B. Ihre am häufigsten verwendeten Pakete und die damit verbundenen Sicherheitslücken in Ihrem Unternehmen.

Sie können SBOMs für alle unterstützten Ressourcen exportieren, die aktiv von Amazon Inspector überwacht werden. Sie können den Status Ihrer Ressourcen unter Bewertung der Abdeckung Ihrer AWS Umgebung durch Amazon Inspector überprüfen.

> **Note**
>
> Amazon Inspector unterstützt den Export von SBOM für Windows EC2-Instances nicht.

Amazon Inspector Inspector-Formate

Amazon Inspector unterstützt den Export von SBOMs in den mit CyclonedX 1.4 und SPDX 2.3 kompatiblen Formaten. Amazon Inspector exportiert SBOMs als `JSON` Dateien in den Amazon S3 S3-Bucket Ihrer Wahl.

> **Note**
>
> Exporte im SPDX-Format von Amazon Inspector sind mit Systemen kompatibel, die SPDX 2.3 verwenden, enthalten jedoch nicht das Feld Creative Commons Zero (CC0). Dies liegt daran, dass die Aufnahme dieses Felds es Benutzern ermöglichen würde, das Material weiterzuverteilen oder zu bearbeiten.

Beispiel für das CyclonedX 1.4 SBOM-Format von Amazon Inspector

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

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

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

Beispiel für das SPDX 2.3 SBOM-Format von Amazon Inspector


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

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

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


Filter für SBOMs

Wenn Sie SBOMs exportieren, können Sie Filter hinzufügen, um Berichte für bestimmte Teilmengen von Ressourcen zu erstellen. Wenn Sie keinen Filter angeben, werden die SBOMs für alle aktiven, unterstützten Ressourcen exportiert. Und wenn Sie ein delegierter Administrator sind, umfasst dies auch Ressourcen für alle Mitglieder. Die folgenden Filter sind verfügbar:

- AccountID — Dieser Filter kann verwendet werden, um SBOMs für alle Ressourcen zu exportieren, die mit einer bestimmten Konto-ID verknüpft sind.

- EC2-Instance-Tag — Dieser Filter kann verwendet werden, um SBOMs für EC2-Instances mit bestimmten Tags zu exportieren.
- Funktionsname — Dieser Filter kann verwendet werden, um SBOMs für bestimmte Lambda-Funktionen zu exportieren.
- Bild-Tag — Dieser Filter kann verwendet werden, um SBOMs für Container-Images mit bestimmten Tags zu exportieren.
- Lambda-Funktions-Tag — Dieser Filter kann verwendet werden, um SBOMs für Lambda-Funktionen mit bestimmten Tags zu exportieren.
- Ressourcentyp — Dieser Filter kann verwendet werden, um den Ressourcentyp zu filtern: EC2/ECR/Lambda.
- Ressourcen-ID — Dieser Filter kann verwendet werden, um eine SBOM für eine bestimmte Ressource zu exportieren.
- Repository-Name — Dieser Filter kann verwendet werden, um SBOMs für Container-Images in bestimmten Repositorys zu generieren.

SBOMs konfigurieren und exportieren

Um SBOMs zu exportieren, müssen Sie zuerst einen Amazon S3 S3-Bucket und einen AWS KMS Schlüssel konfigurieren, den Amazon Inspector verwenden darf. Sie können Filter verwenden, um SBOMs für bestimmte Teilmengen Ihrer Ressourcen zu exportieren. Um SBOMs für mehrere Konten in einer AWS Organisation zu exportieren, folgen Sie diesen Schritten, während Sie als delegierter Amazon Inspector-Administrator angemeldet sind.

Voraussetzungen

- Unterstützte Ressourcen, die aktiv von Amazon Inspector überwacht werden.
- Ein Amazon S3 S3-Bucket, der mit einer Richtlinie konfiguriert ist, die es Amazon Inspector ermöglicht, Objekte hinzuzufügen. Informationen zur Konfiguration der Richtlinie finden Sie unter Exportberechtigungen konfigurieren.
- Ein AWS KMS Schlüssel, der mit einer Richtlinie konfiguriert ist, die es Amazon Inspector ermöglicht, Ihre Berichte zu verschlüsseln. Informationen zur Konfiguration der Richtlinie finden Sie unter Einen AWS KMS Schlüssel für den Export konfigurieren.

> **Note**
>
> Wenn Sie zuvor einen Amazon S3 S3-Bucket und einen AWS KMS Schlüssel für den Ergebnisexport konfiguriert haben, können Sie denselben Bucket und Schlüssel für den SBOM-Export verwenden.

Wählen Sie Ihre bevorzugte Zugriffsmethode für den Export einer SBOM.

Console

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region mit den Ressourcen aus, für die Sie SBOM exportieren möchten.
3. Wählen Sie im Navigationsbereich die Option SBOMs exportieren aus.
4. (Optional) Verwenden Sie auf der Seite SBOMs exportieren das Menü Filter hinzufügen, um eine Teilmenge von Ressourcen auszuwählen, für die Berichte erstellt werden sollen. Wenn kein Filter angegeben ist, exportiert Amazon Inspector Berichte für alle aktiven Ressourcen. Wenn Sie ein delegierter Administrator sind, umfasst dies alle aktiven Ressourcen in Ihrer Organisation.
5. Wählen Sie unter Exporteinstellung das gewünschte Format für die SBOM aus.
6. Geben Sie eine Amazon S3-URI ein oder wählen Sie Amazon S3 durchsuchen, um einen Amazon S3 S3-Standort zum Speichern der SBOM auszuwählen.
7. Geben Sie einen AWS KMS Schlüssel ein, der für Amazon Inspector konfiguriert ist, um Ihre Berichte zu verschlüsseln.

API

- Verwenden Sie den CreateSbomExportBetrieb der Amazon Inspector Inspector-API, um SBOMs für Ihre Ressourcen programmgesteuert zu exportieren.

  Verwenden Sie in Ihrer Anfrage den `reportFormat` Parameter, um das SBOM-Ausgabeformat anzugeben, und wählen Sie oder. `CYCLONEDX_1_4` `SPDX_2_3` Der `s3Destination` Parameter ist erforderlich, und Sie müssen einen S3-Bucket angeben, der mit einer Richtlinie konfiguriert ist, die es Amazon Inspector ermöglicht, in diesen Bucket

zu schreiben. Verwenden Sie optional `resourceFilterCriteria` Parameter, um den Umfang des Berichts auf bestimmte Ressourcen zu beschränken.

AWS CLI

- AWS Command Line Interface Führen Sie den folgenden Befehl aus, um SBOMs für Ihre Ressourcen mit dem folgenden Befehl zu exportieren:

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

  Ersetzen Sie in Ihrer Anfrage *`FORMAT`* durch das Format Ihrer Wahl, `CYCLONEDX_1_4` oder`SPDX_2_3`. Ersetzen Sie dann das *`user input placeholders`*für das S3-Ziel durch den Namen des S3-Buckets, in den exportiert werden soll, das Präfix, das für die Ausgabe in S3 verwendet werden soll, und den ARN für den KMS-Schlüssel, den Sie zum Verschlüsseln der Berichte verwenden.

Suche in der Amazon Inspector Inspector-Schwachstellendatenbank

Sie können die Sicherheitslückendatenbank von Amazon Inspector nach Sicherheitslücken und Risiken (CVEs) durchsuchen. Amazon Inspector verwendet Informationen aus der Schwachstellendatenbank, um Details zu einer CVE-ID zu erstellen. Sie können auf einer CVE-Detailseite auf diese Details zugreifen.

In diesem Thema wird beschrieben, wie Sie die Amazon Inspector Inspector-Schwachstellendatenbank mithilfe einer CVE-ID durchsuchen und die CVE-Detailseite interpretieren. Informationen zu den Ergebnissen finden Sie unter. Amazon Inspector findet Einzelheiten

> **Note**
>
> Amazon Inspector verfolgt und erstellt Ergebnisse für andere Softwareschwachstellen in der Datenbank. Amazon Inspector unterstützt jedoch nur CVEs mit Plattformen, die im Abschnitt Erkennungsplattformen der CVE-Detailseite aufgeführt sind. Derzeit wird die CVE-Suche nicht unterstützt. Microsoft Windows

Die Schwachstellen-Datenbank wird durchsucht

In diesem Abschnitt wird beschrieben, wie Sie die Schwachstellendatenbank in der Konsole und mit der Amazon Inspector API durchsuchen.

> **Note**
>
> Sie müssen Amazon Inspector in Ihrem aktuellen System aktivieren, AWS-Region bevor Sie die Schwachstellendatenbank durchsuchen können.

Console

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/
2. Wählen Sie im Navigationsbereich die Option Vulnerability database search aus.

3. Geben Sie in der Suchleiste eine CVE-ID ein und wählen Sie Suchen aus.

API

Führen Sie die Amazon Inspector SearchVulnerabilitiesInspector-API aus und geben Sie eine einzelne CVE-ID wie `filterCriteria` im folgenden Format ein:`CVE-<year>-<ID>`.

CVE-Details verstehen

In diesem Abschnitt wird beschrieben, wie die CVE-Detailseite zu interpretieren ist.

CVE-Details

Der Abschnitt mit den CVE-Details enthält die folgenden Informationen:

- Beschreibung und ID des CVE
- CVE-Schweregrad
- Bewertungen des Common Vulnerability Scoring System (CVSS) und des Exploit Prediction Scoring System (EPSS)
- Plattformen zur Erkennung

> **Note**
>
> Wenn dieses Feld leer ist, unterstützt Amazon Inspector keine Erkennung für Ihre CVE-ID.

- Aufzählung der häufigsten Schwächen (CWE)
- Datum der Erstellung und Aktualisierung durch den Anbieter

Informationen zu Sicherheitslücken

Der Bereich Vulnerability Intelligence bietet Bedrohungsdaten wie Exploit-Ziele und das Datum des letzten bekannten öffentlichen Exploits.

Es enthält auch Daten der Cybersecurity and Infrastructure Security Agency (CISA), darunter die Abhilfemaßnahmen, das Datum, an dem das CVE in den Katalog der bekannten Sicherheitslücken aufgenommen wurde, und das Datum, zu dem die CISA erwartet, dass Bundesbehörden das CVE beheben werden.

Referenzen

Der Abschnitt „Referenzen“ enthält Links zu Ressourcen mit weiteren Informationen über das CVE.

EventBridge Amazon-Ereignisschema für Amazon Inspector-Ereignisse

Um die Integration mit anderen Anwendungen, Diensten und Systemen wie Überwachungs- oder Eventmanagementsystemen zu unterstützen, veröffentlicht Amazon Inspector die Ergebnisse automatisch EventBridge als Ereignisse an Amazon. EventBridgeist ein serverloser Event-Bus-Service, der einen Stream von Echtzeitdaten aus Anwendungen und anderen AWS-Services an Ziele wie AWS Lambda Funktionen, Amazon Simple Notification Service-Themen und Amazon Kinesis Data Streams übermittelt. Weitere Informationen EventBridge zu EventBridge Veranstaltungen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Amazon Inspector veröffentlicht Ereignisse zu Ergebnissen, Änderungen der Ressourcenabdeckung und erste Scans einzelner Ressourcen. Jedes Ereignis ist ein JSON-Objekt, das dem EventBridge Schema für AWS Ereignisse entspricht. Da die Daten als EventBridge Ereignis strukturiert sind, können Sie Ergebnisse und unterstützte Amazon Inspector Inspector-Ereignisse einfacher überwachen, verarbeiten und darauf reagieren, indem Sie andere Anwendungen, Dienste und Tools verwenden.

Themen

EventBridge Amazon-Basisschema für Amazon Inspector

Das Folgende ist ein Beispiel für das grundlegende Schema für ein EventBridge Ereignis für Amazon Inspector. Die Veranstaltungsdetails unterscheiden sich je nach Art des Ereignisses.

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

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

Beispiel für das Auffinden von Ereignissen in Amazon Inspector

Im Folgenden finden Sie ein Beispiel für das Schema für ein EventBridge Ereignis mit Ergebnissen von Amazon Inspector. Findungsereignisse werden ausgelöst, wenn Amazon Inspector eine Softwareschwachstelle oder ein Netzwerkproblem in einer Ihrer Ressourcen identifiziert. Eine Anleitung zum Erstellen von Benachrichtigungen als Reaktion auf diese Art von Ereignis finden Sie unterErstellen von benutzerdefinierten Antworten auf Ergebnisse von Amazon Inspector mit Amazon EventBridge.

Die folgenden Felder identifizieren ein Findereignis:

- Das `detail-type` Feld ist auf eingestelltInspector2 Finding.
- Das `detail` Objekt beschreibt den Befund.

Wählen Sie eine der Optionen aus, um die Suche nach Ereignisschemas für verschiedene Ressourcen und Suchtypen anzuzeigen.

Amazon EC2 package vulnerability finding

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

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

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


Amazon EC2 network reachability finding


```
{
```

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

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


Amazon ECR package vulnerability finding


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

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

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

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


Lambda package vulnerability finding


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

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

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

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

Lambda code vulnerability finding

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

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

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

> **Note**
>
> Der Detailwert gibt die JSON-Details eines einzelnen Ergebnisses als Objekt zurück. Es wird nicht die gesamte Syntax der Ergebnisantwort zurückgegeben, die mehrere Ergebnisse innerhalb eines Arrays unterstützt.

Beispiel für ein vollständiges Amazon Inspector Inspector-Ereignisschema für den ersten Scan

Im Folgenden finden Sie ein Beispiel für das EventBridge Ereignisschema für ein Amazon Inspector Inspector-Ereignis zum Abschluss eines ersten Scans. Dieses Ereignis wird ausgelöst, wenn Amazon Inspector einen ersten Scan einer Ihrer Ressourcen abschließt.

Die folgenden Felder kennzeichnen ein Ereignis, bei dem der erste Scan abgeschlossen wurde:

- Das `detail-type` Feld ist auf eingestelltInspector2 Scan.
- Das `detail` Objekt enthält ein `finding-severity-counts` Objekt, das die Anzahl der Ergebnisse in den jeweiligen Schweregradkategorien, wie, und,,,,CRITICAL,,,HIGH, detailliert beschreibtMEDIUM.

Wählen Sie eine der Optionen aus, um je nach Ressourcentyp unterschiedliche Ereignisschemas für den ersten Scan anzuzeigen.

Amazon EC2 instance initial scan

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

Amazon ECR image initial scan

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

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

Lambda function initial scan

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

```
  }
}
```

Beispiel für ein Amazon Inspector Inspector-Abdeckungsereignisschema

Im Folgenden finden Sie ein Beispiel für das EventBridge Ereignisschema für ein Amazon Inspector Inspector-Ereignis zur Berichterstattung. Dieses Ereignis wird ausgelöst, wenn die Scanabdeckung von Amazon Inspector für eine Ressource geändert wird. Die folgenden Felder kennzeichnen ein Abdeckungsereignis:

- Das `detail-type` Feld ist auf eingestelltInspector2 Coverage.
- Das `detail` Objekt enthält ein `scanStatus` Objekt, das den neuen Scanstatus für die Ressource angibt.

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

Integration von Amazon Inspector-Scans in Ihre CI/CD-Pipeline

Sie können Amazon Inspector Inspector-Container-Image-Scans direkt in Ihre CI/CD-Pipeline integrieren, um nach Softwareschwachstellen zu suchen und am Ende Ihres Builds Berichte bereitzustellen. Die von Amazon Inspector generierten Schwachstellenberichte ermöglichen es Ihnen, Risiken vor der Bereitstellung zu untersuchen und zu beheben.

Die Amazon Inspector CI/CD-Integration verwendet eine Kombination aus dem Amazon Inspector SBOM Generator und der Amazon Inspector Scan API, um Schwachstellenberichte für Ihre Container-Images zu erstellen. Der Amazon Inspector SBOM Generator erstellt eine Software-Stückliste (SBOM) aus einem bereitgestellten Container-Image. Anschließend scannt die Amazon Inspector Scan API diese Stückliste und erstellt einen Bericht mit Details zu allen erkannten Sicherheitslücken.

Sie können eine CI/CD-Integration mit Amazon Inspector über die Amazon Inspector-Plugins erreichen, die speziell für einzelne CI/CD-Lösungen entwickelt wurden und auf deren Marketplace erhältlich sind, oder Sie können Ihre eigene benutzerdefinierte Scan-Integration erstellen.

Themen

Plugin-Integration

Amazon Inspector bietet Plugins für unterstützte CI/CD-Lösungen. Sie können diese Plugins von ihren jeweiligen Marketplaces aus installieren und sie dann verwenden, um Amazon Inspector Scans als Build-Schritt in Ihre Pipeline aufzunehmen. Im Schritt zur Plugin-Erstellung wird der Amazon

Inspector SBOM-Generator auf dem von Ihnen bereitgestellten Bild ausgeführt und anschließend die Amazon Inspector Scan-API auf der generierten SBOM ausgeführt.

Im Folgenden finden Sie einen Überblick darüber, wie eine Amazon Inspector CI/CD-Integration über Plugins funktioniert:

1. Sie konfigurieren eine AWS-Konto , um den Zugriff auf die Amazon Inspector Scan API zu ermöglichen. Anweisungen finden Sie unter Einrichtung eines AWS Kontos für die Nutzung der Amazon Inspector CI/CD-Integration.
2. Sie installieren das Amazon Inspector-Plugin vom Marketplace.
3. Sie installieren und konfigurieren die Amazon Inspector SBOM Generator-Binärdatei. Anweisungen finden Sie unter Amazon Inspector SBOM-Generator.
4. Sie fügen Amazon Inspector Scans als Build-Schritt in Ihre CI/CD-Pipeline ein und konfigurieren den Scan.
5. Wenn Sie einen Build ausführen, verwendet das Plugin Ihr Container-Image als Eingabe und führt dann den Amazon Inspector SBOM Generator auf dem Image aus, um eine CycloneDX kompatible SBOM zu generieren.
6. Von dort aus sendet das Plugin die generierte SBOM an einen Amazon Inspector Scan API-Endpunkt, der jede SBOM-Komponente auf Sicherheitslücken überprüft.
7. Die Antwort der Amazon Inspector Scan API wird in einen Schwachstellenbericht in den Formaten CSV, SBOM, JSON und HTML umgewandelt. Der Bericht enthält Details zu allen Sicherheitslücken, die Amazon Inspector gefunden hat.

Unterstützte CI/CD-Lösungen

Amazon Inspector unterstützt derzeit die folgenden CI/CD-Lösungen. Vollständige Anweisungen zur Einrichtung der CI/CD-Integration mithilfe eines Plug-ins erhalten Sie, wenn Sie das Plug-in für Ihre CI/CD-Lösung auswählen:

- Jenkins-Plugin
- TeamCity-Plugin

Benutzerdefinierte Integration

Wenn Amazon Inspector keine Plug-ins für Ihre CI/CD-Lösung bereitstellt, können Sie mithilfe einer Kombination aus dem Amazon Inspector SBOM Generator und der Amazon Inspector Scan API

Ihre eigene benutzerdefinierte CI/CD-Integration erstellen. Sie können auch eine benutzerdefinierte Integration verwenden, um Scans mithilfe der im Amazon Inspector SBOM Generator verfügbaren Optionen zu optimieren.

Im Folgenden finden Sie einen Überblick darüber, wie eine benutzerdefinierte Amazon Inspector CI/CD-Integration funktioniert:

1. Sie konfigurieren eine AWS-Konto , um den Zugriff auf die Amazon Inspector Scan API zu ermöglichen. Anweisungen finden Sie unter Einrichtung eines AWS Kontos für die Nutzung der Amazon Inspector CI/CD-Integration.
2. Sie installieren und konfigurieren die Amazon Inspector SBOM Generator-Binärdatei. Anweisungen finden Sie unter Amazon Inspector SBOM-Generator.
3. Sie verwenden den Amazon Inspector SBOM Generator, um eine CycloneDX kompatible SBOM für Ihr Container-Image zu generieren.
4. Sie verwenden die Amazon Inspector Scan API für die generierte SBOM, um einen Schwachstellenbericht zu erstellen.

Anweisungen zum Einrichten einer benutzerdefinierten Integration finden Sie unter. Erstellen Sie Ihre eigene benutzerdefinierte CI/CD-Pipeline-Integration mit Amazon Inspector Scan

Einrichtung eines AWS Kontos für die Nutzung der Amazon Inspector CI/CD-Integration

Sie müssen sich für eine registrieren AWS-Konto , um die Amazon Inspector CI/CD-Integration nutzen zu können. Sie AWS-Konto müssen über eine IAM-Rolle verfügen, die Ihrer Pipeline Zugriff auf die Amazon Inspector Scan API gewährt.

Führen Sie die Aufgaben in den folgenden Themen aus, um sich für einen zu registrieren AWS-Konto, einen Administratorbenutzer zu erstellen und eine IAM-Rolle für die CI/CD-Integration zu konfigurieren.

> **Note**
>
> Wenn Sie sich bereits für eine angemeldet haben AWS-Konto, können Sie direkt zu. Konfigurieren Sie eine IAM-Rolle für die CI/CD-Integration

Themen

Melde dich für eine an AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Konfigurieren Sie eine IAM-Rolle für die CI/CD-Integration

Um Amazon Inspector-Scanning in Ihre CI/CD-Pipeline zu integrieren, müssen Sie eine IAM-Richtlinie erstellen, die den Zugriff auf die Amazon Inspector Scan API ermöglicht, die die Software-Stückliste (SBOMs) scannt. Anschließend können Sie diese Richtlinie einer IAM-Rolle zuordnen, die Ihr Konto für die Ausführung der Amazon Inspector Scan API übernehmen kann.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.

2. Wählen Sie im Navigationsbereich der IAM-Konsole Richtlinien und dann Richtlinie erstellen aus.
3. Wählen Sie im Policy-Editor JSON aus und fügen Sie die folgende Anweisung ein:

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

4. Wählen Sie Weiter aus.
5. Geben Sie der Richtlinie beispielsweise `InspectorCICDscan-policy` einen Namen und fügen Sie eine optionale Beschreibung hinzu. Wählen Sie dann Create Policy aus. Diese Richtlinie wird der Rolle angehängt, die Sie in den nächsten Schritten erstellen werden.
6. Wählen Sie im Navigationsbereich der IAM-Konsole Rollen und dann Neue Rolle erstellen aus.
7. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus und fügen Sie die folgende Richtlinie ein:

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

8. Wählen Sie Weiter aus.

9. Suchen Sie unter Berechtigungen hinzufügen nach der Richtlinie, die Sie zuvor erstellt haben, wählen Sie sie aus und klicken Sie dann auf Weiter.
10. Geben Sie der Rolle beispielsweise `InspectorCICDscan-role` einen Namen und fügen Sie eine optionale Beschreibung hinzu`Create Role`. Wählen Sie dann.

Amazon Inspector SBOM-Generator

Der Amazon Inspector SBOM Generator (Sbomgen) ist ein binäres Tool, das eine Software-Stückliste (SBOM) für ein Container-Image erstellt. Eine SBOM ist ein gesammeltes Inventar der auf einem System installierten Software.

Sbomgensucht nach Dateien, von denen bekannt ist, dass sie Informationen über installierte Pakete enthalten. Wenn eine dieser Dateien gefunden wird, extrahiert das Tool Paketnamen, Versionen und andere Metadaten. Diese Paketmetadaten werden dann in eine CycloneDX SBOM umgewandelt.

Sbomgenkann als eigenständiges Tool verwendet werden, um CycloneDX SBOM als Datei oder für STDOUT bereitzustellen. Es wird auch als Teil der Amazon Inspector CI/CD-Integration verwendet, die Container-Images automatisch als Teil Ihrer Bereitstellungspipeline scannt. Weitere Informationen finden Sie unter Integration von Amazon Inspector-Scans in Ihre CI/CD-Pipeline.

Unterstützte Pakete und Bildformate

Derzeit Sbomgen kann Inventar für die folgenden Pakettypen erfasst werden:

- Alpine APK
- Debian / Ubuntu DPKG
- Red Hat RPM
- GoPakete durch `go.mod` und `go mod cache`
- JavaPakete durch `pom.properties`
- Node.jsPakete durch `package.json` Dateien im Inneren `node_modules`
- C#-Pakete über Nuget-Dateien (`.deps.json`,, `csprojPackages.config`, packages.lock.json)
- PHP `installed.json` durch und `composer.lock`
- PythonPakete über `requirements.txtPipfile.lock`,`poetry.lock`, und `egg/wheel` Dateien
- RubyPakete durch `Gemfile.lock.gemspec`, und global installierte Gems

- RustPakete durch `Cargo.lock` und `Cargo.toml`

Sbomgenunterstützt die folgenden Container-Image-Manifestformate für Bilder:

- OCI-Image-Manifest
- DockerImage-Manifest Version 2, Schema 2
- DockerImage-Manifest Version 2, Schema 1
- DockerImage-Manifest, Version 1

> **Important**
>
> SbomgenContainer-Images können nicht gescannt werden, wenn sie größer als 5 GB sind, mehr als 60 Ebenen haben oder mehr als 2.000 installierte Pakete enthalten.

Amazon Inspector SBOM Generator installieren () Sbomgen

Sbomgenist nur für Linux-Betriebssysteme verfügbar. Wenn Sie es zur Analyse von Container-Images verwenden, muss ein Container-Service installiert sein, z. B. Docker Podman, odercontainerd.

Für eine optimale Leistung empfehlen wir, die Binärdatei von einem System aus auszuführen, das die folgenden Mindestanforderungen an die Hardware erfüllt:

- 4-fache Kern-CPU
- 8 GB RAM

So installieren Sie Sbomgen

1. Laden Sie die Sbomgen ZIP-Datei von der richtigen URL für Ihre Architektur herunter:

   Linux AMD64:

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

   Linux ARM64:

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

2. Entpacken Sie den Download mit dem folgenden Befehl:

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

3. Suchen Sie im Archiv nach den folgenden Dateien:

   - `inspector-sbomgen`— Dies ist die Binärdatei, die Sie ausführen werden, um SBOMs zu generieren.
   - `README.txt`— Dies ist die Dokumentation zur VerwendungSbomgen.
   - `LICENSE.txt`— Diese Datei enthält die Softwarelizenz fürSbomgen.
   - `licenses`— Dieser Ordner enthält Lizenzinformationen für Pakete von Drittanbietern, die von verwendet werdenSbomgen.
   - `checksums.txt`— Diese Datei enthält Hashes der Sbomgen Binärdatei.
   - `sbom.json`— Dies ist eine CycloneDX SBOM für die Binärdatei. Sbomgen

4. (Optional) Überprüfen Sie die Authentizität und Integrität der Binärdatei mit dem folgenden Befehl:

```
sha256sum < inspector-sbomgen
```

   - Vergleichen Sie die Ergebnisse mit dem Inhalt der `checksums.txt` Datei.

5. Erteilen Sie der Binärdatei mit dem folgenden Befehl die Rechte zur ausführbaren Datei:

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

6. Stellen Sie mit Sbomgen dem folgenden Befehl sicher, dass die Installation erfolgreich abgeschlossen wurde:

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

   Sie sollten die Ausgabe ähnlich der folgenden sehen:

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

Verwenden von Sbomgen

Sie können Sbomgen es verwenden, um eine SBOM für Container-Images zu generieren.

Sie können die Ergebnisse der SBOM-Generierung auch anpassen, indem Sie beispielsweise bestimmte Dateien ausschließen oder definieren, nach welchen Paketen das Tool sucht. Führen Sie den folgenden Befehl aus, um Beispiele für diese und weitere Anwendungsfälle zu erhalten:

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

Um eine SBOM für ein Container-Image zu generieren und das Ergebnis in einer Datei auszugeben

In diesem Beispiel *image:tag*ersetzen Sie es durch die ID Ihres Bilds und durch den Pfad, in *output_path.json*dem die Ausgabe gespeichert werden soll:

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

Authentifizierung bei privaten Registern mit Sbomgen

Sie können aus Ihren Containern, die in privaten Registern gehostet werden, eine SBOM generieren, indem Sie Ihre Anmeldedaten für die private Registrierung angeben. Sie können Ihre Anmeldeinformationen auf verschiedene Weise angeben: durch zwischengespeicherte Anmeldeinformationen, durch eine interaktive Methode oder durch eine nicht interaktive Methode, bei der Ihre Anmeldeinformationen vor der Ausführung als Umgebungsvariablen bereitgestellt werden. Sbomgen

Authentifizierung mit zwischengespeicherten Anmeldeinformationen (empfohlen)

1. Sbomgenversucht, zwischengespeicherte Anmeldeinformationen zu verwenden, sofern diese auf Ihrem Agenten verfügbar sind. Für diese Methode authentifizieren Sie sich zunächst bei Ihrer Container-Registry. Wenn Sie beispielsweise verwendenDocker, können Sie sich mit dem folgenden Befehl bei Ihrer Registrierung authentifizieren: Docker `login`

   ```
   docker login
   ```

2. Nachdem Sie sich erfolgreich bei Ihrer privaten Registrierung authentifiziert haben, können Sie es Sbomgen auf einem Container-Image in dieser Registrierung verwenden. Um das folgende Beispiel zu verwenden, *image:tag*ersetzen Sie es durch den Namen des zu scannenden Bilds:

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

Authentifizierung mit der interaktiven Methode

- Bei dieser Methode geben Sie Ihren Benutzernamen als Parameter an und Sbomgen werden Sie bei Bedarf zur sicheren Passworteingabe aufgefordert. Um das folgende Beispiel zu

verwenden, *image:tag*ersetzen Sie es durch den Namen des zu scannenden Bilds und *your_username*durch einen Benutzernamen, der Zugriff auf dieses Bild hat:

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

Authentifizierung mit einer nicht interaktiven Methode

- Um diese Methode zu verwenden, sollten Sie Ihr Passwort oder Ihr Registrierungstoken in einer TXT-Datei speichern, die nur für den aktuellen Benutzer lesbar ist. Die Textdatei sollte nur Ihr Passwort oder Token in einer einzigen Zeile enthalten. Um das folgende Beispiel zu verwenden, *your_username*ersetzen Sie es durch Ihren Benutzernamen, *password.txt*ersetzen Sie es durch die Datei, die Ihr Passwort oder Token enthält, und *image:tag*ersetzen Sie es durch den Namen des zu scannenden Bilds:

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

Beispielausgaben von Sbomgen

Im Folgenden finden Sie ein Beispiel für eine SBOM für ein Container-Image, das mithilfe von inventarisiert wurde. Sbomgen

Container-Image (SBOM)


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

```
          {
            "alg": "SHA-256",
            "content":
"10ab669cfc99774786301a745165b5957c92ed9562d19972fbf344d4393b5eb1"
          }
        ]
      }
    ],
    "component": {
      "bom-ref": "comp-1",
      "type": "container",
      "name": "fedora:latest",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:image_id",
          "value":
"sha256:c81c8ae4dda7dedc0711daefe4076d33a88a69a28c398688090c1141eff17e50"
        },
        {
          "name": "amazon:inspector:sbom_generator:layer_diff_id",
          "value":
"sha256:eddd0d48c295dc168d0710f70364581bd84b1dda6bb386c4a4de0b61de2f2119"
        }
      ]
    }
  },
  "components": [
    {
      "bom-ref": "comp-2",
      "type": "library",
      "name": "dnf",
      "version": "4.18.0",
      "purl": "pkg:pypi/dnf@4.18.0",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
```

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

```
  ]
}
```

Erstellen Sie Ihre eigene benutzerdefinierte CI/CD-Pipeline-Integration mit Amazon Inspector Scan

Wir empfehlen die Verwendung der Amazon Inspector CI/CD-Plugins, sofern sie auf Ihrem CI/CD-Marktplatz verfügbar sind. Eine Liste der verfügbaren Plugins finden Sie unter. Unterstützte CI/CD-Lösungen

Wenn Amazon Inspector keine Plug-ins für Ihre CI/CD-Lösung bereitstellt, können Sie mithilfe einer Kombination aus dem Amazon Inspector SBOM Generator und der Amazon Inspector Scan API Ihre eigene benutzerdefinierte CI/CD-Integration erstellen. Sie können auch eine benutzerdefinierte Integration verwenden, um Scans mithilfe der im Amazon Inspector SBOM Generator verfügbaren Optionen zu optimieren.

Um Ihre eigene benutzerdefinierte Integration einzurichten

1. Konfigurieren Sie eine AWS-Konto , um den Zugriff auf die Amazon Inspector Scan API zu ermöglichen. Anweisungen finden Sie unter Einrichtung eines AWS Kontos für die Nutzung der Amazon Inspector CI/CD-Integration.
2. Installieren und konfigurieren Sie die Amazon Inspector SBOM Generator-Binärdatei. Anweisungen finden Sie unter Amazon Inspector SBOM Generator installieren () Sbomgen.
3. Verwenden Sie den SBOM-Generator, um eine SBOM-Datei für ein Container-Image zu erstellen, das Sie scannen möchten. Um das folgende Beispiel zu verwenden, *image:id*ersetzen Sie es durch den Namen des zu scannenden Bilds und durch den Speicherort, an *sbom_path.json*dem die SBOM-Ausgabe gespeichert werden soll:

   ```
   ./inspector-sbomgen container –image image:id -o sbom_path.json
   ```

4. Rufen Sie die `inspector-scan` API auf, um die generierte SBOM zu scannen und einen Schwachstellenbericht zu erstellen. Um das folgende Beispiel zu verwenden, ersetzen Sie *sbom_path.json* durch den Dateipfad zu einer gültigen CyclonedX-kompatiblen SBOM-Datei. *Ersetzen Sie dann ENDPOINT durch den API-Endpunkt für den, für den Sie derzeit authentifiziert sind, und ersetzen AWS-Region Sie REGION durch die entsprechende Region.* Eine Endpunkte für die Amazon Inspector Scan API vollständige Liste der Regionen und Endpunkte finden Sie unter.

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

API-Ausgabeformate

Die Amazon Inspector Scan API kann einen Schwachstellenbericht im CycloneDX 1.5-Format oder Amazon Inspector Finding JSON ausgeben. Die Standardeinstellung kann mithilfe des `--output-format` Flags geändert werden.

Beispiel für eine Ausgabe im CycloneDX 1.5-Format


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

```
        }
      ],
      "timestamp": "2023-06-28T14:15:53.760Z"
    },
    "components": [
      {
        "bom-ref": "comp-1",
        "type": "library",
        "name": "log4j-core",
        "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.12.1",
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:path",
            "value": "/home/dev/foo.jar"
          }
        ]
      }
    ],
    "vulnerabilities": [
      {
        "bom-ref": "vuln-1",
        "id": "CVE-2021-44228",
        "source": {
          "name": "NVD",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
        },
        "references": [
          {
            "id": "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            }
          },
          {
            "id": "GHSA-jfh8-c2jp-5v3q",
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            }
          }
        ],
        "ratings": [
```

```
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v3-1/"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          },
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v2/"
            },
            "score": 9.3,
            "severity": "critical",
            "method": "CVSSv2",
            "vector": "AC:M/Au:N/C:C/I:C/A:C"
          },
          {
            "source": {
              "name": "EPSS",
              "url": "https://www.first.org/epss/"
            },
            "score": 0.97565,
            "severity": "none",
            "method": "other",
            "vector": "model:v2023.03.01,date:2023-06-27T00:00:00+0000"
          },
          {
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
          },
          {
            "source": {
              "name": "GITHUB",
```

```
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          }
        ],
        "cwes": [
          400,
          20,
          502
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "advisories": [
          {
            "url": "https://www.intel.com/content/www/us/en/security-center/advisory/
intel-sa-00646.html"
          },
          {
            "url": "https://support.apple.com/kb/HT213189"
          },
          {
            "url": "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/"
          },
          {
            "url": "https://logging.apache.org/log4j/2.x/security.html"
          },
          {
            "url": "https://www.debian.org/security/2021/dsa-5020"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf"
          },
          {
```

```
            "url": "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpujan2022.html"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpuapr2022.html"
          },
          {
            "url": "https://twitter.com/kurtseifried/status/1469345530182455296"
          },
          {
            "url": "https://tools.cisco.com/security/center/content/
CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd"
          },
          {
            "url": "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html"
          },
          {
            "url": "https://www.kb.cert.org/vuls/id/930724"
          }
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "affects": [
          {
            "ref": "comp-1"
```

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

Beispiel für eine Ausgabe im Inspector-Format

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

```
      "critical": 1,
      "high": 0,
      "medium": 0,
      "low": 0
    },
    "vulnerabilities": [
      {
        "id": "CVE-2021-44228",
        "severity": "critical",
        "source": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228",
        "related": [
          "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
          "GHSA-jfh8-c2jp-5v3q"
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "references": [
          "https://www.intel.com/content/www/us/en/security-center/advisory/intel-
sa-00646.html",
          "https://support.apple.com/kb/HT213189",
          "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/",
          "https://logging.apache.org/log4j/2.x/security.html",
          "https://www.debian.org/security/2021/dsa-5020",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf",
          "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html",
          "https://www.oracle.com/security-alerts/cpujan2022.html",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/",
          "https://www.oracle.com/security-alerts/cpuapr2022.html",
          "https://twitter.com/kurtseifried/status/1469345530182455296",
```

```
          "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-
sa-apache-log4j-qRuKNEbd",
          "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html",
          "https://www.kb.cert.org/vuls/id/930724"
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "properties": {
          "cisa_kev_date_added": "2021-12-10T00:00:00Z",
          "cisa_kev_date_due": "2021-12-24T00:00:00Z",
          "cwes": [
            400,
            20,
            502
          ],
          "cvss": [
            {
              "source": "NVD",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
              "cvss2_base_score": 9.3,
              "cvss2_base_vector": "AC:M/Au:N/C:C/I:C/A:C"
            },
            {
              "source": "SNYK",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
            },
            {
              "source": "GITHUB",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
            }
          ],
          "epss": 0.97565,
          "exploit_available": true,
          "exploit_last_seen_in_public": "2023-03-06T00:00:00Z"
        },
        "affects": [
          {
```

```
            "installed_version": "pkg:maven/org.apache.logging.log4j/log4j-
core@2.12.1",
            "fixed_version": "2.15.0",
            "path": "/home/dev/foo.jar"
          }
        ]
      }
    ]
  }
}
```

Verwenden des Amazon Jenkins Inspector-Plug-ins

Das Jenkins Plugin nutzt die Amazon Inspector SBOM Generator-Binärdatei und die Amazon Inspector Scan API, um am Ende Ihres Builds detaillierte Berichte zu erstellen, sodass Sie Risiken vor der Bereitstellung untersuchen und beheben können.

Amazon Inspector ist ein Schwachstellen-Management-Service, der Container-Images auf der Grundlage von CVEs nach Sicherheitslücken in Betriebssystemen und Programmiersprachenpaketen durchsucht.

Mit dem Amazon Jenkins Inspector-Plugin können Sie Amazon Inspector Inspector-Schwachstellenscans zu Ihrer Jenkins Pipeline hinzufügen.

> **Note**
>
> Amazon Inspector Vulnerability Scans können so konfiguriert werden, dass Pipeline-Ausführungen je nach Anzahl und Schweregrad der erkannten Sicherheitslücken bestanden oder fehlschlagen.

Die neueste Version des Jenkins Plug-ins finden Sie im Jenkins Marketplace unter https://plugins.jenkins.io/amazon-inspector-image-scanner/.

In den folgenden Schritten wird beschrieben, wie Sie das Amazon Jenkins Inspector-Plugin einrichten.

> **Important**
>
> Bevor Sie die folgenden Schritte ausführen, müssen Sie Jenkins auf Version 2.387.3 oder höher aktualisieren, damit das Plugin ausgeführt werden kann.

Schritt 1. Richten Sie ein AWS-Konto

Konfigurieren Sie eine AWS-Konto mit einer IAM-Rolle, die den Zugriff auf die Amazon Inspector Scan API ermöglicht. Anweisungen finden Sie unter Einrichtung eines AWS Kontos für die Nutzung der Amazon Inspector CI/CD-Integration.

Schritt 2. Installieren Sie das Amazon Inspector Jenkins-Plugin

Das folgende Verfahren beschreibt, wie Sie das Amazon Inspector Jenkins-Plugin vom Jenkins Dashboard aus installieren.

1. Wählen Sie im Jenkins-Dashboard Manage Jenkins und anschließend Manage Plugins aus.
2. Wählen Sie „Verfügbar“.
3. Suchen Sie auf der Registerkarte Verfügbar nach Amazon Inspector Scans und installieren Sie dann das Plugin.

(Optional) Schritt 3. Fügen Sie Docker-Anmeldeinformationen hinzu Jenkins

> **Note**
>
> Fügen Sie nur Docker-Anmeldeinformationen hinzu, wenn sich das Docker-Image in einem privaten Repository befindet. Andernfalls überspringen Sie diesen Schritt.

Das folgende Verfahren beschreibt, wie Sie Docker-Anmeldeinformationen vom Jenkins Dashboard Jenkins aus hinzufügen.

1. Wählen Sie im Jenkins-Dashboard Manage Jenkins, Credentials und dann System aus.
2. Wählen Sie Globale Anmeldeinformationen und dann Anmeldeinformationen hinzufügen aus.
3. Wählen Sie unter Kind die Option Benutzername mit Passwort aus.

4. Wählen Sie unter Bereich die Option Global (Jenkins, Knoten, Elemente, alle untergeordneten Elemente usw.) aus.
5. Geben Sie Ihre Daten ein und wählen Sie dann OK.

(Optional) Schritt 4. Fügen Sie AWS Anmeldeinformationen hinzu

> **Note**
>
> Fügen Sie nur AWS Anmeldeinformationen hinzu, wenn Sie sich anhand eines IAM-Benutzers authentifizieren möchten. Andernfalls überspringen Sie diesen Schritt.

Im folgenden Verfahren wird beschrieben, wie Sie AWS Anmeldeinformationen über das Jenkins Dashboard hinzufügen.

1. Wählen Sie im Jenkins-Dashboard Manage Jenkins, Credentials und dann System aus.
2. Wählen Sie Globale Anmeldeinformationen und dann Anmeldeinformationen hinzufügen aus.
3. Wählen Sie für Kind die Option AWS-Anmeldeinformationen aus.
4. Geben Sie Ihre Daten ein, einschließlich Ihrer Zugriffsschlüssel-ID und Ihres geheimen Zugangsschlüssels, und wählen Sie dann OK.

Schritt 5. Fügen Sie CSS-Unterstützung in einem Jenkins Skript hinzu

Das folgende Verfahren beschreibt, wie Sie CSS-Unterstützung in einem Jenkikns Skript hinzufügen.

1. Starten Sie Jenkins neu.
2. Wählen Sie im Dashboard Manage Jenkins, Nodes, Built-In Node und dann Script Console aus.
3. Fügen Sie im Textfeld die Zeile hinzu und wählen Sie **`System.setProperty("hudson.model.DirectoryBrowserSupport.CSP", "")`** dann Ausführen aus.

Schritt 6: Fügen Sie Amazon Inspector Scan zu Ihrem Build hinzu

Sie können Amazon Inspector Scan zu Ihrem Build hinzufügen, indem Sie Ihrem Projekt einen Build-Schritt hinzufügen oder die Jenkins deklarative Pipeline verwenden.

Amazon Inspector Scan zu Ihrem Build, indem Sie Ihrem Projekt einen Build-Schritt hinzufügen

1. Scrollen Sie auf der Konfigurationsseite nach unten zu Build Steps und wählen Sie Build-Schritt hinzufügen aus. Wählen Sie dann Amazon Inspector Scan aus.
2. Wählen Sie zwischen zwei Inspector-Sbomgen-Installationsmethoden: Automatisch oder Manuell.

   a. (Option 1) Wählen Sie Automatisch, um die neueste Version von inspector-sbomgen herunterzuladen. Wenn Sie diese Methode wählen, stellen Sie sicher, dass Sie die CPU-Architektur auswählen, die dem System entspricht, auf dem das Plugin ausgeführt wird.

   b. (Option 2) Wählen Sie Manuell, wenn Sie die Amazon Inspector SBOM Generator-Binärdatei für das Scannen einrichten möchten. Wenn Sie diese Methode wählen, stellen Sie sicher, dass Sie den vollständigen Pfad zu einer zuvor heruntergeladenen Version von inspector-sbomgen angeben.

   Weitere Informationen finden Sie unter Installation von Amazon Inspector SBOM Generator (Sbomgen) in Amazon Inspector SBOM Generator.
3. Gehen Sie wie folgt vor, um die Konfiguration des Amazon Inspector Scan-Build-Schritts abzuschließen:

   a. Geben Sie Ihre Bild-ID ein. Das Bild kann lokal, remote oder archiviert sein. Bildnamen sollten der Docker Benennungskonvention entsprechen. Wenn Sie ein exportiertes Bild analysieren, geben Sie den Pfad zur erwarteten TAR-Datei an. Sehen Sie sich das folgende Beispiel für Image-ID-Pfade an:

      i. Für lokale oder Remote-Container: `NAME[:TAG|@DIGEST]`

      ii. Für eine TAR-Datei: `/path/to/image.tar`

   b. Wählen Sie einen aus AWS-Region, über den die Scananforderung gesendet werden soll.

   c. (Optional) Wählen Sie für Docker-Anmeldeinformationen Ihren Docker Benutzernamen aus. Tun Sie dies nur, wenn sich Ihr Container-Image in einem privaten Repository befindet.

   d. (Optional) Sie können die folgenden unterstützten AWS Authentifizierungsmethoden bereitstellen:

      i. (Optional) Geben Sie für die IAM-Rolle einen Rollen-ARN an (arn:aws:iam: :role/). *`AccountNumberRoleName`*

ii. (Optional) Wählen Sie für AWS-Anmeldeinformationen die ID aus, um sich anhand eines IAM-Benutzers zu authentifizieren.

iii. (Optional) Geben Sie als AWS Profilname den Namen eines Profils an, das mithilfe eines Profilnamens authentifiziert werden soll.

e. (Optional) Geben Sie die Schwellenwerte für Sicherheitslücken pro Schweregrad an. Wenn die von Ihnen angegebene Zahl während eines Scans überschritten wird, schlägt die Image-Erstellung fehl. Wenn die Werte alle sind`0`, ist der Build erfolgreich, unabhängig davon, ob Sicherheitslücken gefunden wurden.

4. Wählen Sie Speichern.

Fügen Sie Amazon Inspector Scan mithilfe der Jenkins deklarativen Pipeline zu Ihrem Build hinzu

Sie können Amazon Inspector Scan mithilfe der deklarativen Jenkins-Pipeline automatisch oder manuell zu Ihrem Build hinzufügen.

Um die deklarative SBOMGen-Pipeline automatisch herunterzuladen

- Verwenden Sie die folgende Beispielsyntax, um Amazon Inspector Scan zu einem Build hinzuzufügen. Basierend auf Ihrer bevorzugten Betriebssystemarchitektur des Amazon Inspector SBOM Generator-Downloads ersetzen Sie *`SBOMGEN_SOURCE`* durch LinuxAMD64 oder LinuxARM64. Ersetzen Sie *`IMAGE_PATH`* durch den Pfad zu Ihrem Image (z. B. *`alpine:latest`*), *`IAM_ROLE durch den ARN der IAM-Rolle`*, die Sie in Schritt 1 konfiguriert haben, und *`ID durch Ihre Docker Anmeldeinformations-ID`*, wenn Sie ein privates Repository verwenden. Sie können optional Schwellenwerte für Sicherheitslücken aktivieren und Werte für jeden Schweregrad angeben.

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

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

Um die deklarative SBOMGen-Pipeline manuell herunterzuladen

- Verwenden Sie die folgende Beispielsyntax, um Amazon Inspector Scan zu einem Build hinzuzufügen. *Ersetzen Sie SBOMGEN_PATH durch den Pfad zum Amazon Inspector SBOM Generator, den Sie in Schritt 3 installiert haben, IMAGE_PATH durch den Pfad zu Ihrem Image (z. B. alpine:latest), IAM_ROLE durch den ARN der IAM-Rolle, die Sie in Schritt 1 konfiguriert haben, und ID durch Ihre Anmeldeinformations-ID, wenn Sie ein privates Repository verwenden.* Docker Sie können optional Schwellenwerte für Sicherheitslücken aktivieren und Werte für jeden Schweregrad angeben.

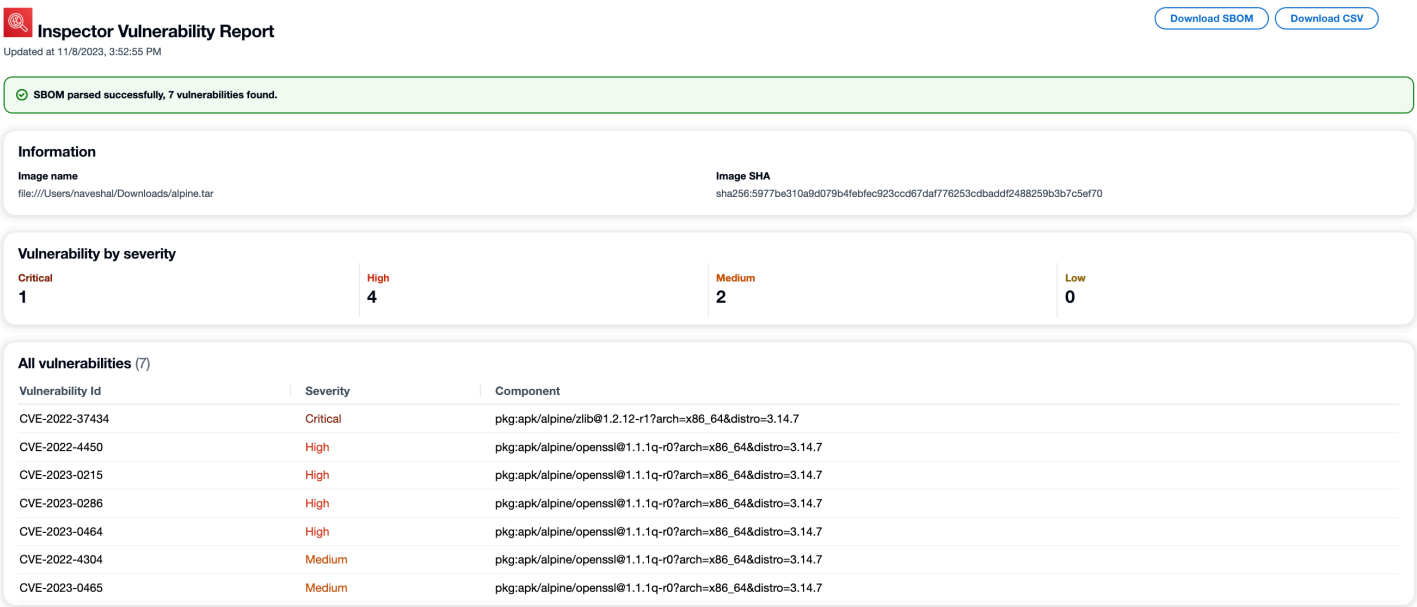
> **Note**
>
> *Platzieren Sie es Sbomgen im Jenkins-Verzeichnis und geben Sie den Pfad zum Jenkins-Verzeichnis im Plugin an (z. B. /opt/folder/arm64/inspector-sbomgen).*

```
pipeline {
    agent any
```

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

Schritt 7. Sehen Sie sich Ihren Amazon Inspector Inspector-Schwachstellenbericht an

1. Vervollständigen Sie einen neuen Build Ihres Projekts.
2. Wählen Sie nach Abschluss des Builds ein Ausgabeformat aus den Ergebnissen aus. Wenn Sie HTML auswählen, haben Sie die Möglichkeit, eine JSON-, SBOM- oder CSV-Version des Berichts herunterzuladen. Im Folgenden wird ein Beispiel für einen HTML-Bericht gezeigt:



Fehlerbehebung

Im Folgenden sind häufig auftretende Fehler aufgeführt, die bei der Verwendung des Amazon Inspector Scan-Plug-ins auftreten könnenJenkins.

Anmeldeinformationen konnten nicht geladen werden oder STS-Ausnahmefehler

Fehler:

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

Auflösung

Holen Sie sich `aws_access_key_id` und `aws_secret_access_key` für Ihr AWS Konto. Aufstellen `aws_access_key_id` und `aws_secret_access_key` rein`~/.aws/credentials`.

Inspector-SBOMGen-Pfadfehler

Fehler:

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

Auflösung

Gehen Sie wie folgt vor, um das Problem zu beheben.

1. Platzieren Sie die richtige Betriebssystemarchitektur Inspector-SBOMGen im Jenkins Verzeichnis Weitere Informationen finden Sie unter Amazon Inspector SBOM Generator.
2. Erteilen Sie mit dem folgenden Befehl ausführbare Rechte für die Binärdatei:. `chmod +x inspector-sbomgen`
3. Geben Sie im Plugin den richtigen Jenkins Computerpfad an, z. `/opt/folder/arm64/inspector-sbomgen` B.
4. Speichern Sie die Konfiguration und führen Sie den Jenkins Job aus.

Verwenden des Amazon TeamCity Inspector-Plug-ins

Das Amazon TeamCity Inspector-Plugin bietet Ihnen die Möglichkeit, Amazon Inspector Inspector-Schwachstellenscans zu Ihrer TeamCity Pipeline hinzuzufügen. Das Plugin nutzt die Amazon Inspector SBOM Generator-Binärdatei und die Amazon Inspector Scan API, um am Ende Ihres Builds detaillierte Berichte zu erstellen, sodass Sie Risiken vor der Bereitstellung untersuchen und beheben können. Je nach Anzahl und Schweregrad der erkannten Sicherheitslücken können die Scans auch so konfiguriert werden, dass Pipeline-Ausführungen erfolgreich ausgeführt werden oder nicht.

Amazon Inspector ist ein von angebotener Schwachstellen-Management-Service AWS , der Container-Images auf der Grundlage von CVEs nach Sicherheitslücken in Betriebssystemen und Programmiersprachenpaketen scannt. Weitere Informationen zur Amazon Inspector CI/CD-Integration finden Sie unter. Integration von Amazon Inspector-Scans in Ihre CI/CD-Pipeline

Eine Liste der Pakete und Container-Image-Formate, die das Amazon Inspector-Plugin unterstützt, finden Sie unter,Unterstützte Pakete und Bildformate.

Sie können die neueste Version des Plug-ins im TeamCity Marketplace unter https://plugins.jetbrains.com/plugin/23236 — einsehenamazon-inspector-scanner. Folgen Sie alternativ den Schritten in den einzelnen Abschnitten dieses Dokuments, um das Amazon TeamCity Inspector-Plugin einzurichten:

1. Richten Sie ein AWS-Konto.
   - Konfigurieren Sie eine AWS-Konto mit einer IAM-Rolle, die den Zugriff auf die Amazon Inspector Scan API ermöglicht. Anweisungen finden Sie unter Einrichtung eines AWS Kontos für die Nutzung der Amazon Inspector CI/CD-Integration.

2. Installieren Sie das Amazon TeamCity Inspector-Plugin.
   a. Gehen Sie in Ihrem Dashboard zu Administration > Plugins.
   b. Suchen Sie nach Amazon Inspector Scans.
   c. Installieren Sie das -Plug-in.
3. Installieren Sie den Amazon Inspector SBOM Generator.
   - Installieren Sie die Amazon Inspector SBOM Generator-Binärdatei in Ihrem Teamcity-Serververzeichnis. Anweisungen finden Sie unter Amazon Inspector SBOM Generator installieren () Sbomgen.
4. Fügen Sie Ihrem Projekt einen Amazon Inspector Scan-Build-Schritt hinzu.
   a. Scrollen Sie auf der Konfigurationsseite nach unten zu Build Steps, wählen Sie Build-Schritt hinzufügen und dann Amazon Inspector Scan aus.
   b. Konfigurieren Sie den Erstellungsschritt Amazon Inspector Scan, indem Sie die folgenden Details eingeben:
      - Fügen Sie einen Schrittnamen hinzu.
      - Wählen Sie zwischen zwei Installationsmethoden für Amazon Inspector SBOM Generator: Automatisch oder Manuell.
        - Lädt automatisch die neueste Version von Amazon Inspector SBOM Generator herunter, die auf Ihrer System- und CPU-Architektur basiert.
        - Für das Handbuch müssen Sie einen vollständigen Pfad zu einer zuvor heruntergeladenen Version von Amazon Inspector SBOM Generator angeben.

        Weitere Informationen finden Sie unter Installation von Amazon Inspector SBOM Generator (SBOM Generator) in Amazon Inspector SBOM Generator.
      - Geben Sie Ihre Bild-ID ein. Ihr Bild kann lokal, remote oder archiviert sein. Bildnamen sollten der Docker Benennungskonvention entsprechen. Wenn Sie ein exportiertes Bild analysieren, geben Sie den Pfad zur erwarteten TAR-Datei an. Sehen Sie sich das folgende Beispiel für Image-ID-Pfade an:
        - Für lokale oder Remote-Container: `NAME[:TAG|@DIGEST]`
        - Für eine TAR-Datei: `/path/to/image.tar`
      - Geben Sie für IAM-Rolle den ARN für die Rolle ein, die Sie in Schritt 1 konfiguriert haben.
      - Wählen Sie eine aus AWS-Region, über die die Scananforderung gesendet werden soll.

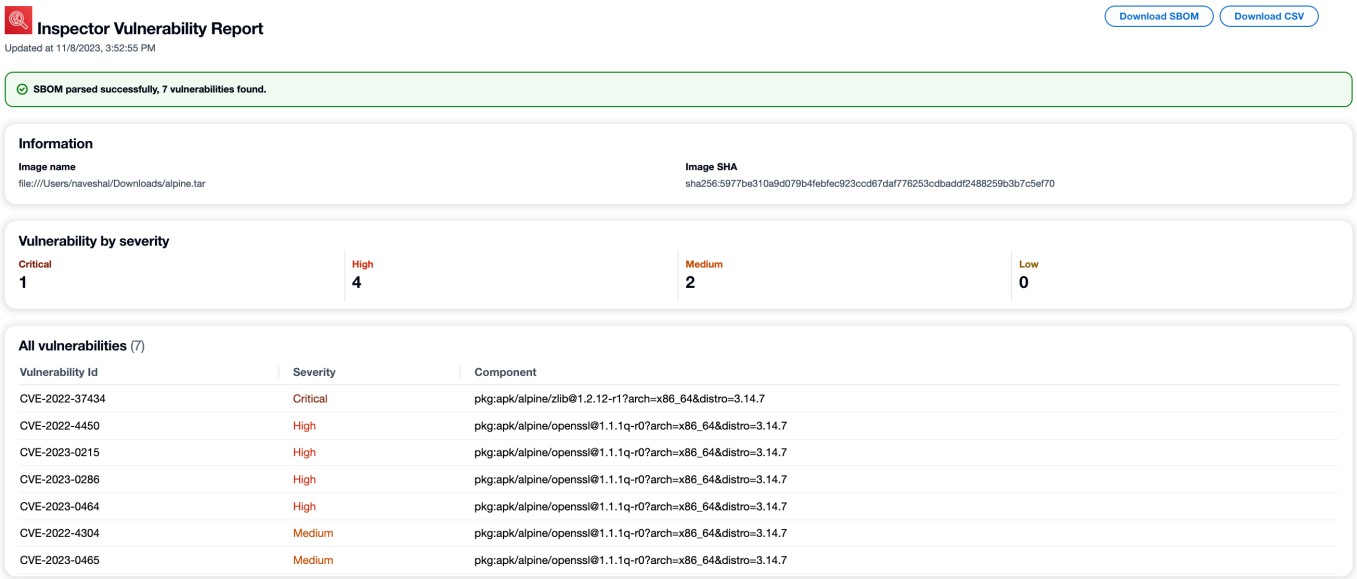
- (Optional) Geben Sie für die Docker-Authentifizierung Ihren Docker-Benutzernamen und Ihr Docker-Passwort ein. Tun Sie dies nur, wenn sich Ihr Container-Image in einem privaten Repository befindet.
- (Optional) Geben Sie für die AWS Authentifizierung Ihre AWS Zugriffsschlüssel-ID und Ihren AWS geheimen Schlüssel ein. Tun Sie dies nur, wenn Sie sich anhand von AWS Anmeldeinformationen authentifizieren möchten.
- (Optional) Geben Sie die Schwellenwerte für Sicherheitslücken pro Schweregrad an. Wenn die von Ihnen angegebene Zahl während eines Scans überschritten wird, schlägt die Image-Erstellung fehl. Wenn die Werte alle sind, ist `0` der Build unabhängig von der Anzahl der gefundenen Sicherheitslücken erfolgreich.

c. Wählen Sie Speichern.

5. Sehen Sie sich Ihren Amazon Inspector-Sicherheitslückenbericht an.

   a. Vervollständigen Sie einen neuen Build Ihres Projekts.

   b. Wenn der Build abgeschlossen ist, wählen Sie ein Ausgabeformat aus den Ergebnissen aus. Wenn Sie HTML auswählen, haben Sie die Möglichkeit, eine JSON-, SBOM- oder CSV-Version des Berichts herunterzuladen. Im Folgenden finden Sie ein Beispiel für einen HTML-Bericht:



Amazon CycloneDX Inspector-Namespaces

Amazon Inspector hat CycloneDX Namespaces und Eigenschaftsnamen für die Verwendung mit SBOMs reserviert, die vom Amazon Inspector SBOM Generator und der Amazon Inspector Scan API erstellt wurden. Auf dieser Seite werden alle benutzerdefinierten Schlüssel-/Werteigenschaften dokumentiert, die zu Komponenten in CycloneDX SBOMs hinzugefügt werden können, die mit den Amazon Inspector Inspector-Tools erstellt wurden. Weitere Informationen zu CycloneDX Immobilientaxonomien finden Sie in der offiziellen Dokumentation.

`amazon:inspector:sbom_scanner`Namespace-Taxonomie

Der `amazon:inspector:sbom_scanner` Namespace wird von der Amazon Inspector Scan API verwendet. Er besitzt die folgenden Eigenschaften:

Eigenschaft	Beschreibung
`amazon:inspector:sbom_scanner:critical_vulnerabilities`	Anzahl der Gesamtzahl der in der SBOM gefundenen Sicherheitslücken mit kritischem Schweregrad.
`amazon:inspector:sbom_scanner:high_vulnerabilities`	Anzahl der Gesamtzahl der in der SBOM gefundenen Sicherheitslücken mit hohem Schweregrad.
`amazon:inspector:sbom_scanner:medium_vulnerabilities`	Anzahl der Gesamtzahl der in der SBOM gefundenen Sicherheitslücken mit mittlerem Schweregrad.
`amazon:inspector:sbom_scanner:low_vulnerabilities`	Anzahl der Gesamtzahl der in der SBOM gefundenen Sicherheitslücken mit niedrigem Schweregrad.
`amazon:inspector:sbom_scanner:info`	Stellt den Scankontext für eine bestimmte Komponente bereit, zum Beispiel: „Komponente gescannt: Keine Sicherheitslücken gefunden“.
`amazon:inspector:sbom_scanner:warning`	Stellt den Kontext dafür bereit, warum eine bestimmte Komponente nicht gescannt wurde,

Eigenschaft	Beschreibung
	zum Beispiel: „Komponente übersprungen: keine URL angegeben.“
`amazon:inspector:sbom_scanner:fixed_version:` *`component_bom_ref`*	Stellt die behobene Version der angegebenen Komponente für die angegebene Sicherheitsanfälligkeit bereit.
`amazon:inspector:sbom_scanner:exploit_available`	Zeigt an, ob ein Exploit für die angegebene Sicherheitsanfälligkeit verfügbar ist.
`amazon:inspector:sbom_scanner:exploit_last_seen_in_public`	Gibt an, wann ein Exploit für die angegebene Sicherheitsanfälligkeit zuletzt öffentlich bekannt wurde.
`amazon:inspector:sbom_scanner:cisa_kev_date_added`	Gibt an, wann die Sicherheitsanfälligkeit in den Katalog der bekannten Sicherheitslücken der CISA aufgenommen wurde.
`amazon:inspector:sbom_scanner:cisa_kev_date_due`	Gibt an, wann die Behebung der Sicherheitslücke gemäß dem CISA-Katalog mit den bekannten Sicherheitslücken fällig ist.
`amazon:inspector:sbom_scanner:path`	Der Pfad zu der Datei, die die Betreff-Paketinformationen lieferte.

`amazon:inspector:sbom_generator`Namespace-Taxonomie

Der `amazon:inspector:sbom_generator` Namespace wird vom Amazon Inspector SBOM Generator verwendet. Er besitzt die folgenden Eigenschaften:

Eigenschaft	Beschreibung
`amazon:inspector:sbom_generator:os_hostname`	Der Hostname des Systems, das inventarisiert wird.

Eigenschaft	Beschreibung
`amazon:inspector:sbom_generator:kernel_name`	Der Kernelname des Systems, das inventarisiert wird.
`amazon:inspector:sbom_generator:kernel_version`	Die Kernelversion des Systems, das inventarisiert wird.
`amazon:inspector:sbom_generator:cpu_architecture`	Die CPU-Architektur des Systems, das inventarisiert wird, z. B. x86_64.
`amazon:inspector:sbom_generator:image_id`	Der Hash der Konfigurationsdatei des Container-Images, auch bekannt als Image-ID.
`amazon:inspector:sbom_generator:layer_diff_id`	Der Hash der unkomprimierten Container-Image-Ebene.
`amazon:inspector:sbom_generator:source_file_scanner`	Der Scanner, der die Datei gefunden hat, die Paketinformationen enthält, zum Beispiel:`/var/lib/dpkg/status` .
`amazon:inspector:sbom_generator:source_package_collector`	Der Collector, der den Paketnamen und die Version aus einer bestimmten Datei extrahiert hat.
`amazon:inspector:sbom_generator:source_path`	Der Pfad zu der Datei, aus der die Betreff-Paketinformationen extrahiert wurden.
`amazon:inspector:sbom_generator:is_duplicate_package`	Zeigt an, dass das Betreff-Paket von mehr als einem Dateiscanner gefunden wurde.
`amazon:inspector:sbom_generator:go_toolchain`	Gibt die Go Compiler- oder Toolchainversion an, die zur Erstellung einer ausführbaren Go-Datei verwendet wurde.
`amazon:inspector:sbom_generator:expires_before`	das Datum, bevor das SSL-Zertifikat gültig ist.

Eigenschaft	Beschreibung
`amazon:inspector:sbom_generator:expires_after`	das Datum, nach dem das SSL-Zertifikat ungültig ist.
`amazon:inspector:sbom_generator:is_expired`	ein boolescher Wert, der angibt, ob das SSL-Zertifikat abgelaufen ist.

Automatisiertes Scannen von Ressourcen mit Amazon Inspector

Das agentenlose Scannen von Amazon Inspector für Amazon EC2 befindet sich in der Vorschauversion. Ihre Nutzung der Amazon EC2-Scanfunktion ohne Agenten unterliegt Abschnitt 2 der AWS Servicebedingungen („Betas und Vorschauen“).

Amazon Inspector verwendet eine eigene, speziell entwickelte Scan-Engine. Diese Engine überwacht Ihre Ressourcen auf Softwareschwachstellen oder offene Netzwerkpfade, die zu beeinträchtigten Workloads, böswilliger Nutzung von Ressourcen oder unberechtigtem Zugriff auf Ihre Daten führen können. Wenn Amazon Inspector eine Sicherheitslücke entdeckt, erstellt es einen Befund. Zu den Ergebnissen gehören Details im Zusammenhang mit der Entdeckung, die Ihnen bei der Behebung der Sicherheitsanfälligkeit helfen sollen. Sie können die Ergebnisse auf der Amazon Inspector Inspector-Konsole und mithilfe der Amazon Inspector Inspector-API überprüfen. Weitere Informationen finden Sie unter Ergebnisse in Amazon Inspector verwalten.

Bei Aktivierung erkennt Amazon Inspector automatisch alle infrage kommenden Ressourcen und beginnt mit kontinuierlichen Scans dieser Ressourcen. Amazon Inspector sucht nach Softwareschwachstellen und unbeabsichtigten Netzwerkbedrohungen. Amazon Inspector führt auch Scans als Reaktion auf Ereignisse wie die Installation einer neuen Anwendung oder eines Patches durch.

Wenn Sie Amazon Inspector zum ersten Mal aktivieren, wird Ihr Konto automatisch für alle Scantypen registriert. Die folgenden Themen behandeln spezifische Details zu den von Amazon Inspector bereitgestellten Scantypen. Amazon Inspector kategorisiert Scantypen basierend auf dem Ressourcentyp, der von einer Sicherheitsanfälligkeit betroffen ist. Die folgenden Themen behandeln, welche Ressourcen Amazon Inspector scannt, was neue Scans für diese Ressourcen initiiert und wie Scans für jeden Ressourcentyp konfiguriert werden.

Themen

- AWS Lambda Scanfunktionen mit Amazon Inspector
- Deaktivieren eines Scantyps

Wenn Sie Amazon Inspector zum ersten Mal aktivieren, wird Ihr Konto automatisch für die folgenden Scantypen registriert: Amazon Amazon EC2-Scannen, Amazon ECR-Scannen, Lambda-Standardscans. Das Lambda-Code-Scannen ist eine optionale Ebene des Lambda-Funktionsscannens, die Sie jederzeit aktivieren können.

Übersicht der Amazon Inspector-Scantypen

Amazon Inspector bietet eine Reihe verschiedener Scantypen, die sich auf bestimmte Ressourcentypen in Ihrer AWS Umgebung konzentrieren.

Amazon EC2-Scannen

Wenn Sie das Amazon EC2-Scannen aktivieren, scannt Amazon Inspector Ihre Amazon EC2 EC2-Instances auf Sicherheitslücken in Betriebssystempaketen und Programmiersprachenpaketen sowie auf die Erreichbarkeit über das Netzwerk. Amazon Inspector scannt Ihre EC2-Instance auf Common Vulnerabilities and Exposures (CVE) und Netzwerkprobleme. Amazon Inspector führt Scans mithilfe des auf Ihrer Instance installierten SSM-Agenten oder mithilfe von Amazon EBS-Snapshots von Instances durch. Weitere Informationen zu Scans für Amazon EC2 finden Sie unterScannen von Amazon EC2 EC2-Instances mit Amazon Inspector.

Amazon ECR-Scannen

Wenn Sie das Amazon ECR-Scannen aktivieren, konvertiert Amazon Inspector alle Container-Repositorys für Basic Scanning in Ihrer privaten Registrierung in Enhanced Scanning mit kontinuierlichem Scannen. Sie können diese Einstellung auch optional so konfigurieren, dass nur bei Push gescannt wird oder dass ausgewählte Repositorys anhand von Einschlussregeln gescannt werden. Alle Bilder, die innerhalb der letzten 30 Tage übertragen oder innerhalb der letzten 90 Tage abgerufen wurden, werden zunächst gescannt. Amazon Inspector überwacht Bilder standardmäßig weiterhin für eine Dauer von 90 Tagen. Diese Einstellung kann jederzeit geändert werden. Weitere Informationen zu Scans für Amazon ECR finden Sie unterScannen von Amazon ECR-Container-Bildern mit Amazon Inspector.

Lambda-Standardabtastung

Wenn Sie das Lambda-Standardscannen aktivieren, erkennt Amazon Inspector die Lambda-Funktionen in Ihrem Konto und beginnt sofort damit, sie auf Sicherheitslücken zu scannen. Amazon Inspector scannt neue Lambda-Funktionen und -Layer, wenn sie bereitgestellt werden, und scannt sie erneut, wenn sie aktualisiert werden oder wenn neue Common Vulnerabilities and Exposures (CVEs) veröffentlicht werden. Weitere Hinweise zum Scannen von Lambda-Funktionen finden Sie unterAWS Lambda Scanfunktionen mit Amazon Inspector.

Lambda-Standardscannen + Lambda-Code-Scannen

Diese Can-Option kombiniert Lambda-Standard-Scanning mit Lambda-Code-Scanning. Wenn das Lambda-Code-Scannen aktiviert ist, erkennt Amazon Inspector die Lambda-Funktionen und -Ebenen in Ihrem Konto und scannt Ihre Anwendungspaketabhängigkeiten auf Code-Schwachstellen. Das Lambda-Code-Scannen scannt den benutzerdefinierten Anwendungscode in Ihren Lambda-Funktionen auf Code-Schwachstellen. Diese beiden Scantypen müssen zusammen aktiviert werden. Weitere Informationen finden Sie unter Scannen von Lambda-Code mit Amazon Inspector.

Einen Scantyp aktivieren

Sie können jederzeit einen neuen Amazon Inspector-Scantyp aktivieren. Sobald Sie einen Scantyp aktiviert haben, beginnt Amazon Inspector sofort mit dem Scannen geeigneter Ressourcen für diesen Scantyp. Eine Übersicht der verfügbaren Scantypen finden Sie unterÜbersicht der Amazon Inspector-Scantypen. Im Folgenden wird beschrieben, was passiert, wenn Sie die einzelnen Scantypen zum ersten Mal aktivieren:

- Amazon EC2-Scannen — Wenn Sie Amazon Inspector Amazon EC2-Scanning für ein Konto aktivieren, scannt Amazon Inspector alle geeigneten Instances in Ihrem Konto auf Paketschwachstellen und Probleme mit der Netzwerkerreichbarkeit. Das Amazon Inspector SSM-Plugin ist auf all Ihren Windows SSM-verwalteten Hosts installiert. Weitere Informationen finden Sie unter Instanzen scannen Windows. Darüber hinaus erstellt Amazon Inspector die folgenden SSM-Verknüpfungen in Ihrem Konto:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`

- `InvokeInspectorSsmPlugin-do-not-delete`.

- Amazon ECR-Scannen — Wenn Sie das Scannen von Amazon ECR-Container-Images für ein Konto aktivieren, ändert sich der Amazon ECR-Scantyp für private Repositorys in diesem Konto von Basic Scanning with Amazon ECR zu Enhanced Scanning with Amazon Inspector. Anschließend werden alle geeigneten Amazon ECR-Container-Images, die innerhalb der letzten 30 Tage übertragen oder innerhalb der letzten 90 Tage abgerufen wurden, auf Paketschwachstellen gescannt. Darüber hinaus ist Ihre Amazon ECR-Rescan-Dauer für das Datum von Image-Push und Pull auf 90 Tage festgelegt.
- Lambda-Standard-Scanning — Wenn Sie das Lambda-Standardscannen in einem Konto aktivieren, werden alle Lambda-Funktionen in Ihrem Konto, die in den letzten 90 Tagen aufgerufen oder aktualisiert wurden, auf Sicherheitslücken in Paketen gescannt. Zusätzlich wird in Ihrem Konto ein mit dem CloudTrail Service verknüpfter Kanal erstellt.
- Lambda-Standardscanning + Lambda-Code-Scanning — Diese Lambda-Funktionsscantypen werden zusammen aktiviert. Wenn Sie das Lambda-Code-Scannen in einem Konto aktivieren, werden alle Lambda-Funktionen in Ihrem Konto, die in den letzten 90 Tagen aufgerufen oder aktualisiert wurden, auf Code-Schwachstellen gescannt.

Scans aktivieren

Wenn Sie der delegierte Administrator für Amazon Inspector in einer AWS Organisation sind, können Sie mithilfe eines von Amazon Inspector2-on entwickelten Shell-Skripts automatisch verschiedene Amazon Inspector-Scantypen für mehrere Konten in mehreren Regionen aktivieren. enablement-with-cli GitHub Andernfalls, um dieses Verfahren für eine Umgebung mit mehreren Konten über die Konsole abzuschließen, führen Sie die folgenden Schritte aus, während Sie als delegierter Amazon Inspector-Administrator angemeldet sind.

Console

Um Scans zu aktivieren

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit AWS-Region der Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie einen neuen Scantyp aktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Kontoverwaltung aus.

4. Wählen Sie auf der Seite Kontoverwaltung die Konten aus, für die Sie einen Scantyp aktivieren möchten.
5. Wählen Sie Aktivieren und wählen Sie die Art des Scannens aus, den Sie aktivieren möchten.
6. (Empfohlen) Wiederholen Sie diese Schritte AWS-Region für jeden, für den Sie diesen Scantyp aktivieren möchten.

API

Führen Sie den Vorgang „API aktivieren“ aus. Geben Sie in der Anfrage die Konto-IDs an, für die Sie Scans aktivieren, und das Idempotenz-Token sowie eine oder mehrere von`EC2`,, oder `LAMBDA_CODE` für`ECR`, oder`LAMBDA`, `resourceTypes` um Scans dieses Typs zu aktivieren.

Scannen von Amazon EC2 EC2-Instances mit Amazon Inspector

Das agentenlose Scannen von Amazon Inspector für Amazon EC2 befindet sich in der Vorschauversion. Ihre Nutzung der Amazon EC2-Scanfunktion ohne Agenten unterliegt Abschnitt 2 der AWS Servicebedingungen („Betas und Vorschauen“).

Das Amazon Inspector EC2-Scannen extrahiert Metadaten aus Ihrer EC2-Instance und vergleicht diese Metadaten dann mit Regeln, die in Sicherheitsempfehlungen gesammelt wurden, um Ergebnisse zu erzielen. Amazon Inspector scannt Instances auf Sicherheitslücken in Paketen und auf Probleme mit der Erreichbarkeit des Netzwerks. Informationen zu den Arten von Ergebnissen, die für diese Probleme erzielt wurden, finden Sie unter. Typen in Amazon Inspector finden

Amazon Inspector führt alle 24 Stunden Scans zur Netzwerkerreichbarkeit durch, während Paketschwachstellenscans je nach der mit der Instance verknüpften Scanmethode in einem variablen Rhythmus durchgeführt werden.

Scan-Methoden

Scans nach Sicherheitslücken in Paketen können mit einer agentenbasierten oder agentenlosen Scanmethode durchgeführt werden. Diese Scanmethoden bestimmen, wie und wann Amazon Inspector das Softwareinventar von einer EC2-Instance für Paketschwachstellenscans erfasst. Bei der agentenbasierten Methode wird der Softwareinventar vom SSM-Agent erfasst, während bei der agentenlosen Methode Amazon EBS-Snapshots anstelle eines Agenten verwendet werden.

Die von Amazon Inspector verwendeten Scanmethoden hängen von der Einstellung für den Scanmodus Ihres Kontos ab. Weitere Informationen finden Sie unterDer Scanmodus wird verwaltet.

Informationen zur Aktivierung von Amazon EC2-Scans finden Sie unterEinen Scantyp aktivieren.

Agentengestütztes Scannen

Agentenbasierte Scans werden kontinuierlich mit dem SSM-Agenten auf allen geeigneten Instanzen durchgeführt. Für agentenbasierte Scans verwendet Amazon Inspector SSM-Verknüpfungen und über diese Verknüpfungen installierte Plugins, um Softwarebestand aus Ihren Instances zu sammeln. Zusätzlich zu Paket-Schwachstellenscans für Betriebssystempakete kann das agentenbasierte Scannen von Amazon Inspector auch Paketschwachstellen in Paketen in Programmiersprachenpaketen in Linux-basierten Instances erkennen. Tiefgreifende Inspektion von Amazon Inspector für Amazon EC2 EC2-Linux-Instances

Der folgende Prozess erklärt, wie Amazon Inspector SSM verwendet, um Inventar zu sammeln und agentenbasierte Scans durchzuführen:

1. Amazon Inspector erstellt SSM-Verknüpfungen in Ihrem Konto, um Inventar aus Ihren Instances zu sammeln. Bei einigen Instance-Typen (Windows und Linux) installieren diese Verknüpfungen Plugins auf einzelnen Instances, um Inventar zu sammeln.
2. Mithilfe von SSM extrahiert Amazon Inspector Paketinventar aus einer Instance.
3. Amazon Inspector bewertet das extrahierte Inventar und generiert Ergebnisse für alle erkannten Sicherheitslücken.

In Frage kommende Instanzen

Amazon Inspector verwendet die agentenbasierte Methode, um eine Instance zu scannen, wenn sie die folgenden Bedingungen erfüllt:

- Die Instance hat ein unterstütztes Betriebssystem. Eine Liste der unterstützten Betriebssysteme finden Sie in der Spalte Unterstützung für agentengestütztes Scannen unter. the section called “Unterstützte Betriebssysteme für Amazon EC2-Scans”
- Die Instance wird nicht von Scans durch Amazon Inspector EC2-Ausschluss-Tags ausgeschlossen.
- Die Instance wird SSM-verwaltet. Anweisungen zur Überprüfung und Konfiguration des Agenten finden Sie unter. Den SSM-Agenten konfigurieren

Verhalten beim Scannen auf Agentenbasis

Bei Verwendung der agentenbasierten Scanmethode initiiert Amazon Inspector in den folgenden Situationen neue Schwachstellenscans von EC2-Instances:

- Wenn Sie eine neue EC2-Instance starten.
- Wenn Sie neue Software auf einer vorhandenen EC2-Instance (Linux und Mac) installieren.
- Wenn Amazon Inspector seiner Datenbank ein neues CVE-Element (Common Vulnerabilities and Exposures) hinzufügt und dieses CVE für Ihre EC2-Instance (Linux und Mac) relevant ist.

Amazon Inspector aktualisiert das Feld Zuletzt gescannt für eine EC2-Instance, wenn ein erster Scan abgeschlossen ist. Danach wird das Feld Zuletzt gescannt aktualisiert, wenn Amazon Inspector das SSM-Inventar auswertet (standardmäßig alle 30 Minuten) oder wenn eine Instance erneut gescannt wird, weil ein neuer CVE, der sich auf diese Instance auswirkt, zur Amazon Inspector Inspector-Datenbank hinzugefügt wurde.

Sie können auf der Kontoverwaltungsseite auf der Registerkarte Instances überprüfen, wann eine EC2-Instance zuletzt auf Sicherheitslücken gescannt wurde, oder indem Sie den Befehl verwenden. ListCoverage

Den SSM-Agenten konfigurieren

Damit Amazon Inspector mithilfe der agentenbasierten Scanmethode Softwareschwachstellen für eine Amazon EC2-Instance erkennen kann, muss es sich bei der Instance um eine verwaltete Instance in Amazon EC2 Systems Manager (SSM) handeln. Bei einer von SSM verwalteten Instance ist der SSM-Agent installiert und läuft, und SSM ist berechtigt, die Instance zu verwalten. Wenn Sie SSM bereits zur Verwaltung Ihrer Instanzen verwenden, sind für agentenbasierte Scans keine weiteren Schritte erforderlich.

Der SSM-Agent wird standardmäßig auf EC2-Instances installiert, die aus einigen Amazon Machine Images (AMIs) erstellt wurden. Weitere Informationen finden Sie unter Über SSM Agent im AWS Systems Manager Benutzerhandbuch. Selbst wenn er installiert ist, müssen Sie den SSM-Agenten möglicherweise manuell aktivieren und SSM die Berechtigung zur Verwaltung Ihrer Instanz erteilen.

Das folgende Verfahren beschreibt, wie Sie eine Amazon EC2 EC2-Instance mithilfe eines IAM-Instance-Profils als verwaltete Instance konfigurieren. Das Verfahren enthält auch Links zu detaillierteren Informationen im AWS Systems Manager Benutzerhandbuch.

AmazonSSMManagedInstanceCoreist die empfohlene Richtlinie, die Sie verwenden sollten, wenn Sie ein Instanzprofil anhängen. Diese Richtlinie verfügt über alle Berechtigungen, die für das Scannen mit Amazon Inspector EC2 erforderlich sind.

> **Note**
>
> Mithilfe der SSM-Standardhostverwaltungskonfiguration können Sie auch die SSM-Verwaltung all Ihrer EC2-Instances automatisieren, ohne IAM-Instanzprofile verwenden zu müssen. Weitere Informationen finden Sie unter Standardkonfiguration für die Host-Verwaltung.

So konfigurieren Sie SSM für eine Amazon EC2 EC2-Instance

1. Wenn es noch nicht von Ihrem Betriebssystemanbieter installiert wurde, installieren Sie den SSM-Agent. Weitere Informationen finden Sie unter Arbeiten mit dem SSM-Agenten.
2. Verwenden Sie den AWS CLI , um zu überprüfen, ob der SSM-Agent ausgeführt wird. Weitere Informationen finden Sie unter Prüfen des Status des SSM-Agents und Starten des Agenten.
3. Erteilen Sie SSM die Erlaubnis, Ihre Instanz zu verwalten. Sie können die Erlaubnis erteilen, indem Sie ein IAM-Instanzprofil erstellen und es an Ihre Instanz anhängen. Wir empfehlen die Verwendung dieser AmazonSSMManagedInstanceCoreRichtlinie, da diese Richtlinie über die Berechtigungen für SSM Distributor, SSM Inventory und SSM State Manager verfügt, die Amazon Inspector für Scans benötigt. Anweisungen zum Erstellen eines Instanzprofils mit diesen Berechtigungen und zum Anhängen einer Instanz finden Sie unter Instanzberechtigungen für Systems Manager Systems Manager konfigurieren.
4. (Optional) Aktivieren Sie automatische Updates für den SSM-Agent. Weitere Informationen finden Sie unter Automatisieren von Updates für den SSM-Agenten.
5. (Optional) Konfigurieren Sie Systems Manager für die Verwendung eines Amazon Virtual Private Cloud (Amazon VPC) -Endpunkts. Weitere Informationen finden Sie unter Amazon VPC-Endpoints erstellen.

> **Important**
>
> Amazon Inspector benötigt eine Systems Manager State Manager-Zuordnung in Ihrem Konto, um den Bestand an Softwareanwendungen zu erfassen. Amazon Inspector erstellt

automatisch eine Assoziation, die aufgerufen wird, `InspectorInventoryCollection-do-not-delete` falls noch keine vorhanden ist.
Amazon Inspector benötigt außerdem eine Ressourcendatensynchronisierung und erstellt automatisch eine, die aufgerufen wird, `InspectorResourceDataSync-do-not-delete` falls noch keine vorhanden ist. Weitere Informationen finden Sie unter Konfiguration der Ressourcendatensynchronisierung für Inventar im AWS Systems Manager Benutzerhandbuch. Für jedes Konto kann eine festgelegte Anzahl von Ressourcendatensynchronisierungen pro Region festgelegt werden. Weitere Informationen finden Sie unter Maximale Anzahl von Ressourcendatensynchronisierungen (AWS-Konto pro Region) in SSM-Endpunkten und -Kontingenten. Wenn Sie dieses Maximum erreicht haben, müssen Sie eine Ressourcendatensynchronisierung löschen, siehe Ressourcendatensynchronisierungen verwalten.

Für das Scannen erstellte SSM-Ressourcen

Amazon Inspector benötigt eine Reihe von SSM-Ressourcen in Ihrem Konto, um Amazon EC2-Scans auszuführen. Die folgenden Ressourcen werden erstellt, wenn Sie das Amazon Inspector EC2-Scannen zum ersten Mal aktivieren:

> **Note**
>
> Wenn eine dieser SSM-Ressourcen gelöscht wird, während Amazon Inspector Amazon EC2-Scannen für Ihr Konto aktiviert ist, versucht Amazon Inspector, sie beim nächsten Scanintervall neu zu erstellen.

`InspectorInventoryCollection-do-not-delete`

Dies ist eine Systems Manager State Manager (SSM) -Zuordnung, die Amazon Inspector verwendet, um Softwareanwendungsinventar aus Ihren Amazon EC2 EC2-Instances zu sammeln. Wenn Ihr Konto bereits über eine SSM-Verknüpfung für die Erfassung von Inventar verfügt`InstanceIds*`, verwendet Amazon Inspector diese, anstatt eine eigene zu erstellen.

`InspectorResourceDataSync-do-not-delete`

Dies ist eine Ressourcendatensynchronisierung, die Amazon Inspector verwendet, um gesammelte Inventardaten von Ihren Amazon EC2 EC2-Instances an einen Amazon S3 S3-Bucket zu senden, der Amazon Inspector gehört. Weitere Informationen finden Sie unter

Konfiguration der Ressourcendatensynchronisierung für Inventar im AWS Systems Manager Benutzerhandbuch.

`InspectorDistributor-do-not-delete`

Dies ist eine SSM-Verknüpfung, die Amazon Inspector zum Scannen von Windows-Instances verwendet. Diese Assoziation installiert das Amazon Inspector SSM-Plugin auf Ihren Windows-Instances. Wenn die Plugin-Datei versehentlich gelöscht wird, wird sie durch diese Verknüpfung beim nächsten Zuordnungsintervall erneut installiert.

`InvokeInspectorSsmPlugin-do-not-delete`

Dies ist eine SSM-Verknüpfung, die Amazon Inspector zum Scannen von Windows-Instances verwendet. Diese Zuordnung ermöglicht Amazon Inspector, Scans mithilfe des Plug-ins zu initiieren. Sie können damit auch benutzerdefinierte Intervalle für Scans von Windows-Instances festlegen. Weitere Informationen finden Sie unter Einstellung benutzerdefinierter Zeitpläne für Instance-Scans Windows.

`InspectorLinuxDistributor-do-not-delete`

Dies ist eine SSM-Assoziation, die Amazon Inspector für Amazon EC2 Linux Deep Inspection verwendet. Diese Assoziation installiert das Amazon Inspector SSM-Plugin auf Ihren Linux-Instances.

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

Dies ist eine SSM-Verbindung, die Amazon Inspector für Amazon EC2 Linux Deep Inspection verwendet. Diese Zuordnung ermöglicht es Amazon Inspector, Scans mithilfe des Plug-ins zu initiieren.

> **Note**
>
> Wenn Sie Amazon Inspector Amazon EC2 Scanning oder Deep Inspection deaktivieren, werden alle SSM-Ressourcen automatisch von den entsprechenden Linux-Hosts deinstalliert.

Scannen ohne Agenten

Amazon Inspector verwendet für berechtigte Instances eine agentenlose Scanmethode, wenn sich Ihr Konto im Hybrid-Scanmodus befindet (der sowohl agentenbasierte als auch agentenlose Scans umfasst). Für Scans ohne Agenten verwendet Amazon Inspector EBS-Snapshots, um ein

Softwareinventar aus Ihren Instances zu erfassen. Instances, die mit der agentenlosen Methode gescannt wurden, werden sowohl auf Sicherheitslücken in Betriebssystempaketen als auch in Anwendungsprogrammiersprachenpaketen gescannt.

> **Note**
>
> Beim Scannen von Linux-Instances auf Sicherheitslücken in Paketen in der Programmiersprache werden bei der agentenlosen Methode alle verfügbaren Pfade gescannt, wohingegen die agentengestützte Suche nur die Standardpfade und zusätzliche Pfade scannt, die Sie als Teil angeben. Tiefgreifende Inspektion von Amazon Inspector für Amazon EC2 EC2-Linux-Instances Dies kann dazu führen, dass dieselbe Instanz unterschiedliche Ergebnisse erzielt, je nachdem, ob sie mit der agentenbasierten Methode oder der agentenlosen Methode gescannt wird.

Der folgende Prozess erklärt, wie Amazon Inspector EBS-Snapshots verwendet, um Inventar zu sammeln und agentenlose Scans durchzuführen:

1. Amazon Inspector erstellt einen EBS-Snapshot aller Volumes, die an die Instance angehängt sind. Während Amazon Inspector es verwendet, wird der Snapshot in Ihrem Konto gespeichert und mit `InspectorScan` einem Tag-Schlüssel und einer eindeutigen Scan-ID als Tag-Wert gekennzeichnet.
2. Amazon Inspector ruft mithilfe von EBS Direct-APIs Daten aus den Snapshots ab und bewertet sie auf Sicherheitslücken. Die Ergebnisse werden für alle erkannten Sicherheitslücken generiert.
3. Amazon Inspector löscht die EBS-Snapshots, die es in Ihrem Konto erstellt hat.

In Frage kommende Instances

Amazon Inspector verwendet die agentenlose Methode, um eine Instance zu scannen, wenn sie die folgenden Bedingungen erfüllt:

- Die Instance hat ein unterstütztes Betriebssystem. Eine Liste der unterstützten Betriebssysteme finden Sie in der Spalte Unterstützung für agentengestütztes Scannen unter. the section called “Unterstützte Betriebssysteme für Amazon EC2-Scans”
- Die Instance wird nicht von Scans durch Amazon Inspector EC2-Ausschluss-Tags ausgeschlossen.
- Die Instance hat den Status `Unmanaged EC2 instanceStale inventory`, oder`No inventory`.

- Die Instance ist EBS-gestützt und hat eines der folgenden Dateisystemformate:
  - `ext3`
  - `ext4`
  - `xfs`

Verhalten beim Scannen ohne Agenten

Wenn Ihr Konto für Hybrid-Scanning konfiguriert ist, führt Amazon Inspector alle 24 Stunden agentenlose Scans auf geeigneten Instances durch. Amazon Inspector erkennt und scannt jede Stunde neue infrage kommende Instances, einschließlich neuer Instances ohne SSM-Agenten oder bereits existierende Instances mit Status, der sich auf geändert hat. `SSM_UNMANAGED`

Amazon Inspector aktualisiert das Feld Zuletzt gescannt für eine Amazon EC2 EC2-Instance, wenn nach einem agentenlosen Scan extrahierte Snapshots aus einer Instance gescannt werden.

Sie können auf der Kontoverwaltungsseite auf der Registerkarte Instances überprüfen, wann eine EC2-Instance zuletzt auf Sicherheitslücken gescannt wurde, oder indem Sie den Befehl verwenden. ListCoverage

Der Scanmodus wird verwaltet

Ihr EC2-Scanmodus bestimmt, welche Scanmethoden Amazon Inspector bei der Durchführung von EC2-Scans in Ihrem Konto verwendet. Sie können den Scanmodus für Ihr Konto auf der Seite mit den EC2-Scaneinstellungen unter Allgemeine Einstellungen einsehen. Eigenständige Konten oder von Amazon Inspector delegierte Administratoren können den Scanmodus ändern. Wenn Sie den Scanmodus als delegierter Administrator von Amazon Inspector festlegen, wird dieser Scanmodus für alle Mitgliedskonten in Ihrer Organisation festgelegt. Amazon Inspector bietet die folgenden Scanmodi:

Agentengestütztes Scannen — In diesem Scanmodus verwendet Amazon Inspector ausschließlich die agentenbasierte Scanmethode, um nach Sicherheitslücken in Paketen zu suchen. Dieser Scanmodus scannt nur SSM-verwaltete Instances in Ihrem Konto, bietet jedoch den Vorteil, dass als Reaktion auf neue CVES oder Änderungen an den Instances kontinuierliche Scans bereitgestellt werden. Agentenbasiertes Scannen bietet auch Amazon Inspector Deep Inspection für berechtigte Instances. Dies ist der Standard-Scanmodus für neu aktivierte Konten.

Hybrid-Scan — In diesem Scanmodus verwendet Amazon Inspector eine Kombination aus agentenbasierten und agentenlosen Methoden, um nach Sicherheitslücken in Paketen zu suchen.

Für berechtigte EC2-Instances, auf denen der SSM-Agent installiert und konfiguriert ist, verwendet Amazon Inspector die agentenbasierte Methode. Für berechtigte Instances, die nicht über SSM verwaltet werden, verwendet Amazon Inspector die agentenlose Methode für berechtigte EBS-gestützte Instances.

Um den Scanmodus zu ändern

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Ihren EC2-Scanmodus ändern möchten.
3. Wählen Sie im seitlichen Navigationsbereich unter Allgemeine Einstellungen die Option EC2-Scaneinstellungen aus.
4. Wählen Sie unter Scanmodus die Option Bearbeiten aus.
5. Wählen Sie einen Scanmodus und dann Änderungen speichern aus.

Instances von Amazon Inspector-Scans ausschließen

Sie können bestimmte Instances taggen, um sie von Amazon Inspector-Scans auszuschließen. Wenn Sie Instances von Scans ausschließen, können Sie verhindern, dass Warnmeldungen nicht bearbeitet werden können. Ausgeschlossene Instanzen werden Ihnen nicht in Rechnung gestellt.

Um eine EC2-Instance von Scans auszuschließen, kennzeichnen Sie diese Instance mit dem folgenden Schlüssel:

- `InspectorEc2Exclusion`

Der Wert ist optional.

Weitere Informationen zum Hinzufügen von Tags finden Sie unter Taggen Ihrer Amazon EC2 EC2-Ressourcen.

Darüber hinaus können Sie ein verschlüsseltes EBS-Volume von Scans ohne Agenten ausschließen, indem Sie den AWS KMS Schlüssel, mit dem das Volume verschlüsselt wurde, mit dem Tag kennzeichnen. `InspectorEc2Exclusion` Weitere Informationen finden Sie unter Kennzeichnen von Schlüsseln

Unterstützte Betriebssysteme

Amazon Inspector scannt unterstützte Mac-, Windows- und Linux-EC2-Instances auf Sicherheitslücken in Betriebssystempaketen. Für Linux-Instances kann Amazon Inspector Ergebnisse für Anwendungsprogrammiersprachenpakete erstellen, die verwendet Tiefgreifende Inspektion von Amazon Inspector für Amazon EC2 EC2-Linux-Instances werden. Für Mac- und Windows-Instances werden nur Betriebssystempakete gescannt.

Informationen zu unterstützten Betriebssystemen, einschließlich der Betriebssysteme, die ohne SSM-Agent gescannt werden können, finden Sie unterUnterstützte Betriebssysteme für Amazon EC2-Scans.

Tiefgreifende Inspektion von Amazon Inspector für Amazon EC2 EC2-Linux-Instances

Amazon Inspector erweitert seinen Amazon EC2-Scanbereich um eine gründliche Inspektion. Mit einer gründlichen Inspektion erkennt Amazon Inspector Paketschwachstellen für Anwendungsprogrammiersprachenpakete in Ihren Linux-basierten Amazon EC2 EC2-Instances.

Amazon Inspector scannt Standardpfade für Programmiersprachen-Paketbibliotheken. Sie können zusätzlich zu den Standardpfaden auch benutzerdefinierte Pfade konfigurieren. Weitere Informationen finden Sie unter Benutzerdefinierte Pfade für die Tiefeninspektion mit Amazon Inspector.

Amazon Inspector führt mithilfe von Daten, die mit dem Amazon Inspector SSM-Plugin gesammelt wurden, gründliche Inspektionsscans durch. Um das Plugin zu verwalten und eine gründliche Inspektion für Linux durchzuführen, erstellt Amazon Inspector automatisch die folgende SSM-Verknüpfung `InvokeInspectorLinuxSsmPlugin-do-not-delete` in Ihrem Konto. Dies tritt auf, wenn Amazon Inspector die Tiefeninspektion aktiviert.

Amazon Inspector sammelt alle 6 Stunden den aktualisierten Anwendungsbestand von Instances zur gründlichen Prüfung.

Eine Liste der Programmiersprachen, die Amazon Inspector für Deep Inspection unterstützt, finden Sie unterUnterstützte Programmiersprachen: Amazon EC2 Deep Inspection.

> **Note**
>
> Deep Inspection wird für Windows- oder Mac-Instances nicht unterstützt.

Deep Inspection aktivieren oder deaktivieren

> **Note**
>
> Deep Inspection wird automatisch als Teil des Amazon EC2-Scans für Konten aktiviert, die Amazon Inspector nach dem 17. April 2023 aktivieren.

Sie können in der Amazon Inspector-Konsole in der Amazon EC2-Scanspalte auf der Kontoverwaltungsseite überprüfen, ob Deep Inspection für ein Konto aktiv ist. Wenn die Tiefeninspektion nicht aktiv ist, steht in dieser Spalte Aktiviert (Tiefeninspektion deaktiviert). Verwenden Sie die API, um den Aktivierungsstatus programmgesteuert zu überprüfen. GetEc2DeepInspectionConfiguration Oder verwenden Sie für mehrere Konten die BatchGetMemberEc2DeepInspectionStatusAPI.

Wenn Sie Amazon Inspector vor dem 17. April 2023 aktiviert haben, können Sie Deep Inspection über das Konsolenbanner oder die UpdateEc2DeepInspectionConfigurationAPI aktivieren. Wenn Sie der delegierte Administrator für eine Organisation in Amazon Inspector sind, können Sie die BatchUpdateMemberEc2DeepInspectionStatusAPI verwenden, um sie für sich und Ihre Mitgliedskonten zu aktivieren.

Sie können Deep Inspection über die UpdateEc2DeepInspectionConfigurationAPI deaktivieren. Mitgliedskonten in einer Organisation können Deep Inspection nicht deaktivieren. Stattdessen muss das Mitgliedskonto von seinem delegierten Administrator mithilfe der BatchUpdateMemberEc2DeepInspectionStatusAPI deaktiviert werden.

Über das Amazon Inspector SSM-Plugin für Linux

Amazon Inspector verwendet das Amazon Inspector SSM-Plugin, um eine gründliche Inspektion Ihrer Linux-Instances durchzuführen. Das Amazon Inspector SSM-Plugin wird automatisch auf Ihren Linux-Instances im folgenden Verzeichnis installiert:`/opt/aws/inspector/bin`. Der Name der ausführbaren Datei lautet`inspectorssmplugin`.

> **Note**
>
> Amazon Inspector verwendet Systems Manager Distributor, um das Plugin in Ihrer Amazon EC2 EC2-Instance bereitzustellen. Systems Manager Distributor unterstützt die Betriebssysteme, die im Systems Manager-Handbuch unter Unterstützte Paketplattformen

und Architekturen aufgeführt sind. Das Betriebssystem Ihrer Amazon EC2 EC2-Instance muss von Systems Manager Distributor und Amazon Inspector für Amazon Inspector unterstützt werden, um Deep Inspection-Scans durchführen zu können.

Amazon Inspector erstellt die folgenden Dateiverzeichnisse, um Daten zu verwalten, die für die Tiefeninspektion mit dem Amazon Inspector SSM-Plugin gesammelt wurden:

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - `packages.txt`In diesem Verzeichnis werden die vollständigen Pfade zu Paketen gespeichert, die bei der Tiefeninspektion entdeckt wurden. Wenn Amazon Inspector dasselbe Paket mehrmals auf Ihrer Instance entdeckt hat, listet diese Datei jeden Speicherort auf, an dem das Paket gefunden wurde.

Amazon Inspector speichert Protokolle für das Plugin im `/var/log/amazon/inspector` Verzeichnis.

Deinstallation des Amazon Inspector SSM-Plug-ins

Wenn die `inspectorssmplugin` Datei versehentlich gelöscht wird, versucht die `InspectorLinuxDistributor-do-not-delete` SSM-Verknüpfung, das Plugin beim nächsten Scanintervall erneut zu installieren.

Wenn Sie das Amazon EC2-Scannen deaktivieren, wird das Plugin automatisch von allen Linux-Hosts deinstalliert.

Benutzerdefinierte Pfade für die Tiefeninspektion mit Amazon Inspector

Sie können benutzerdefinierte Pfade konfigurieren, nach denen Amazon Inspector sucht, wenn er Ihre Linux-Amazon EC2-Instances eingehend inspiziert. Wenn Sie einen benutzerdefinierten Pfad hinzufügen, scannt Amazon Inspector nach Paketen in diesem Verzeichnis und allen Unterverzeichnissen darin.

Alle Konten können bis zu 5 benutzerdefinierte Pfade für ihr individuelles Konto definieren. Wenn Sie der delegierte Administrator für Ihre Organisation sind, können Sie 5 zusätzliche Pfade definieren, die für Ihre gesamte Organisation gelten. Dies entspricht insgesamt bis zu 10 benutzerdefinierten Pfaden, die pro Konto in der Organisation gescannt werden.

Amazon Inspector scannt alle benutzerdefinierten Pfade zusätzlich zu den folgenden Standardpfaden, die für alle Konten gescannt werden:

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

> **Note**
>
> Benutzerdefinierte Pfade müssen lokale Pfade sein. Amazon Inspector scannt keine zugewiesenen Netzwerkpfade wie Network File System (NFS) -Mounts oder Amazon S3 S3-Dateisystem-Mounts.

Formatierung für benutzerdefinierte Pfade

Im Folgenden finden Sie ein Beispiel für das Format für einen benutzerdefinierten Pfad: `/home/usr1/project01`

Ihre benutzerdefinierten Pfade dürfen nicht länger als 256 Zeichen sein.

Es gibt ein Limit von 5.000 Paketen pro Instanz und ein maximales Zeitlimit für die Erfassung des Paketinventars von 15 Minuten. Wir empfehlen, dass Sie versuchen, benutzerdefinierte Pfade zu wählen, um diese Beschränkungen zu umgehen.

Legen Sie in der Konsole einen benutzerdefinierten Pfad fest

Console

Melden Sie sich als delegierter Amazon Inspector-Administrator an und folgen Sie den folgenden Schritten, um benutzerdefinierte Pfade für Ihre Organisation hinzuzufügen.

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie das Lambda-Standardscannen aktivieren möchten.

3. Wählen Sie im seitlichen Navigationsbereich unter Allgemeine Einstellungen die Option EC2-Scaneinstellungen aus.
4. Wählen Sie unter Benutzerdefinierte Pfade für Ihr eigenes Konto die Option Bearbeiten aus, um Pfade für Ihr individuelles Konto hinzuzufügen. Wenn Sie der delegierte Administrator sind, können Sie im Bereich Benutzerdefinierte Pfade für Ihre Organisation die Option Bearbeiten auswählen, um benutzerdefinierte Pfade für alle Konten innerhalb der Organisation hinzuzufügen.
5. Geben Sie Ihre benutzerdefinierten Pfade in die Textfelder ein.
6. Wählen Sie Speichern, um Ihre benutzerdefinierten Pfade zu speichern. Amazon Inspector wird diese Pfade bei seiner nächsten gründlichen Inspektion berücksichtigen.

API

Führen Sie den Befehl UpdateEc2DeepInspectionConfiguration aus. `packagePaths`Geben Sie ein Array von Pfaden an, die gescannt werden sollen.

Unterstützte Programmiersprachen

Bei Linux-Instances kann Amazon Inspector Deep Inspector neben Sicherheitslücken in Betriebssystempaketen auch Ergebnisse für Programmiersprachenpakete für Anwendungen liefern. Bei Mac- und Windows-Instances werden nur Betriebssystempakete gescannt.

Informationen zu den unterstützten Programmiersprachen finden Sie unterUnterstützte Programmiersprachen für Amazon Inspector Deep Inspection.

Scannen von Windows EC2-Instances mit Amazon Inspector

> **Note**
>
> Am 31. August 2022 erweiterte Amazon Inspector seinen Amazon EC2-Scanbereich auf laufende EC2-Instances. Windows

Amazon Inspector erkennt automatisch alle unterstützten Windows Instances und nimmt sie ohne zusätzliche Aktionen in kontinuierliche Scans auf. Informationen darüber, welche Instances unterstützt werden, finden Sie unterUnterstützte Betriebssysteme für Amazon EC2-Scans.

Im Gegensatz zu Scans für Linux-basierte Instances führt Amazon Inspector Windows Scans in regelmäßigen Abständen durch. WindowsInstances werden zunächst bei Entdeckung gescannt und dann alle 6 Stunden gescannt. Das standardmäßige Scanintervall von 6 Stunden ist jedoch einstellbar. Weitere Informationen finden Sie unter Einstellung benutzerdefinierter Zeitpläne für Instance-Scans Windows. Im Folgenden finden Sie eine Übersicht darüber, wie Amazon Inspector Inspector Windows Instances scannt:

1. Wenn das Amazon EC2-Scannen aktiviert ist, erstellt Amazon Inspector neue SSM-Verknüpfungen für Ihre Windows Ressourcen: `InspectorDistributor-do-not-deleteInspectorInventoryCollection-do-not-delete`, und. `InvokeInspectorSsmPlugin-do-not-delete`
2. Die `InspectorDistributor-do-not-delete` SSM-Zuordnung verwendet das `AWS-ConfigureAWSPackage` SSM-Dokument und das `AmazonInspector2-InspectorSsmPlugin` SSM Distributor-Paket, um das Amazon Inspector SSM-Plugin auf Ihren Instances zu installieren. Windows Weitere Informationen finden Sie unter Über das Amazon Inspector SSM-Plugin für Windows.
3. Die `InvokeInspectorSsmPlugin-do-not-delete` SSM Association führt das Amazon Inspector SSM-Plugin in regelmäßigen Abständen aus, um Instance-Daten zu sammeln und Amazon Inspector Inspector-Ergebnisse zu generieren. Standardmäßig beträgt das Intervall alle 6 Stunden. Sie können dies jedoch anpassen, indem Sie mithilfe von SSM einen Cron-Ausdruck oder einen Rate-Ausdruck für die Assoziation festlegen. Weitere Informationen finden Sie im Benutzerhandbuch unter Referenz: Cron- und Rate-Ausdrücke für Systems Manager.AWS Systems Manager

> **Note**
>
> Amazon Inspector stellt aktualisierte OVAL-Definitionsdateien (Open Vulnerability and Assessment Language) im S3-Bucket bereit`inspector2-oval-prod-`*`REGION`*. Dieser S3-Bucket enthält die in Scans verwendeten OVAL-Definitionen und sollte nicht geändert werden. Wenn Sie diese Einstellung ändern, wird Amazon Inspector daran gehindert, nach neuen CVEs zu suchen, sobald diese veröffentlicht werden.

Amazon Inspector-Scananforderungen für Windows Instances

Um eine Windows Instance zu scannen, setzt Amazon Inspector voraus, dass die Instance die folgenden Kriterien erfüllt:

- Die Instance ist eine von SSM verwaltete Instance. Anweisungen zum Einrichten Ihrer Instanz für das Scannen finden Sie unterDen SSM-Agenten konfigurieren.
- Das Instanzbetriebssystem ist eines der unterstützten Windows Betriebssysteme. Eine vollständige Liste der unterstützten Betriebssysteme finden Sie unterUnterstützte Betriebssysteme für Amazon EC2-Scans.
- Auf der Instance ist das Amazon Inspector SSM-Plugin installiert. Amazon Inspector installiert bei Entdeckung automatisch das Amazon Inspector SSM-Plugin für verwaltete Instances. Einzelheiten zum Plugin finden Sie im nächsten Thema.

> **Note**
>
> Wenn Ihr Host in einer Amazon VPC ohne ausgehenden Internetzugang läuft, erfordert das Windows Scannen, dass Ihr Host auf regionale Amazon S3 S3-Endpunkte zugreifen kann. Informationen zur Konfiguration eines Amazon S3 S3-Amazon-VPC-Endpunkts finden Sie unter Erstellen eines Gateway-Endpunkts im Amazon Virtual Private Cloud-Benutzerhandbuch. Wenn Ihre Amazon VPC-Endpunktrichtlinie den Zugriff auf externe S3-Buckets einschränkt, müssen Sie ausdrücklich den Zugriff auf den von Amazon Inspector verwalteten Bucket in Ihrem zulassen AWS-Region , in dem die zur Bewertung Ihrer Instance verwendeten OVAL-Definitionen gespeichert sind. Dieser Bucket hat das folgende Format:. `inspector2-oval-prod-`*`REGION`*

Über das Amazon Inspector SSM-Plugin für Windows

Das Amazon Inspector SSM-Plugin ist erforderlich, damit Amazon Inspector Ihre Windows Instances scannen kann. Das Amazon Inspector SSM-Plugin wird automatisch auf Ihren Windows Instances in installiert`C:\Program Files\Amazon\Inspector`, und die ausführbare Binärdatei wird benannt`InspectorSsmPlugin.exe`.

Die folgenden Dateispeicherorte werden erstellt, um Daten zu speichern, die das Amazon Inspector SSM-Plugin sammelt:

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

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

> **Note**
>
> Standardmäßig wird das Amazon Inspector SSM-Plugin mit niedrigerer Priorität ausgeführt.

Deinstallation des Amazon Inspector SSM-Plug-ins

Wenn die `InspectorSsmPlugin.exe` Datei versehentlich gelöscht wird, installiert die `InspectorDistributor-do-not-delete` SSM-Verknüpfung das Plugin beim nächsten Scanintervall erneut. Windows Wenn Sie das Amazon Inspector SSM-Plugin deinstallieren möchten, können Sie die Aktion Deinstallieren für das `AmazonInspector2-ConfigureInspectorSsmPlugin` Dokument verwenden.

Darüber hinaus wird das Amazon Inspector SSM-Plugin automatisch von allen Windows Hosts deinstalliert, wenn Sie das Amazon EC2-Scannen deaktivieren.

> **Note**
>
> Wenn Sie den SSM Agent deinstallieren, bevor Sie Amazon Inspector deaktivieren, verbleibt das Amazon Inspector SSM-Plugin auf dem Windows Host, sendet aber keine Daten mehr an das Amazon Inspector SSM-Plugin. Weitere Informationen finden Sie unter Amazon Inspector deaktivieren.

Einstellung benutzerdefinierter Zeitpläne für Instance-Scans Windows

Sie können die Zeit zwischen Ihren Windows Amazon EC2 EC2-Instance-Scans anpassen, indem Sie einen Cron-Ausdruck oder einen Rate-Ausdruck für die `InvokeInspectorSsmPlugin-do-not-delete` Zuordnung mithilfe von SSM festlegen. Weitere Informationen finden Sie unter Referenz: Cron- und Rate-Ausdrücke für Systems Manager im AWS Systems Manager Benutzerhandbuch oder verwenden Sie die folgenden Anweisungen.

Wählen Sie eines der folgenden Codebeispiele aus, um die Scan-Taktfrequenz für Windows Instances von der Standardeinstellung 6 Stunden auf 12 Stunden zu ändern, indem Sie entweder einen Rate- oder einen Cron-Ausdruck verwenden.

In den folgenden Beispielen müssen Sie die AssociationIdfür die angegebene Assoziation verwenden. `InvokeInspectorSsmPlugin-do-not-delete` Sie können Ihre abrufen, AssociationIdindem Sie den folgenden AWS CLI Befehl ausführen:

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

> **Note**
>
> Da AssociationIdes sich um Regional handelt, müssen Sie zunächst für jede ID eine eindeutige ID abrufen AWS-Region. Anschließend können Sie den Befehl ausführen, um die Scanfrequenz in jeder Region zu ändern, in der Sie einen benutzerdefinierten Scan-Zeitplan für Windows Instances festlegen möchten.

Example rate expression

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

Example cron expression

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

Scannen von Amazon ECR-Container-Bildern mit Amazon Inspector

Amazon Inspector scannt in Amazon ECR gespeicherte Container-Images auf Softwareschwachstellen, um Erkenntnisse zu Sicherheitslücken in Paketen zu generieren. Informationen zu den Arten von Ergebnissen, die für diese Probleme erstellt wurden, finden Sie unterTypen in Amazon Inspector finden.

Wenn Sie Amazon Inspector-Scans für Amazon ECR aktivieren, legen Sie Amazon Inspector als Ihren bevorzugten Scan-Service für Ihre private Registrierung fest. Dadurch wird das standardmäßige Standardscannen, das von Amazon ECR kostenlos bereitgestellt wird, durch das erweiterte Scannen ersetzt, das über Amazon Inspector bereitgestellt und abgerechnet wird.

Das erweiterte Scannen von Amazon Inspector bietet Ihnen den Vorteil, dass Sicherheitslücken sowohl für Betriebssysteme als auch für Programmiersprachenpakete auf Registrierungsebene gescannt werden können. Sie können die Ergebnisse, die mit dem erweiterten Scannen auf Bildebene entdeckt wurden, für jede Ebene des Bilds in der Amazon ECR-Konsole überprüfen. Darüber hinaus können Sie diese Ergebnisse in anderen Diensten überprüfen und mit ihnen arbeiten, die für grundlegende Scanergebnisse nicht verfügbar sind, einschließlich AWS Security Hub Amazon EventBridge. Sie können die bei Scans entdeckten Ergebnisse in der Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home einsehen. Informationen zum Arbeiten mit Ergebnissen finden Sie unterErgebnisse in Amazon Inspector verwalten.

Anweisungen zur Aktivierung von Amazon ECR-Scans finden Sie unterEinen Scantyp aktivieren.

Scanverhalten für Amazon ECR-Scans

Wenn Sie das ECR-Scannen zum ersten Mal aktivieren und Ihr Repository für kontinuierliches Scannen konfiguriert ist, erkennt Amazon Inspector alle geeigneten Bilder, die Sie innerhalb von 30 Tagen übertragen oder innerhalb der letzten 90 Tage abgerufen haben. Dann scannt Amazon Inspector die erkannten Bilder und setzt ihren Scanstatus auf`active`. Amazon Inspector überwacht weiterhin Bilder, solange sie innerhalb der letzten 90 Tage (standardmäßig) oder innerhalb der von Ihnen konfigurierten ECR-Rescan-Dauer übertragen oder abgerufen wurden. Weitere Informationen finden Sie unter Konfiguration der Dauer des ECR-Neuscans.

Für kontinuierliches Scannen initiiert Amazon Inspector in den folgenden Situationen neue Schwachstellenscans von Container-Images:

- Immer wenn ein neues Container-Image übertragen wird.
- Immer wenn Amazon Inspector seiner Datenbank ein neues CVE-Element (Common Vulnerabilities and Exposures) hinzufügt und dieses CVE für dieses Container-Image relevant ist (nur kontinuierliches Scannen).

Wenn Sie Ihr Repository für On-Push-Scannen konfigurieren, werden Bilder nur gescannt, wenn Sie sie per Push übertragen.

Sie können im Tab Container-Images auf der Kontoverwaltungsseite oder mithilfe der ListCoverageAPI überprüfen, wann ein Container-Image zuletzt auf Sicherheitslücken überprüft wurde. Amazon Inspector aktualisiert das Feld Zuletzt gescannt am eines Amazon ECR-Bilds als Reaktion auf die folgenden Ereignisse:

- Wenn Amazon Inspector einen ersten Scan eines Container-Images abschließt.
- Wenn Amazon Inspector ein Container-Image erneut scannt, weil ein neues CVE-Element (Common Vulnerabilities and Exposures), das sich auf dieses Container-Image auswirkt, zur Amazon Inspector Inspector-Datenbank hinzugefügt wurde.

Unterstützte Betriebssysteme und Medientypen

Informationen zu unterstützten Betriebssystemen finden Sie unterUnterstützte Betriebssysteme für Amazon ECR-Scans.

Amazon Inspector-Scans von Amazon ECR-Repositorys decken die folgenden unterstützten Medientypen ab:

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

> **Note**
>
> Scratch-Bilder und `DockerV2ListMediaType` Bilder werden nicht unterstützt.

Konfiguration erweiterter Scans für Amazon ECR-Repositorys

Wenn Sie Amazon Inspector-Scans für Amazon ECR-Container-Images aktivieren, ändern Sie die Scan-Konfigurationseinstellungen für Ihre private Registrierung. Der Scantyp für Ihre Registrierung wurde von Basic Scanning auf Enhanced Scanning, bereitgestellt von Amazon Inspector, geändert. Weitere Informationen finden Sie unter Scannen von Bildern im Amazon ECR-Benutzerhandbuch.

Sie können die Einstellungen für erweitertes Scannen auf Repository-Ebene in ECR verwalten. Sie können für Ihre Repositorys zwischen kontinuierlichem Scannen und On-Push-Scannen

wählen. Kontinuierliches Scannen umfasst On-Push-Scans und automatische Rescans. Beim On-Push-Scannen wird nur gescannt, wenn Sie ein Bild zum ersten Mal per Push übertragen. Bei beiden Optionen können Sie den Scanbereich mithilfe von Einschlussfiltern verfeinern. Wenn Sie das erweiterte Scannen zum ersten Mal aktivieren, sind Ihre Einstellungen standardmäßig auf Kontinuierliches Scannen aller Repositorys eingestellt.

So konfigurieren Sie Ihre erweiterten Scaneinstellungen

1. Öffnen Sie die Amazon ECR-Konsole unter https://console.aws.amazon.com/ecr/.
2. Wählen Sie in der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der sich die Repositorys befinden, die Sie scannen.
3. Wählen Sie im Navigationsbereich Private Registrierung und anschließend Scannen aus.
4. Vergewissern Sie sich, dass unter Scantyp die Option Erweitertes Scannen ausgewählt ist. Ist dies nicht der Fall, wählen Sie Verbessertes Scannen aus.

   Standardmäßig ist die Option Alle Repositorys kontinuierlich scannen ausgewählt, wodurch die vollständige Amazon Inspector-Scanabdeckung für alle Repositorys aktiviert wird.
5. Deaktivieren Sie die Option Alle Repositorys kontinuierlich scannen, um zu filtern, welche Repositorys kontinuierlich oder per Push gescannt werden.

Weitere Informationen zur Konfiguration erweiterter Scans finden Sie unter Enhanced Scanning verwenden im Amazon ECR-Benutzerhandbuch.

Konfiguration der Dauer des ECR-Neuscans

Die Einstellung für die Dauer des erneuten Scans in ECR bestimmt, wie lange Amazon Inspector kontinuierlich Container-Images in Repositorys überwacht. Sie können die Dauer des erneuten Scans für das Image-Push-Datum und das Image-Pull-Datum konfigurieren. Die Standard-Scandauer für neue Konten, einschließlich neuer Konten, die zu einer Organisation hinzugefügt wurden, beträgt 90 Tage.

Dauer des Bild-Push-Datums

Die Dauer des Image-Push-Datums bestimmt, wie lange Amazon Inspector Bilder kontinuierlich überwacht, nachdem sie nach dem letzten Pull-Datum in Repositorys übertragen wurden. Die folgenden Optionen sind für die Dauer des erneuten Scans verfügbar:

- 14 Tage

- 30 Tage
- 60 Tage
- 90 Tage (Standard)
- 180 Tage
- Nutzungsdauer

Dauer des Bild-Abruf-Datums

Die Dauer des Bild-Abruf-Datums bestimmt, wie lange Amazon Inspector Bilder nach dem letzten Abrufdatum kontinuierlich überwacht. Die folgenden Optionen sind für die Dauer des erneuten Scans verfügbar:

- 14 Tage
- 30 Tage
- 60 Tage
- 90 Tage (Standard)
- 180 Tage

Amazon Inspector überwacht ein Bild weiterhin und scannt es erneut, solange es innerhalb der konfigurierten Push- und Pull-Daten übertragen oder abgerufen wurde. Wenn das Bild nicht innerhalb der konfigurierten Push- und Pull-Daten übertragen oder abgerufen wurde, beendet Amazon Inspector die Überwachung.

> **Note**
>
> Wenn Amazon Inspector die Überwachung eines Bilds beendet, setzt es den Statuscode für den Bildscan auf `inactive` und den Ursachencode auf`expired`. Anschließend wird geplant, dass alle zugehörigen Bildergebnisse geschlossen werden.

Stellen Sie die Dauer des erneuten Scans so ein, dass sie am besten zu Ihrer Umgebung passt. Wenn Sie beispielsweise häufig Bilder erstellen, wählen Sie eine kürzere Scandauer. Wenn Sie Bilder über einen längeren Zeitraum verwenden, sollten Sie auch eine längere Scandauer wählen.

Wenn Sie die Dauer des erneuten Scans von einem delegierten Administratorkonto aus konfigurieren, wendet Amazon Inspector die Einstellung auf alle Mitgliedskonten in der Organisation an.

Um die Dauer des ECR-Neuscans zu konfigurieren

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Allgemeine Einstellungen und anschließend ECR-Scaneinstellungen aus.
3. Wählen Sie in den ECR-Scaneinstellungen unter Dauer des erneuten ECR-Scans die Dauer des Bild-Push-Datums und die Dauer des Bild-Pulldatums aus, die Sie festlegen möchten.
4. Wählen Sie Speichern. Ihre neuen Einstellungen werden sofort übernommen.

> **Note**
>
> Wenn Sie die Dauer des Push-Datums verlängern, wendet Amazon Inspector die Änderung auf alle aktiv gescannten Bilder in Repositorys an, die für kontinuierliches Scannen konfiguriert sind. Inaktive Bilder bleiben jedoch inaktiv, auch wenn Sie sie innerhalb der neuen Dauer per Push übertragen haben.

AWS Lambda Scanfunktionen mit Amazon Inspector

Die Unterstützung von Amazon Inspector für AWS Lambda Funktionen bietet kontinuierliche, automatisierte Bewertungen von Sicherheitslücken für Lambda-Funktionen und -Layer. Amazon Inspector bietet zwei Arten des Scannens für Lambda. Diese Scantypen suchen nach verschiedenen Arten von Sicherheitslücken.

Standard-Scanning mit Amazon Inspector Lambda

Dies ist der standardmäßige Lambda-Scantyp. Das Lambda-Standardscannen scannt Anwendungsabhängigkeiten innerhalb einer Lambda-Funktion und ihrer Schichten auf Paketschwachstellen. Weitere Informationen finden Sie unter Lambda-Standardabtastung.

Scannen von Lambda-Code mit Amazon Inspector

Dieser Scantyp scannt den benutzerdefinierten Anwendungscode in Ihren Funktionen und Ebenen auf Code-Schwachstellen. Sie können entweder den Lambda-Standardscan einzeln oder zusammen mit dem Lambda-Codescan aktivieren. Weitere Informationen finden Sie unter Scannen von Lambda-Code mit Amazon Inspector.

Wenn Sie Lambda-Scanning aktivieren, erstellt Amazon Inspector die folgenden AWS CloudTrail serviceverknüpften Kanäle in Ihrem Konto:

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

Amazon Inspector verwaltet diese Kanäle und verwendet sie, um Ihre CloudTrail Ereignisse im Hinblick auf Scans zu überwachen. Weitere Informationen zu serviceverknüpften Kanälen finden Sie unter Dienstverknüpfte Kanäle mit der CloudTrail AWS CLI anzeigen.

> **Note**
>
> Die von Amazon Inspector erstellten serviceverknüpften Kanäle ermöglichen es Ihnen, CloudTrail Ereignisse in Ihrem Konto so zu sehen, als ob Sie eine CloudTrail Spur gehabt hätten. Wir empfehlen Ihnen jedoch, eigene CloudTrail zu erstellen, um Ereignisse für Ihr Konto zu verwalten.

Anweisungen zur Aktivierung von Lambda-Funktionsscans finden Sie unterEinen Scantyp aktivieren.

Scanverhalten beim Scannen mit Lambda-Funktionen

Nach der Aktivierung scannt Amazon Inspector alle Lambda-Funktionen, die in den letzten 90 Tagen in Ihrem Konto aufgerufen oder aktualisiert wurden. Amazon Inspector initiiert Schwachstellenscans von Lambda-Funktionen in den folgenden Situationen:

- Sobald Amazon Inspector eine vorhandene Lambda-Funktion entdeckt.
- Wenn Sie eine neue Lambda-Funktion für den Lambda-Service bereitstellen.
- Wenn Sie ein Update für den Anwendungscode oder die Abhängigkeiten einer vorhandenen Lambda-Funktion oder ihrer Layer bereitstellen.

- Immer wenn Amazon Inspector seiner Datenbank ein neues CVE-Element (Common Vulnerabilities and Exposures) hinzufügt und dieses CVE für Ihre Funktion relevant ist.

Amazon Inspector überwacht jede Lambda-Funktion während ihrer gesamten Lebensdauer, bis sie entweder gelöscht oder vom Scannen ausgeschlossen wird.

Sie können im Tab Lambda-Funktionen auf der Kontoverwaltungsseite oder mithilfe der API überprüfen, wann eine Lambda-Funktion zuletzt auf Sicherheitslücken überprüft wurde. ListCoverage Amazon Inspector aktualisiert das Feld Zuletzt gescannt am für eine Lambda-Funktion als Reaktion auf die folgenden Ereignisse:

- Wenn Amazon Inspector einen ersten Scan einer Lambda-Funktion abschließt.
- Wenn eine Lambda-Funktion aktualisiert wird.
- Wenn Amazon Inspector eine Lambda-Funktion erneut scannt, weil ein neues CVE-Element, das sich auf diese Funktion auswirkt, zur Amazon Inspector Inspector-Datenbank hinzugefügt wurde.

Unterstützte Laufzeiten und geeignete Funktionen

Amazon Inspector unterstützt unterschiedliche Laufzeiten für Lambda-Standardscans und Lambda-Code-Scans. Eine Liste der unterstützten Laufzeiten für jeden Scan-Typ finden Sie unter und. Unterstützte Laufzeiten: Amazon Inspector Lambda Standard-Scanning Unterstützte Laufzeiten: Amazon Inspector Lambda-Code-Scanning

Zusätzlich zu einer unterstützten Laufzeit muss eine Lambda-Funktion die folgenden Kriterien erfüllen, um für Amazon Inspector-Scans in Frage zu kommen:

- Die Funktion wurde in den letzten 90 Tagen aufgerufen oder aktualisiert.
- Die Funktion ist markiert`$LATEST`.
- Die Funktion ist nicht von Scans nach Tags ausgeschlossen.

> **Note**
>
> Lambda-Funktionen, die in den letzten 90 Tagen nicht aufgerufen oder geändert wurden, werden automatisch von Scans ausgeschlossen. Amazon Inspector setzt das Scannen einer automatisch ausgeschlossenen Funktion fort, wenn sie erneut aufgerufen wird oder wenn Änderungen am Lambda-Funktionscode vorgenommen werden.

Standard-Scanning mit Amazon Inspector Lambda

Das Standard-Scannen von Amazon Inspector Lambda identifiziert Softwareschwachstellen in den Abhängigkeiten von Anwendungspaketen, die Sie Ihrem Lambda-Funktionscode und den Lambda-Funktionsschichten hinzufügen. Wenn Ihre Lambda-Funktion beispielsweise eine Version des `python-jwt` Pakets mit einer bekannten Sicherheitslücke verwendet, generiert der Lambda-Standardscan einen Befund für diese Funktion.

Wenn Amazon Inspector eine Sicherheitslücke in den Abhängigkeiten Ihrer Lambda-Funktionsanwendung feststellt, erstellt Amazon Inspector eine detaillierte Suche nach dem Typ der Sicherheitslücke in Paketen.

Anweisungen zur Aktivierung eines Scan-Typs finden Sie unterEinen Scantyp aktivieren.

> **Note**
>
> Das Lambda-Standardscannen scannt nicht die AWS SDK-Abhängigkeit, die standardmäßig in der Lambda-Laufzeitumgebung installiert ist. Amazon Inspector scannt nur Abhängigkeiten, die mit dem Funktionscode hochgeladen oder von einer Ebene übernommen wurden.

> **Note**
>
> Wenn Sie das Standardscannen von Amazon Inspector Lambda deaktivieren, wird auch das Scannen von Amazon Inspector Lambda-Code deaktiviert.

Funktionen vom Lambda-Standardscan ausschließen

Sie können bestimmte Funktionen taggen, um sie von Amazon Inspector Lambda-Standardscans auszuschließen. Wenn Sie Funktionen von Scans ausschließen, können Sie verhindern, dass Warnmeldungen nicht bearbeitet werden können.

Um eine Lambda-Funktion vom Lambda-Standardscan auszuschließen, kennzeichnen Sie die Funktion mit dem folgenden Schlüssel-Wert-Paar:

- Schlüssel: `InspectorExclusion`
- Wert: `LambdaStandardScanning`

Um eine Funktion vom Lambda-Standardscan auszuschließen

1. Öffnen Sie die Lambda-Konsole unter https://console.aws.amazon.com/lambda/.
2. Wählen Sie Funktionen aus.
3. Wählen Sie in der Funktionstabelle den Namen einer Funktion aus, die Sie vom Amazon Inspector Lambda-Standardscan ausschließen möchten.
4. Wählen Sie Konfiguration und dann im Menü Tags aus.
5. Wählen Sie Tags verwalten und dann Neues Tag hinzufügen aus.
6. Geben Sie in das Feld Schlüssel `InspectorExclusion` und dann in das Feld Wert die Eingabe ein`LambdaStandardScanning`.
7. Wählen Sie Speichern, um das Tag hinzuzufügen und Ihre Funktion vom Amazon Inspector Lambda-Standardscan auszuschließen.

Weitere Informationen zum Hinzufügen von Tags in Lambda finden Sie unter Verwenden von Tags in Lambda-Funktionen.

Scannen von Lambda-Code mit Amazon Inspector

> **Important**
>
> Beim Codescan werden Codefragmente aus Lambda-Funktionen erfasst, um erkannte Sicherheitslücken hervorzuheben. Diese Snippets können hartcodierte Anmeldeinformationen oder andere vertrauliche Materialien im Klartext enthalten.

Das Lambda-Codescanning von Amazon Inspector scannt den benutzerdefinierten Anwendungscode innerhalb einer Lambda-Funktion auf Codeschwachstellen auf der Grundlage bewährter AWS Sicherheitsmethoden. Durch das Scannen von Lambda-Code können Injektionsfehler, Datenlecks, schwache Kryptografie oder fehlende Verschlüsselung in Ihrem Code erkannt werden. Informationen zu den verfügbaren Regionen finden Sie unter. Verfügbarkeit regionsspezifischer Feature

Das Lambda-Standardscannen ist eine Funktion, die die Abhängigkeiten von Anwendungspaketen bewertet, die in einer Funktion für häufig auftretende Sicherheitslücken und Risiken (CVE) verwendet werden. Sie können das Lambda-Code-Scannen zusammen mit dem Lambda-Standard-Scanning aktivieren.

Amazon Inspector bewertet Ihren Anwendungscode für Lambda-Funktionen mithilfe von automatisiertem Denken und maschinellem Lernen, das Ihren Anwendungscode analysiert, um die allgemeine Einhaltung der Sicherheitsbestimmungen zu gewährleisten. Es identifiziert Richtlinienverstöße und Sicherheitslücken auf der Grundlage interner Detektoren, die in Zusammenarbeit mit Amazon entwickelt wurden CodeGuru. Eine Liste möglicher Erkennungen finden Sie in der CodeGuru Detector Library.

Wenn Amazon Inspector eine Sicherheitslücke im Anwendungscode Ihrer Lambda-Funktion entdeckt, erstellt Amazon Inspector eine detaillierte Suche nach dem Typ der Code-Sicherheitslücke. Dieser Feststellungstyp umfasst die genaue Position des Problems im Code, einen Codeausschnitt, der das Problem zeigt, und einen Lösungsvorschlag. Die vorgeschlagene Behebung umfasst plug-and-play Codeblöcke, mit denen Sie Ihre anfälligen Codezeilen ersetzen können. Diese vorgeschlagenen Codekorrekturen werden zusätzlich zu den allgemeinen Anleitungen zur Behebung dieses Fehlers bereitgestellt.

> **Important**
>
> Vorschläge zur Codekorrektur basieren auf automatisiertem Denken und generativer künstlicher Intelligenz und funktionieren daher möglicherweise nicht wie beabsichtigt. Sie sind für die Vorschläge zur Codekorrektur verantwortlich, die Sie übernehmen. Lesen Sie sich die Vorschläge zur Codekorrektur immer durch, bevor Sie sie übernehmen. Möglicherweise müssen Sie Änderungen an den Vorschlägen zur Codekorrektur vornehmen, um sicherzustellen, dass Ihr Code wie beabsichtigt funktioniert. Weitere Informationen finden Sie in der Richtlinie für verantwortungsvolle KI.

Verschlüsselung Ihres Codes bei der Entdeckung von Sicherheitslücken

Codefragmente, die im Zusammenhang mit der Entdeckung einer Code-Schwachstelle mithilfe von Lambda-Code-Scanning erkannt wurden, werden vom Dienst gespeichert. CodeGuru Standardmäßig wird zur Verschlüsselung Ihres Codes ein AWS eigener Schlüssel verwendet, der von gesteuert CodeGuru wird. Sie können jedoch Ihren eigenen, vom Kunden verwalteten Schlüssel für die Verschlüsselung über die Amazon Inspector API verwenden. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand für den Code in Ihren Ergebnissen

Das Lambda-Code-Scannen kann zusammen mit dem Lambda-Standard-Scanning aktiviert werden. Anweisungen zur Aktivierung eines Scan-Typs finden Sie unter. Einen Scantyp aktivieren

Funktionen vom Lambda-Code-Scannen ausschließen

Sie können bestimmte Funktionen taggen, um sie von Amazon Inspector Lambda-Codescans auszuschließen. Wenn Sie Funktionen von Scans ausschließen, können Sie verhindern, dass Warnmeldungen nicht bearbeitet werden können.

Um eine Lambda-Funktion aus Amazon Inspector auszuschließen, kennzeichnen Lambda-Codescans die Funktion mit dem folgenden Schlüssel-Wert-Paar:

- Schlüssel: `InspectorCodeExclusion`
- Wert: `LambdaCodeScanning`

Um eine Funktion vom Lambda-Code-Scan auszuschließen

1. Melden Sie sich bei der Lambda-Konsole unter https://console.aws.amazon.com/lambda/ an.
2. Wählen Sie Funktionen aus.
3. Wählen Sie in der Funktionstabelle den Namen einer Funktion aus, die Sie vom Amazon Inspector Lambda-Code-Scan ausschließen möchten.
4. Wählen Sie Konfiguration und dann im Menü Tags aus.
5. Wählen Sie Tags verwalten und dann Neues Tag hinzufügen aus.
6. Geben Sie in das Feld Schlüssel `InspectorCodeExclusion` und dann in das Feld Wert die Eingabe ein`LambdaCodeScanning`.
7. Wählen Sie Speichern, um das Tag hinzuzufügen und Ihre Funktion vom Amazon Inspector Lambda-Code-Scan auszuschließen.

Weitere Informationen zum Hinzufügen von Tags in Lambda finden Sie unter Verwenden von Tags in Lambda-Funktionen.

Deaktivieren eines Scantyps

Sie können einen neuen Amazon Inspector-Scantyp jederzeit deaktivieren. Wenn Sie einen Scantyp deaktivieren, verlieren Sie den Zugriff auf alle vorhandenen Ergebnisse, die mit diesem Scantyp erzielt wurden. Wenn Sie den Scan-Typ reaktivieren, werden Ihre berechtigten Ressourcen gescannt und Amazon Inspector liefert neue Ergebnisse. Um Ihre Ergebnisdaten aufzuzeichnen, können Sie Ihre Ergebnisse exportieren, bevor Sie sie deaktivieren. Weitere Informationen finden Sie unter Ergebnisberichte aus Amazon Inspector exportieren.

Wenn Sie einen Scantyp deaktivieren, können je nach deaktiviertem Scantyp bestimmte Änderungen an diesem AWS Konto vorgenommen werden. Die folgenden Änderungen treten auf, wenn Sie diese Suchtypen deaktivieren:

- Amazon EC2-Scannen — Wenn Sie Amazon Inspector Amazon EC2-Scans für ein Konto deaktivieren, werden die folgenden von Amazon Inspector verwendeten SSM-Verknüpfungen gelöscht:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`. Darüber hinaus wird das Amazon Inspector SSM-Plugin, das über diese Verknüpfung installiert wurde, von all Ihren Windows Hosts entfernt. Weitere Informationen finden Sie unter Instanzen scannen Windows.
- Amazon ECR-Scannen — Wenn Sie das Scannen von Amazon ECR-Container-Bildern für ein Konto deaktivieren, ändert sich der Amazon ECR-Scantyp für dieses Konto von Erweitertes Scannen mit Amazon Inspector zu Standard-Scannen mit Amazon ECR.
- Lambda-Standardscan — Wenn Sie den Lambda-Standardscan in einem Konto deaktivieren, wird der Lambda-Code-Scan deaktiviert, sofern der Code-Scan ebenfalls aktiv war. Außerdem wird der mit dem CloudTrail Service verknüpfte Kanal gelöscht, der bei der Aktivierung des Scannens erstellt wurde.

Scans deaktivieren

Wenn Sie alle Scanarten für ein Konto deaktivieren, wird Amazon Inspector für dieses Konto in diesem Konto deaktiviert. AWS-Region Weitere Informationen finden Sie unter Amazon Inspector deaktivieren.

Um dieses Verfahren für eine Umgebung mit mehreren Konten abzuschließen, folgen Sie diesen Schritten, während Sie als delegierter Amazon Inspector-Administrator angemeldet sind.

Console

Um Scans zu deaktivieren

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.

2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Scans deaktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Kontoverwaltung aus.
4. Wählen Sie die Registerkarte Konten, um den Scanstatus eines Kontos anzuzeigen.
5. Aktivieren Sie das Kontrollkästchen jedes Kontos, für das Sie Scans deaktivieren möchten.
6. Wählen Sie Aktionen und wählen Sie unter den Deaktivierungsoptionen den Scantyp aus, den Sie deaktivieren möchten.
7. (Empfohlen) Wiederholen Sie diese Schritte AWS-Region für jeden Scantyp, für den Sie diesen Scantyp deaktivieren möchten.

API

Führen Sie den Vorgang „API deaktivieren“ aus. Geben Sie in der Anfrage die Konto-IDs an, für die Sie Scans deaktivieren möchten, und `resourceTypes` geben Sie eine oder mehrere der,, oder an, an, an`EC2`, an, an`ECR`, an`LAMBDA`, um Scans `LAMBDA_CODE` zu deaktivieren.

Center for Internet Security (CIS) scannt nach EC2-Instances

Wenn Sie Amazon Inspector EC2-Scans für ein Konto aktivieren, ermöglichen Sie Amazon Inspector, CIS-Scans durchzuführen oder zu planen. Amazon Inspector CIS scannt die Betriebssysteme Ihrer Amazon EC2 EC2-Instances, um festzustellen, ob sie gemäß den Best-Practice-Empfehlungen des Center for Internet Security konfiguriert sind. Das CIS Security Benchmarks-Programm bietet branchenübliche Konfigurationsgrundlagen und bewährte Methoden für die sichere Konfiguration eines Systems. Weitere Informationen finden Sie unter Was sind CIS-Benchmarks?

Amazon Inspector führt CIS-Scans auf Amazon EC2 EC2-Zielinstanzen auf der Grundlage der Instance-Tags und des Scan-Zeitplans durch, die Sie in einer Scan-Konfiguration definieren. Für jede Ziel-Instance führt Amazon Inspector eine Reihe von Prüfungen an der Instance durch. Bei jeder Prüfung wird bewertet, ob Ihre Systemkonfiguration einer bestimmten CIS-Benchmark-Empfehlung entspricht. Jeder Scheck hat eine CIS-Check-ID und einen Titel, was direkt mit einer CIS-Benchmark-Empfehlung für diese Plattform korreliert. Wenn ein Scan abgeschlossen ist, können Sie sich die Ergebnisse ansehen und sehen, welche Prüfungen Ihre Instance für dieses System bestanden, fehlgeschlagen oder übersprungen hat.

EC2-Instance-Anforderungen für Amazon Inspector CIS-Scans

Um einen CIS-Scan auf Ihrer Instance auszuführen, setzt Amazon Inspector voraus, dass die Instance die folgenden Kriterien erfüllt:

- Das Instance-Betriebssystem ist eines der unterstützten Betriebssysteme für CIS-Scans. Eine vollständige Liste der unterstützten Betriebssysteme finden Sie unterUnterstützte Betriebssysteme: CIS-Scanning.
- Die Instance ist eine von Amazon EC2 Systems Manager (SSM) verwaltete Instance. Weitere Informationen finden Sie unter Arbeiten mit dem SSM-Agenten.
- Auf der Instance ist das Amazon Inspector SSM-Plugin installiert. Amazon Inspector installiert dieses Plugin automatisch für SSM-verwaltete Instances.
- Die Instance verfügt über ein Instance-Profil, das SSM Berechtigungen zur Verwaltung der Instance und Amazon Inspector zur Ausführung von CIS-Scans für diese Instance gewährt. Um diese Berechtigungen zu gewähren, fügen Sie die ManagedCispolicy Richtlinien AmazonInspector2FullAccess, AmazonSSM ManagedInstanceCore und AmazonInspector2 einer IAM-Rolle hinzu und fügen Sie diese Rolle Ihrer Instance als Instance-Profil hinzu. Anweisungen

zum Erstellen und Anhängen eines Instance-Profils finden Sie unter Arbeiten mit IAM-Rollen im Amazon EC2 EC2-Benutzerhandbuch.

> **Note**
>
> Die Aktivierung von Amazon Inspector Deep Inspection ist nicht mehr erforderlich, wenn ein CIS-Scan auf einer Instance ausgeführt wird. Wenn Sie Deep Inspection deaktivieren, setzt Amazon Inspector die Installation des SSM-Agenten fort, aber das Plugin wird nicht mehr aufgerufen, um Deep Inspection auszuführen. Das bedeutet, dass die folgende Verknüpfung in Ihrem Konto vorhanden sein wird:. `InspectorLinuxDistributor-do-not-delete`

CIS-Scans ausführen

Sie können einen CIS-Scan entweder einmal auf Anforderung oder als geplanten wiederkehrenden Scan ausführen. Um einen Scan auszuführen, müssen Sie zunächst eine Scankonfiguration erstellen.

Wenn Sie eine Scankonfiguration erstellen, geben Sie Tag-Schlüssel-Wert-Paare an, die für Ziel-Instances verwendet werden sollen. Wenn Sie der von Amazon Inspector delegierte Administrator für eine Organisation sind, können Sie in der Scan-Konfiguration mehrere Konten angeben, und Amazon Inspector sucht in jedem dieser Konten nach Instances mit den angegebenen Tags. Sie wählen das CIS-Benchmark-Level für den Scan. Für jeden Benchmark unterstützt CIS ein Level-1- und Level-2-Profil, das als Ausgangsbasis für verschiedene Sicherheitsstufen dient, die in verschiedenen Umgebungen möglicherweise erforderlich sind.

- Stufe 1 — empfiehlt grundlegende Sicherheitseinstellungen, die auf jedem System konfiguriert werden können. Die Implementierung dieser Einstellungen sollte kaum oder gar nicht zu Betriebsunterbrechungen führen. Ziel dieser Empfehlungen ist es, die Anzahl der Eintrittspunkte in Ihre Systeme zu verringern und so Ihre allgemeinen Cybersicherheitsrisiken zu verringern.
- Stufe 2 — empfiehlt erweiterte Sicherheitseinstellungen für Hochsicherheitsumgebungen. Die Implementierung dieser Einstellungen erfordert Planung und Koordination, um das Risiko geschäftlicher Auswirkungen zu minimieren. Ziel dieser Empfehlungen ist es, Sie bei der Einhaltung gesetzlicher Vorschriften zu unterstützen.

Stufe 2 erweitert Ebene 1. Wenn Sie Level 2 wählen, sucht Amazon Inspector nach allen Konfigurationen, die für Level 1 und Level 2 empfohlen werden.

Nachdem Sie die Parameter für Ihren Scan definiert haben, können Sie wählen, ob Sie ihn als einmaligen Scan, der nach Abschluss der Konfiguration ausgeführt wird, oder als wiederkehrender Scan ausführen möchten. Wiederkehrende Scans können täglich, wöchentlich oder monatlich zu einem Zeitpunkt Ihrer Wahl ausgeführt werden.

> **Tip**
>
> Wir empfehlen, einen Tag und eine Uhrzeit zu wählen, die sich während der Ausführung des Scans am wenigsten auf Ihr System auswirken.

Um eine CIS-Scankonfiguration zu erstellen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite den Ort aus, AWS-Region an dem Sie einen CIS-Scan ausführen möchten.
3. Wählen Sie im Navigationsbereich unter On-Demand-Scans die Option CIS-Scans aus.
4. Wählen Sie Neuen Scan erstellen aus.
   a. Geben Sie einen Namen für die Scan-Konfiguration ein.
   b. Geben Sie als Zielressource den Schlüssel und den entsprechenden Wert eines Tags auf den Instanzen ein, die Sie scannen möchten. Sie können insgesamt 25 Tags angeben, die in den Scan aufgenommen werden sollen, und für jeden Schlüssel können Sie bis zu fünf verschiedene Werte angeben.
   c. Wählen Sie ein CIS-Benchmark-Level. Sie können Level 1 für grundlegende Sicherheitskonfigurationen oder Level 2 für erweiterte Sicherheitskonfigurationen wählen.
5. Geben Sie für Zielkonten an, welche Konten in den Scan aufgenommen werden sollen. Ein eigenständiges Konto oder ein Mitglied einer Organisation kann Self auswählen, um eine Scan-Konfiguration für sein Konto zu erstellen. Ein von Amazon Inspector delegierter Administrator kann Alle Konten auswählen, um alle Konten innerhalb der Organisation anzusprechen, oder Konten angeben und eine Untergruppe von Mitgliedskonten als Ziel angeben. Der delegierte Administrator kann `SELF` anstelle einer Konto-ID eine Konto-ID eingeben, um eine Scan-Konfiguration für sein eigenes Konto zu erstellen. Weitere Informationen finden Sie unter Überlegungen zur Verwaltung von Amazon Inspector CIS-Scans in einer AWS Organisation.

6. Wählen Sie einen Zeitplan für die Scans. Wählen Sie zwischen Einmaliger Scan, der ausgeführt wird, sobald Sie die Scankonfiguration erstellt haben, und Wiederkehrenden Scans, die zu der von Ihnen festgelegten Zeit ausgeführt werden, bis sie gelöscht werden.
7. Wählen Sie Erstellen, um die Erstellung der Scankonfiguration abzuschließen.

CIS-Scankonfigurationen anzeigen und bearbeiten

Sie können Ihre zuvor geplanten Scans jederzeit anzeigen oder bearbeiten.

Um eine CIS-Scankonfiguration anzuzeigen oder zu bearbeiten

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite den Ort aus, an AWS-Region dem Sie Ihre CIS-Scan-Konfiguration erstellt haben.
3. Wählen Sie im Navigationsbereich unter On-Demand-Scans die Option CIS-Scans aus.
4. Wählen Sie Geplant, um die Konfigurationen für geplante Scans anzuzeigen.
5. Wählen Sie in der Spalte „Name der Scan-Konfiguration“ ein Element aus, um die Details für diese Scan-Konfiguration zu öffnen.
6. (Optional) Wählen Sie Bearbeiten, um die Parameter dieses Scans zu ändern.

Ergebnisse Ihrer CIS-Scans anzeigen

Amazon Inspector erstellt bei jeder Ausführung einer Scan-Konfiguration einen Scanauftrag und sammelt die Ergebnisse des Scans unter einer eindeutigen Scan-ID.

Die Scanergebnisse sind nach Abschluss des Scans 90 Tage lang verfügbar. Sie können die Ergebnisse des Scans nach Scheck oder nach Zielressource aggregiert anzeigen.

Nach Schecks aggregierte Scanergebnisse

Die Ergebnisse des Scans sind nach jeder einzelnen Prüfung gruppiert, die während des Scans durchgeführt wurde. Für jede Prüfung erhalten Sie einen Bericht darüber, wie viele Ressourcen bestanden, ausgefallen sind oder übersprungen wurden.

Nach Ressourcen aggregierte Scanergebnisse

Die Ergebnisse des Scans sind nach jeder Ressource gruppiert, auf die die Scankonfiguration abzielte. Für jede Ressource erhalten Sie einen Bericht darüber, welche Prüfungen eine Ressource für diese Ressource bestanden, fehlgeschlagen oder übersprungen hat.

Um die Scanergebnisse anzuzeigen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite den Ort aus, AWS-Region an dem Sie die Scanergebnisse anzeigen möchten.
3. Wählen Sie im Navigationsbereich unter On-Demand-Scans die Option CIS-Scans aus.
4. Wählen Sie in der Spalte Scan-ID die ID des Scans aus, für den Sie Ergebnisse anzeigen möchten.
5. Wählen Sie aus, wie Sie Ihre Scanergebnisse anzeigen möchten:
   - Wählen Sie die Registerkarte Checks, um die nach Prüfungen aggregierten Scan-Ergebnisse anzuzeigen.
     - Wählen Sie für eine aufgeführte Prüfung in der Spalte Ressourcenstatus eine Zahl aus „Bestanden“, „Übersprungen“ oder „Fehlgeschlagen“ aus, um eine nach diesem Status und dieser Prüfung gefilterte Ansicht der Ressourcen zu öffnen.
   - Wählen Sie die Registerkarte Gescannte Ressourcen, um die nach Ressourcen aggregierten Scanergebnisse anzuzeigen.
     - Wählen Sie eine Ressource aus, um einen Detailbereich zu öffnen, in dem die Prüfungen aufgeführt sind, die die Ressource bestanden, fehlgeschlagen oder übersprungen hat.
6. (Optional) Verwenden Sie die Filterleiste in beiden Ansichten, um Ihre Ergebnisse zu verfeinern.

Sie können die Ergebnisse eines CIS-Scans über die Konsole oder die API herunterladen.

Um Scan-Ergebnisse herunterzuladen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit der AWS-Region Auswahl in der oberen rechten Ecke der Seite den Ort aus, AWS-Region an dem Sie die Scanergebnisse anzeigen möchten.

3. Wählen Sie im Navigationsbereich unter On-Demand-Scans die Option CIS-Scans aus.
4. Wählen Sie in der Spalte Scan-ID die ID des Scans aus, für den Sie Ergebnisse anzeigen möchten.
5. Wählen Sie Herunterladen aus. Wenn Sie der delegierte Administrator sind, können Sie wählen, ob Sie Ergebnisse für bestimmte Mitgliedskonten herunterladen möchten.

Überlegungen zur Verwaltung von Amazon Inspector CIS-Scans in einer AWS Organisation

Wenn CIS-Scans innerhalb einer Organisation ausgeführt werden, interagieren Mitgliedskonten und von Amazon Inspector delegierte Administratoren auf unterschiedliche Weise mit CIS-Scankonfigurationen und Scanergebnissen.

Wenn ein delegierter Administrator eine CIS-Scan-Konfiguration für alle Konten oder eine Liste von Mitgliedskonto-IDs erstellt, ist die Organisation Eigentümer dieser Scan-Konfiguration. Unabhängig davon, welches Konto der aktuelle delegierte Administrator ist, kann er die Scankonfigurationen verwalten, die der Organisation gehören, auch wenn sie von einem anderen Konto erstellt wurden. CIS-Scankonfigurationen, die der Organisation gehören, haben einen ARN, der die Organisations-ID als Besitzer auflistet, und zwar nach dem folgenden Muster:`arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId`*. Die Konto-ID ist die ID des Verwaltungskontos der Organizations.

> **Important**
>
> Sie können den CIS-Scankonfigurationen, die der Organisation gehören, keine Tags hinzufügen.

Wenn ein delegierter Administrator eine Scankonfiguration erstellt und `SELF` als Zielkonto angibt, ist sein Konto für diese Scankonfiguration verantwortlich. Selbst wenn sie ihr Unternehmen verlassen, können sie diese Scankonfiguration weiterhin verwalten.

> **Note**
>
> Ein delegierter Administrator kann die Ziele einer Scankonfiguration, auf die es abzielt`SELF`, nicht ändern.

Scankonfigurationen, die von Mitgliedskonten, eigenständigen Konten oder delegierten Administratoren `SELF` als Ziel erstellt wurden, gehören dem Konto, das sie erstellt hat. Diese CIS-Scankonfigurationen haben einen ARN, der dieses Konto nach dem Muster als Besitzer auflistet:`arn:aws:inspector2:Region:111122223333:owner/111122223333/cis-configuration/scanId`. Die Konto-ID ist das Konto, das den Scan erstellt hat.

Ein Mitgliedskonto in einer Organisation kann Scankonfigurationen für sein eigenes Konto erstellen. Der delegierte Administrator kann die von Mitgliedern erstellten Scankonfigurationen einsehen, sie jedoch nicht bearbeiten oder löschen. Wenn ein Mitgliedskonto die Organisation verlässt, kann der delegierte Administrator die von diesem Konto erstellten Scankonfigurationen nicht mehr sehen.

Der delegierte Administrator kann die Scanergebnisse aller Konten in der Organisation einsehen, auch die von Mitgliedern geplanten. Ein Mitgliedskonto kann die Ergebnisse aller CIS-Scans nach Ressourcen in seinem Konto einsehen, einschließlich der vom delegierten Administrator geplanten.

Amazon Inspector-eigene Amazon S3 S3-Buckets, die für Amazon Inspector CIS-Scans verwendet werden

Amazon Inspector stellt aktualisierte OVAL-Definitionsdateien (Open Vulnerability and Assessment Language) bereit, die für CIS-Scans erforderlich sind. In der folgenden Tabelle sind alle Amazon Inspector-eigenen Amazon S3 S3-Buckets mit OVAL-Definitionen aufgeführt, die CIS-Scan je nach unterstützter Version verwendet. AWS-Region Die Buckets sollten bei Bedarf in VPCs auf die Zulassungsliste gesetzt werden.

> **Note**
>
> Die Details für jeden der folgenden Amazon S3-Buckets, die Amazon Inspector gehören, können sich nicht ändern. Die Liste kann jedoch aktualisiert werden, um neue AWS-Regionen Support-Neuigkeiten widerzuspiegeln. Sie können diese Buckets nicht für andere Amazon S3 S3-Operationen oder in Ihren eigenen Amazon S3 S3-Buckets verwenden.

CIS-Bucket	AWS-Region
`cis-datasets-prod-arn-5908f6f`	Europe (Stockholm)
`cis-datasets-prod-bah-8f88801`	Middle East (Bahrain)

CIS-Bucket	AWS-Region
`cis-datasets-prod-bjs-0f40506`	China (Peking)
`cis-datasets-prod-bom-435a167`	Asien-Pazifik (Mumbai)
`cis-datasets-prod-cdg-f3a9c58`	Europa (Paris)
`cis-datasets-prod-cgk-09eb12f`	Asien-Pazifik (Jakarta)
`cis-datasets-prod-cmh-63030b9`	USA Ost (Ohio)
`cis-datasets-prod-cpt-02c5c6f`	Afrika (Kapstadt)
`cis-datasets-prod-dub-984936f`	Europa (Irland)
`cis-datasets-prod-fra-6eb96eb`	Europa (Frankfurt)
`cis-datasets-prod-gru-de69f99`	Südamerika (São Paulo)
`cis-datasets-prod-hkg-8e30800`	Asien-Pazifik (Hongkong)
`cis-datasets-prod-iad-8438411`	USA Ost (Nord-Virginia)
`cis-datasets-prod-icn-f4eff1c`	Asien-Pazifik (Seoul)
`cis-datasets-prod-kix-5743b21`	Asien-Pazifik (Osaka)
`cis-datasets-prod-lhr-8b1fbd0`	Europa (London)
`cis-datasets-prod-mxp-7b1bbce`	Europa (Milan)
`cis-datasets-prod-nrt-464f684`	Asien-Pazifik (Tokio)
`cis-datasets-prod-osu-5bead6f`	AWS GovCloud (US-Ost)
`cis-datasets-prod-pdt-adadf9c`	AWS GovCloud (US-West)
`cis-datasets-prod-pdx-acfb052`	USA West (Oregon)
`cis-datasets-prod-sfo-1515ba8`	USA West (Nordkalifornien)

CIS-Bucket	AWS-Region
`cis-datasets-prod-sin-309725b`	Asien-Pazifik (Singapur)
`cis-datasets-prod-syd-f349107`	Asien-Pazifik (Sydney)
`cis-datasets-prod-yul-5e0c95e`	Kanada (Zentral)
`cis-datasets-prod-zhy-5a8eacb`	China (Ningxia)
`cis-datasets-prod-zrh-67e0e3d`	Europa (Zürich)

Bewertung der Abdeckung Ihrer AWS Umgebung durch Amazon Inspector

Um Ihnen bei der Einschätzung und Interpretation der Reichweite Ihrer AWS Umgebung durch Amazon Inspector zu helfen, finden Sie auf der Seite Kontoverwaltung auf der Amazon Inspector-Konsole Statistiken und Details zum Status der Amazon Inspector-Scans für Ihre Konten und Ressourcen. Auf dieser Seite können Sie aggregierte Statistiken und andere Daten für Ihre Ressourcen einsehen. Sie können auch eine eingehende Analyse der Reichweite von Amazon Inspector für einzelne Ressourcen durchführen und die Ergebnisse für bestimmte Ressourcen detailliert überprüfen. Wenn Sie der delegierte Amazon Inspector-Administrator für eine Organisation sind, enthalten die Daten Statistiken und Details für alle Konten in Ihrer Organisation.

Um die Abdeckung Ihrer AWS Umgebung durch Amazon Inspector zu beurteilen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Kontoverwaltung aus.
3. Wählen Sie auf der Seite Kontoverwaltung die Registerkarte für eine von fünf verschiedenen Deckungsansichten aus:
   - Konten, für den Versicherungsschutz auf Kontoebene.
   - Instances, für die Abdeckung von Amazon Elastic Compute Cloud (Amazon EC2) -Instances.
   - Repositorys, um die Repositorys von Amazon Elastic Container Registry (Amazon ECR) abzudecken.
   - Bilder, für die Berichterstattung über Amazon ECR-Container-Images.
   - Lambda, zur Abdeckung von Lambda-Funktionen.

In den Themen dieses Abschnitts werden die Informationen beschrieben, die auf jeder Registerkarte bereitgestellt werden, einschließlich des Scanstatus, den eine einzelne Ressource haben kann.

Themen

- Bewertung der Reichweite von Amazon ECR-Container-Images
- Bewertung des Funktionsumfangs AWS Lambda

Bewertung der Deckung auf Kontoebene

Wenn Ihr Konto nicht Teil einer Organisation ist oder nicht das delegierte Amazon Inspector-Administratorkonto für eine Organisation ist, finden Sie auf der Registerkarte Konten Informationen über Ihr Konto und den Status des Ressourcenscans für Ihr Konto. Auf dieser Registerkarte können Sie das Scannen für alle oder nur bestimmte Arten von Ressourcen für Ihr Konto aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Automatisiertes Scannen von Ressourcen mit Amazon Inspector.

Wenn es sich bei Ihrem Konto um das delegierte Amazon Inspector-Administratorkonto für eine Organisation handelt, bietet die Registerkarte Konten automatische Aktivierungseinstellungen für Konten in Ihrer Organisation und listet alle Konten in Ihrer Organisation auf. Für jedes Konto gibt die Liste an, ob Amazon Inspector für das Konto aktiviert ist, und wenn ja, welche Arten von Ressourcenscans für das Konto aktiviert sind. Als delegierter Administrator können Sie auf dieser Registerkarte die Einstellungen für die automatische Aktivierung für Ihr Unternehmen ändern. Sie können auch bestimmte Arten des Ressourcenscans für einzelne Mitgliedskonten aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Die Aktivierung von Amazon Inspector scannt nach Mitgliedskonten.

Bewertung der Abdeckung von Amazon EC2 EC2-Instances

Auf der Registerkarte Instances werden Amazon EC2 EC2-Instances in Ihrer AWS Umgebung angezeigt. Die Listen sind auf den folgenden Registerkarten in Gruppen unterteilt:

- Alle — Zeigt alle Instanzen in Ihrer Umgebung an. In der Spalte Status wird der aktuelle Scanstatus für eine Instance angezeigt.
- Scannen — Zeigt alle Instances an, die Amazon Inspector in Ihrer Umgebung aktiv überwacht und scannt.
- Nicht scannen — Zeigt alle Instances an, die Amazon Inspector in Ihrer Umgebung nicht überwacht und scannt. Die Spalte Grund gibt an, warum Amazon Inspector eine Instance nicht überwacht und scannt.

  Eine EC2-Instance kann aus verschiedenen Gründen auf der Registerkarte „Nicht gescannt“ angezeigt werden. Amazon Inspector verwendet AWS Systems Manager (SSM) und den SSM-

Agenten, um Ihre EC2-Instances automatisch zu überwachen und auf Sicherheitslücken zu scannen. Wenn auf einer Instance der SSM-Agent nicht ausgeführt wird, sie keine AWS Identity and Access Management (IAM-) Rolle hat, die Systems Manager unterstützt, oder auf der kein unterstütztes Betriebssystem oder keine unterstützte Architektur ausgeführt wird, kann Amazon Inspector die Instance nicht überwachen und scannen. Weitere Informationen finden Sie unter Amazon EC2 EC2-Instances scannen.

Auf jeder Registerkarte gibt die Spalte Konto an, wer Eigentümer einer AWS-Konto Instance ist.

EC2-Instance-Tags — In dieser Spalte werden die mit der Instance verknüpften Tags angezeigt. Anhand dieser Spalte können Sie feststellen, ob Ihre Instance anhand von Stichwörtern von Scans ausgeschlossen wurde.

Betriebssystem — In dieser Spalte wird der Betriebssystemtyp angezeigt. Dieser kann, `WINDOWS` `MACLINUX`, oder `UNKNOWN` sein.

Überwacht mit — In dieser Spalte wird angezeigt, ob Amazon Inspector für diese Instance die agentenbasierte oder die agentenlose Scanmethode verwendet.

Zuletzt gescannt — In dieser Spalte wird angezeigt, wann Amazon Inspector diese Ressource zuletzt auf Sicherheitslücken überprüft hat. Die Häufigkeit, mit der Amazon Inspector Scans durchführt, hängt von der Scanmethode ab, die zum Scannen der Instance verwendet wird.

Um weitere Details zu einer EC2-Instance zu überprüfen, wählen Sie den Link in der Spalte EC2-Instance. Amazon Inspector zeigt dann Details zur Instance und aktuelle Ergebnisse für die Instance an. Um die Details eines Ergebnisses zu überprüfen, wählen Sie den Link in der Titelspalte. Informationen zu diesen Details finden Sie unterAmazon Inspector findet Einzelheiten.

Statuswerte für Amazon EC2 EC2-Instances scannen

Für eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance sind die möglichen Statuswerte wie folgt:

- Aktive Überwachung — Amazon Inspector überwacht und scannt die Instance kontinuierlich.
- EC2-Instance gestoppt — Amazon Inspector hat die Suche nach der Instance angehalten, da sich die Instance in einem gestoppten Zustand befindet. Alle vorhandenen Ergebnisse bleiben bestehen, bis die Instance beendet wird. Wenn die Instance neu gestartet wird, fährt Amazon Inspector automatisch mit dem Scannen nach der Instance fort.

- Interner Fehler — Ein interner Fehler ist aufgetreten, als Amazon Inspector versuchte, die Instance zu scannen. Amazon Inspector behebt den Fehler automatisch und setzt den Scanvorgang so schnell wie möglich fort.
- Kein Inventar — Amazon Inspector konnte das Inventar der Softwareanwendung, das nach der Instance gescannt werden soll, nicht finden. Die Amazon Inspector Inspector-Verknüpfungen für die Instance wurden möglicherweise gelöscht oder konnten möglicherweise nicht ausgeführt werden.

  Um dieses Problem zu beheben, stellen Sie bitte AWS Systems Manager sicher, dass die `InspectorInventoryCollection-do-not-delete` Zuordnung besteht und ihr Zuordnungsstatus erfolgreich ist. Verwenden Sie außerdem AWS Systems Manager Fleet Manager, um das Softwareanwendungsinventar für die Instanz zu überprüfen.
- Ausstehende Deaktivierung — Amazon Inspector hat das Scannen der Instance beendet. Die Instance wird deaktiviert, bis die Bereinigungsaufgaben abgeschlossen sind.
- Erster Scan steht aus — Amazon Inspector hat die Instance für einen ersten Scan in die Warteschlange gestellt.
- Ressource beendet — Die Instance wurde beendet. Amazon Inspector bereinigt derzeit die vorhandenen Ergebnisse und Deckungsdaten für die Instanz.
- Veraltetes Inventar — Amazon Inspector war nicht in der Lage, ein aktualisiertes Softwareanwendungsinventar zu sammeln, das innerhalb der letzten 7 Tage für die Instance erfasst wurde.

  Um dieses Problem zu beheben, stellen Sie AWS Systems Manager sicher, dass die erforderlichen Amazon Inspector Inspector-Verknüpfungen vorhanden sind und für die Instance ausgeführt werden. Verwenden Sie außerdem AWS Systems Manager Fleet Manager, um das Softwareanwendungsinventar für die Instance zu überprüfen.
- Nicht verwaltete EC2-Instance — Amazon Inspector überwacht oder scannt die Instance nicht. Die Instance wird nicht von verwaltet. AWS Systems Manager

  Um dieses Problem zu beheben, können Sie das von AWS Systems Manager Automation AWSSupport-TroubleshootManagedInstance runbookbereitgestellte Tool verwenden. Nachdem Sie die Konfiguration AWS Systems Manager für die Verwaltung der Instance vorgenommen haben, beginnt Amazon Inspector automatisch, die Instance kontinuierlich zu überwachen und zu scannen.
- Nicht unterstütztes Betriebssystem — Amazon Inspector überwacht oder scannt die Instance nicht. Die Instance verwendet ein Betriebssystem oder eine Architektur, die Amazon Inspector

nicht unterstützt. Eine Liste der Betriebssysteme, die Amazon Inspector unterstützt, finden Sie unterUnterstützte Betriebssysteme für Amazon EC2-Scans.

- Aktive Überwachung mit teilweisen Fehlern — Dieser Status bedeutet, dass das EC2-Scannen zwar aktiv ist, aber es liegen Fehler vor. Tiefgreifende Inspektion von Amazon Inspector für Amazon EC2 EC2-Linux-Instances Bei tiefgreifenden Inspektionen kann es sich um folgende Fehler handeln:
  - Das Limit für die Erfassung von Paketen mit Tiefeninspektion wurde überschritten — Die Instance hat das Limit von 5000 Paketen für die Tiefeninspektion von Amazon Inspector überschritten. Um die Tiefeninspektion für diese Instance fortzusetzen, können Sie versuchen, die mit dem Konto verknüpften benutzerdefinierten Pfade anzupassen.
  - Das tägliche SSM-Inventarlimit für Deep Inspection wurde überschritten — Der SSM-Agent konnte kein Inventar an Amazon Inspector senden, da das SSM-Kontingent für die pro Instance und Tag gesammelten SSM-Inventardaten für diese Instance bereits erreicht wurde. Weitere Informationen finden Sie unter Amazon EC2 Systems Manager Endpoints and Quotas.
  - Zeitlimit für die Abholung bei Tiefeninspektion überschritten — Amazon Inspector konnte den Paketbestand nicht extrahieren, da die Paketabholzeit den maximalen Schwellenwert von 15 Minuten überschritten hat.
  - Deep Inspection hat kein Inventar — Das Amazon Inspector SSM-Plugin war noch nicht in der Lage, ein Inventar von Paketen für diese Instanz zu sammeln. Dies ist normalerweise das Ergebnis eines ausstehenden Scans. Wenn dieser Status jedoch nach 6 Stunden weiterhin besteht, verwenden Sie Amazon EC2 Systems Manager, um sicherzustellen, dass die erforderlichen Amazon Inspector Inspector-Verknüpfungen vorhanden sind und für die Instance ausgeführt werden.

Einzelheiten zur Konfiguration der Scaneinstellungen für eine EC2-Instance finden Sie unter. Amazon EC2 EC2-Instances scannen

Bewertung der Abdeckung von Amazon ECR-Repositorien

Auf der Registerkarte Repositorys werden Amazon ECR-Repositorys in Ihrer Umgebung angezeigt. AWS Die Listen sind auf den folgenden Registerkarten in Gruppen unterteilt:

- Alle — Zeigt alle Repositorys in Ihrer Umgebung an. In der Spalte Status wird der aktuelle Scanstatus für ein Repository angezeigt.

- Aktiviert — Zeigt alle Repositorys an, für deren Überwachung und Scannen Amazon Inspector in Ihrer Umgebung konfiguriert ist. Die Spalte Status zeigt den aktuellen Scanstatus für ein Repository an.
- Nicht aktiviert — Zeigt alle Repositorys an, die Amazon Inspector in Ihrer Umgebung nicht überwacht und scannt. Die Spalte Grund gibt an, warum Amazon Inspector ein Repository nicht überwacht und scannt.

Auf jeder Registerkarte gibt die Spalte Konto an, wer Eigentümer eines Repositorys ist. AWS-Konto

Um weitere Details zu einem Repository zu überprüfen, wählen Sie den Namen des Repositorys. Amazon Inspector zeigt dann eine Liste der Container-Images im Repository sowie Details zu jedem Bild an. Zu den Details gehören das Image-Tag, der Image-Digest und der Scanstatus. Sie enthalten auch wichtige Ergebnisstatistiken, wie z. B. die Anzahl kritischer Ergebnisse für das Bild. Wählen Sie das Bild-Tag für das Bild aus, um weitere Informationen zu erhalten und die unterstützenden Daten für die Suche nach Statistiken zu überprüfen.

Statuswerte für Amazon ECR-Repositorys scannen

Für ein Amazon Elastic Container Registry (Amazon ECR) -Repository sind die möglichen Statuswerte:

- Aktiviert (Kontinuierlich) — Für ein Repository überwacht Amazon Inspector kontinuierlich die Bilder in diesem Repository. Die erweiterte Scan-Einstellung für das Repository ist auf kontinuierliches Scannen eingestellt. Amazon Inspector scannt neue Bilder zunächst, wenn sie übertragen werden, und scannt Bilder erneut, wenn ein neues CVE veröffentlicht wird, das für dieses Bild relevant ist. Amazon Inspector überwacht weiterhin die Bilder in diesem Repository für die von Ihnen konfigurierte ECR-Scandauer.
- Aktiviert (bei Push) — Amazon Inspector scannt automatisch einzelne Container-Images im Repository, wenn ein neues Image übertragen wird. Das erweiterte Scannen ist für das Repository aktiviert und so eingestellt, dass bei Push gescannt wird.
- Zugriff verweigert — Amazon Inspector darf weder auf das Repository noch auf Container-Images im Repository zugreifen.

  Um dieses Problem zu beheben, stellen Sie sicher, dass AWS Identity and Access Management (IAM-) Richtlinien für das Repository Amazon Inspector den Zugriff auf das Repository ermöglichen.

- Deaktiviert (Manuell) — Amazon Inspector überwacht oder scannt keine Container-Images im Repository. Die Amazon ECR-Scaneinstellung für das Repository ist auf einfaches manuelles Scannen eingestellt.

  Um mit dem Scannen von Bildern im Repository mit Amazon Inspector zu beginnen, ändern Sie die Scan-Einstellung für das Repository auf Erweitertes Scannen und wählen Sie dann, ob Bilder kontinuierlich oder nur dann gescannt werden sollen, wenn ein neues Bild übertragen wird.
- Aktiviert (bei Push) — Amazon Inspector scannt automatisch einzelne Container-Images im Repository, wenn ein neues Image übertragen wird. Die erweiterte Scan-Einstellung für das Repository ist auf Scan on Push eingestellt.
- Interner Fehler — Ein interner Fehler ist aufgetreten, als Amazon Inspector versuchte, das Repository zu scannen. Amazon Inspector behebt den Fehler automatisch und setzt den Scanvorgang so schnell wie möglich fort.

Für Einzelheiten zur Konfiguration der Scan-Einstellungen für RepositorysAmazon ECR-Container-Bilder scannen.

Bewertung der Reichweite von Amazon ECR-Container-Images

Auf der Registerkarte Images werden Amazon ECR-Container-Images in Ihrer AWS Umgebung angezeigt. Die Listen sind auf den folgenden Registerkarten in Gruppen unterteilt:

- Alle — Zeigt alle Container-Images in Ihrer Umgebung an. In der Spalte Status wird der aktuelle Scanstatus für ein Bild angezeigt.
- Scannen — Zeigt alle Container-Images an, für deren Überwachung und Scannen Amazon Inspector in Ihrer Umgebung konfiguriert ist. Die Spalte Status zeigt den aktuellen Scanstatus für ein Bild an.
- Nicht scannen — Zeigt alle Container-Images an, die Amazon Inspector in Ihrer Umgebung nicht überwacht und scannt. Die Spalte Grund gibt an, warum Amazon Inspector ein Bild nicht überwacht und scannt.

  Ein Container-Bild kann aus verschiedenen Gründen auf der Registerkarte Nicht aktiviert angezeigt werden. Das Bild ist möglicherweise in einem Repository gespeichert, für das Amazon Inspector-Scans nicht aktiviert sind, oder Amazon ECR-Filterregeln verhindern, dass dieses Repository gescannt wird. Oder das Bild wurde nicht innerhalb der Anzahl von Tagen übertragen oder abgerufen, die Sie für die Dauer des erneuten ECR-Scans konfiguriert haben. Weitere Informationen finden Sie unter Konfiguration der Dauer des ECR-Neuscans.

Auf jeder Registerkarte gibt die Spalte Repository-Name den Namen des Repositorys an, das ein Container-Image speichert. In der Spalte Konto wird der AWS-Konto Eigentümer des Repositorys angegeben. In der Spalte Zuletzt gescannt wird angezeigt, wann Amazon Inspector diese Ressource zuletzt auf Sicherheitslücken überprüft hat. Dies kann Prüfungen beinhalten, wenn die Suchmetadaten aktualisiert wurden, wenn das Anwendungsinventar der Ressource aktualisiert wurde oder wenn als Reaktion auf einen neuen CVE ein erneuter Scan durchgeführt wird. Weitere Informationen finden Sie unter Scanverhalten für Amazon ECR-Scans.

Um weitere Details zu einem Container-Image zu überprüfen, wählen Sie den Link in der Spalte ECR-Container-Image. Amazon Inspector zeigt dann Details zum Bild und aktuelle Ergebnisse für das Bild an. Um die Details eines Ergebnisses zu überprüfen, wählen Sie den Link in der Titelspalte. Informationen zu diesen Details finden Sie unterAmazon Inspector findet Einzelheiten.

Statuswerte für Amazon ECR-Container-Images scannen

Für ein Amazon Elastic Container Registry-Container-Image sind die möglichen Statuswerte wie folgt:

- Aktive Überwachung (kontinuierlich) — Amazon Inspector überwacht das Bild kontinuierlich, und jedes Mal, wenn ein neuer relevanter CVE veröffentlicht wird, werden neue Scans daran durchgeführt. Die Dauer des Amazon ECR-Rescans für das Bild wird jedes Mal aktualisiert, wenn das Bild übertragen oder abgerufen wird. Das erweiterte Scannen ist für das Repository aktiviert, in dem das Bild gespeichert ist, und die erweiterte Scan-Einstellung für das Repository ist auf kontinuierliches Scannen eingestellt.
- Aktiviert (bei Push) — Amazon Inspector scannt das Bild automatisch jedes Mal, wenn ein neues Bild übertragen wird. Das erweiterte Scannen ist für das Repository aktiviert, in dem das Bild gespeichert ist, und die erweiterte Scan-Einstellung für das Repository ist auf Scannen bei Push eingestellt.
- Interner Fehler — Ein interner Fehler ist aufgetreten, als Amazon Inspector versuchte, das Container-Image zu scannen. Amazon Inspector behebt den Fehler automatisch und setzt den Scanvorgang so schnell wie möglich fort.
- Erster Scan steht aus — Amazon Inspector hat das Bild für einen ersten Scan in die Warteschlange gestellt.
- Die Scanberechtigung ist abgelaufen (Fortlaufend) — Amazon Inspector hat den Scanvorgang für das Bild ausgesetzt. Das Bild wurde innerhalb des Zeitraums, den Sie für automatische erneute Scans von Bildern im Repository angegeben haben, nicht aktualisiert. Sie können das Bild per Push oder Pull verschieben, um den Scanvorgang fortzusetzen.

- Die Scanberechtigung ist abgelaufen (On Push) — Amazon Inspector hat den Scanvorgang für das Bild ausgesetzt. Das Bild wurde innerhalb des Zeitraums, den Sie für automatische erneute Scans von Bildern im Repository angegeben haben, nicht aktualisiert. Sie können das Bild per Push übertragen, um den Scanvorgang fortzusetzen.
- Manuelles Scannen der Frequenz (Manuell) — Amazon Inspector scannt das Amazon ECR-Container-Image nicht. Die Amazon ECR-Scaneinstellung für das Repository, in dem das Bild gespeichert ist, ist auf einfaches manuelles Scannen eingestellt. Um das automatische Scannen des Bilds mit Amazon Inspector zu starten, ändern Sie die Repository-Einstellung auf Verbessertes Scannen und wählen Sie dann, ob Bilder kontinuierlich oder nur gescannt werden sollen, wenn ein neues Bild übertragen wird.
- Nicht unterstütztes Betriebssystem — Amazon Inspector überwacht oder scannt das Bild nicht. Das Bild basiert auf einem Betriebssystem, das Amazon Inspector nicht unterstützt, oder es verwendet einen Medientyp, den Amazon Inspector nicht unterstützt.

  Eine Liste der Betriebssysteme, die Amazon Inspector unterstützt, finden Sie unterUnterstützte Betriebssysteme für Amazon ECR-Scans. Eine Liste der Medientypen, die Amazon Inspector unterstützt, finden Sie unter Unterstützte Medientypen.

Einzelheiten zur Konfiguration der Scaneinstellungen für Repositorys und Bilder finden Sie unterAmazon ECR-Container-Bilder scannen.

Bewertung des Funktionsumfangs AWS Lambda

Auf der Registerkarte Lambda werden Lambda-Funktionen in Ihrer AWS Umgebung angezeigt. Auf dieser Seite gibt es zwei Tabellen, eine mit Details zur Funktionsabdeckung für das Lambda-Standardscannen und eine andere für das Scannen von Lambda-Code. Sie können Funktionen auf der Grundlage der folgenden Registerkarten gruppieren:

- Alle — Zeigt alle Lambda-Funktionen in Ihrer Umgebung an. Die Spalte Status zeigt den aktuellen Scanstatus für eine Lambda-Funktion an.
- Scannen — Zeigt die Lambda-Funktionen an, für deren Scannen Amazon Inspector konfiguriert ist. Die Spalte Status zeigt den aktuellen Scanstatus für jede Lambda-Funktion an.
- Nicht scannen — Zeigt die Lambda-Funktionen an, für deren Scannen Amazon Inspector nicht konfiguriert ist. Die Spalte Grund gibt an, warum Amazon Inspector eine Funktion nicht überwacht und scannt.

Eine Lambda-Funktion kann aus verschiedenen Gründen auf der Registerkarte Nicht scannen angezeigt werden. Die Lambda-Funktion gehört möglicherweise zu einem Konto, das nicht zu Amazon Inspector hinzugefügt wurde, oder Filterregeln verhindern, dass diese Funktion gescannt wird. Weitere Informationen finden Sie unter AWS Lambda Funktionen zum Scannen.

Auf jeder Registerkarte gibt die Spalte Funktionsname den Namen der Lambda-Funktion an. In der Spalte Konto wird derjenige angegeben AWS-Konto , dem die Funktion gehört. Runtime gibt die Laufzeit der Funktion an. Die Spalte Status zeigt den aktuellen Scanstatus für jede Lambda-Funktion an. Resource Tags zeigt die Tags an, die auf die Funktion angewendet wurden. In der Spalte Zuletzt gescannt wird angezeigt, wann Amazon Inspector diese Ressource zuletzt auf Sicherheitslücken überprüft hat. Dies kann Prüfungen beinhalten, wenn die Suchmetadaten aktualisiert wurden, wenn das Anwendungsinventar der Ressource aktualisiert wurde oder wenn als Reaktion auf einen neuen CVE ein erneuter Scan durchgeführt wird. Weitere Informationen finden Sie unter Scanverhalten beim Scannen mit Lambda-Funktionen.

Statuswerte für Funktionen werden gescannt AWS Lambda

Für eine Lambda-Funktion sind folgende Statuswerte möglich:

- Aktive Überwachung — Amazon Inspector überwacht und scannt kontinuierlich Lambda-Funktionen. Kontinuierliches Scannen umfasst einen ersten Scan neuer Funktionen, wenn sie in das Repository übertragen werden, und automatische erneute Scans von Funktionen, wenn sie aktualisiert werden oder wenn neue Common Vulnerabilities and Exposures (CVEs) veröffentlicht werden.
- Nach Tag ausgeschlossen — Amazon Inspector scannt diese Funktion nicht, da sie von Tag-Scans ausgeschlossen wurde.
- Die Scanberechtigung ist abgelaufen — Amazon Inspector überwacht diese Funktion nicht, da seit dem letzten Aufruf oder der letzten Aktualisierung mindestens 90 Tage vergangen sind.
- Interner Fehler — Beim Versuch von Amazon Inspector, die Funktion zu scannen, ist ein interner Fehler aufgetreten. Amazon Inspector behebt den Fehler automatisch und setzt den Scanvorgang so schnell wie möglich fort.
- Erster Scan steht aus — Amazon Inspector hat die Funktion für einen ersten Scan in die Warteschlange gestellt.
- Nicht unterstützt — Die Lambda-Funktion hat eine Laufzeit, die nicht unterstützt wird.

Verwaltung mehrerer Konten in Amazon Inspector mit Organizations

Sie können Amazon Inspector verwenden, um mehrere Konten zu verwalten, die über AWS Organizations verknüpft sind. Um mehrere Amazon Inspector-Konten zu verwalten, bestimmt das Organisationsverwaltungskonto ein Konto innerhalb der Organisation als delegiertes Administratorkonto für Amazon Inspector. Der delegierte Administrator verwaltet Amazon Inspector für die Organisation und erhält spezielle Berechtigungen zur Ausführung von Aufgaben im Namen Ihrer Organisation. Zu diesen Aufgaben gehören die Aktivierung oder Deaktivierung von Scans für Mitgliedskonten, die Anzeige aggregierter Suchdaten aus der gesamten Organisation sowie die Erstellung und Verwaltung von Unterdrückungsregeln.

> **Note**
>
> Um Amazon Inspector programmgesteuert für mehrere Konten in mehreren zu aktivieren AWS-Regionen, können Sie ein von Amazon Inspector entwickeltes Shell-Skript verwenden. Weitere Informationen zur Verwendung dieses Skripts finden Sie unter inspector2-enablement-with-cli auf der Website. GitHub

Themen

Die Beziehung zwischen Administrator- und Mitgliedskonten in Amazon Inspector verstehen

Wenn Sie Amazon Inspector in einer Umgebung mit mehreren Konten verwenden, hat das delegierte Administratorkonto von Amazon Inspector Zugriff auf bestimmte Metadaten. Zu diesen Metadaten gehören Amazon EC2- und Amazon ECR-Konfigurationsdaten sowie Ergebnisse der Sicherheitsfeststellungen für Mitgliedskonten. Das Administratorkonto kann auch Regeln zur Unterdrückung von Suchbegriffen erstellen, die auf Mitgliedskonten angewendet werden. Weitere Informationen finden Sie unter Unterdrückung der Ergebnisse von Amazon Inspector mit Unterdrückungsregeln.

Delegierte Administratoraktionen

Wenn der delegierte Administrator Einstellungen auf sein Konto anwendet, werden diese Einstellungen im Allgemeinen auf alle anderen Konten in der Organisation angewendet. Der delegierte Administrator kann auch Informationen für sein eigenes Konto und jedes zugeordnete Mitglied anzeigen und abrufen. Ein delegiertes Administratorkonto von Amazon Inspector kann die folgenden Aktionen ausführen:

- Den Status von Amazon Inspector für zugehörige Konten anzeigen und verwalten, einschließlich der Aktivierung und Deaktivierung von Amazon Inspector.
- Aktivieren oder deaktivieren Sie die Scantypen für alle Mitgliedskonten in der Organisation.
- Zeigen Sie aggregierte Suchdaten für die gesamte Organisation und Suchdetails für alle Mitgliedskonten innerhalb der Organisation an.
- Erstellen und verwalten Sie Unterdrückungsregeln, die für Ergebnisse aller Konten in der Organisation gelten.
- Aktivieren Sie das erweiterte Scannen von Amazon ECR für alle Mitglieder der Organisation.
- Zeigen Sie die Ressourcenabdeckung für die gesamte Organisation an.
- Definieren Sie die Dauer für automatische erneute Scans von ECR-Container-Images für alle Mitgliedskonten in der Organisation. Die Einstellung für die Scandauer des delegierten Administrators hat Vorrang vor allen Einstellungen, die das Mitgliedskonto zuvor festgelegt hat. Alle Konten in der Organisation teilen sich die Dauer der automatisierten erneuten Scans von Amazon ECR für die delegierten Administratoren. Sie können für einzelne Konten keine unterschiedlichen Dauern für erneute Scans festlegen.
- Geben Sie fünf benutzerdefinierte Pfade für Amazon Inspector Deep Inspection für Amazon EC2 an, die für alle Konten in der Organisation verwendet werden. Dies gilt zusätzlich zu den fünf benutzerdefinierten Pfaden, die ein delegierter Administrator für sein individuelles Konto festlegen kann. Weitere Informationen zur Konfiguration benutzerdefinierter Pfade für Deep Inspection finden Sie unterBenutzerdefinierte Pfade für die Tiefeninspektion mit Amazon Inspector.
- Aktivieren und deaktivieren Sie Amazon Inspector Deep Inspection für Mitgliedskonten.
- Exportieren Sie SBOMs für alle Mitgliedskonten in der Organisation.
- Stellen Sie den Amazon EC2-Scanmodus für alle Mitgliedskonten in der Organisation ein. Weitere Informationen finden Sie unter Der Scanmodus wird verwaltet.
- Erstellen und verwalten Sie CIS-Scankonfigurationen für alle Konten in der Organisation, mit Ausnahme von Scankonfigurationen, die von Mitgliedskonten erstellt wurden.

> **Note**
>
> Wenn ein Mitgliedskonto die Organisation verlässt, kann der delegierte Administrator die von diesem Konto geplanten Scankonfigurationen nicht mehr sehen.

- Zeigen Sie die CIS-Scanergebnisse für alle Konten in der Organisation an.

Aktionen für Mitgliedskonten

Ein Mitgliedskonto kann Informationen zu seinem Konto in Amazon Inspector einsehen und abrufen, während die Einstellungen für sein Konto vom delegierten Administrator verwaltet werden. Mitgliedskonten innerhalb einer Organisation können die folgenden Aktionen in Amazon Inspector ausführen:

- Aktivieren Sie Amazon Inspector für ihr eigenes Konto.
- Sehen Sie sich die Ressourcenabdeckung für ihr eigenes Konto an.
- Details zu den Ergebnissen für ihr eigenes Konto anzeigen.
- Sehen Sie sich die Einstellung für die Dauer des automatischen erneuten Scans des ECR-Container-Images für ihr eigenes Konto an.
- Geben Sie fünf benutzerdefinierte Pfade für Amazon Inspector Deep Inspection for EC2 an, die für ihr individuelles Konto verwendet werden. Diese Pfade werden zusätzlich zu allen benutzerdefinierten Pfaden gescannt, die der delegierte Administrator für die Organisation angegeben hat. Weitere Informationen zur Konfiguration von Deep-Inspection-Pfaden finden Sie unterBenutzerdefinierte Pfade für die Tiefeninspektion mit Amazon Inspector.
- Sehen Sie sich die benutzerdefinierten Pfade an, die von Ihrem delegierten Administrator für Amazon Inspector Deep Inspection festgelegt wurden.
- Exportieren Sie SBOMs für alle Ressourcen, die mit ihrem Konto verknüpft sind.
- Sehen Sie sich den Scanmodus für ihr Konto an.
- Erstellen und verwalten Sie CIS-Scankonfigurationen für ihr Konto.
- Sehen Sie sich die Ergebnisse aller CIS-Scans nach Ressourcen in ihrem Konto an, einschließlich der vom delegierten Administrator geplanten Scans.

> **Note**
>
> Nach der Aktivierung kann Amazon Inspector nur durch ein delegiertes Administratorkonto deaktiviert werden.

Benennen eines delegierten Administrators für Amazon Inspector

Wichtige Überlegungen für delegierte Administratoren

Beachten Sie die folgenden Faktoren, die definieren, wie der delegierte Administrator in Amazon Inspector arbeitet:

Ein delegierter Administrator kann maximal 5.000 Mitglieder verwalten.

Jeder delegierte Administrator von Amazon Inspector hat ein Kontingent von 5.000 Mitgliedskonten. Ihre Organisation könnte jedoch mehr als 5.000 Konten umfassen. Wenn Sie mehr als 5.000 Mitgliedskonten haben, erhalten Sie eine Benachrichtigung über das Amazon CloudWatch Personal Health Dashboard und eine E-Mail an das delegierte Administratorkonto.

Ein delegierter Administrator ist Regional.

Im AWS Organizations Gegensatz dazu ist Amazon Inspector ein regionaler Dienst. Das bedeutet, dass Sie für jeden AWS-Region , in dem Sie Amazon Inspector verwenden möchten, einen delegierten Administrator benennen, Mitgliedskonten hinzufügen und Scantypen aktivieren müssen.

Eine Organisation kann nur einen delegierten Administrator haben.

Sie können für eine Organisation nur einen delegierten Administrator für Amazon Inspector haben. Wenn Sie in einer Region ein Konto als delegierten Administrator festgelegt haben, muss dieses Konto Ihr delegierter Administrator in allen anderen Regionen sein.

Durch das Ändern eines delegierten Administrators wird Amazon Inspector für Mitgliedskonten nicht deaktiviert.

Wenn Sie den delegierten Administrator entfernen, wird Amazon Inspector in diesen Konten nicht deaktiviert, und die Scaneinstellungen werden nicht beeinträchtigt.

In Ihrer AWS Organisation müssen alle Funktionen aktiviert sein.

Dies ist die Standardeinstellung für AWS Organizations. Falls sie nicht aktiviert ist, finden Sie weitere Informationen unter Alle Funktionen in Ihrer Organisation aktivieren.

Erforderliche Berechtigungen zum designieren eines delegierten Administrators

Sie benötigen die Erlaubnis, Amazon Inspector zu aktivieren und einen delegierten Amazon Inspector-Administrator zu benennen.

Fügen Sie am Ende einer IAM-Richtlinie die folgende Erklärung hinzu, um diese Berechtigungen zu gewähren.

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Benennen Sie einen delegierten Administrator für Ihre Organisation AWS

Das folgende Verfahren zeigt Ihnen, wie Sie einen delegierten Administrator für Ihre Organisation bestimmen. AWS Wenn diese Benennung abgeschlossen ist, wird Amazon Inspector sowohl für das Verwaltungskonto der Organizations als auch für das gewählte delegierte Administratorkonto aktiviert.

> **Note**
>
> Nur das Verwaltungskonto der Organizations kann einen delegierten Administrator benennen.

Wenn Sie Amazon Inspector zum ersten Mal aktivieren, wird die serviceverknüpfte Rolle (SLR) `AWSServiceRoleForAmazonInspector` für das Konto erstellt. Weitere Informationen darüber, wie Amazon Inspector serviceverknüpfte Rollen verwendet, finden Sie unterVerwenden von

serviceverknüpften Rollen für Amazon Inspector. Allgemeine Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen im IAM-Benutzerhandbuch.

So benennen Sie einen delegierten Administrator für Amazon Inspector

Console

Benennen Sie einen delegierten Administrator in der Konsole

1. Melden Sie sich AWS Management Console mit dem AWS Organizations Verwaltungskonto an.
2. Öffnen Sie die Amazon Inspector AWS-Region Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und geben Sie dann mit der Auswahl oben rechts die Region an, für die Sie einen Administrator benennen möchten.
3. Geben Sie im Bereich Delegierter Administrator die zwölfstellige Konto-ID desjenigen ein AWS-Konto , den Sie als delegierten Amazon Inspector-Administrator für Ihre Organisation festlegen möchten. Wählen Sie dann Administration delegieren.
4. (Empfohlen) Wiederholen Sie die vorherigen Schritte für jeden AWS-Region Schritt.

API

Benennen Sie einen delegierten Administrator, der die API verwendet

- Führen Sie den EnableDelegatedAdminAccountAPI-Vorgang mit den Anmeldeinformationen AWS-Konto des Verwaltungskontos der Organizations. Sie können dazu auch den verwenden AWS Command Line Interface , indem Sie den folgenden CLI-Befehl ausführen:`aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 11111111111`.

> **Note**
>
> Stellen Sie sicher, dass Sie die Konto-ID des Kontos angeben, das Sie zu einem von Amazon Inspector delegierten Administrator machen möchten.

Nachdem Sie den delegierten Administrator angegeben haben, dürfen Sie das AWS Organizations Verwaltungskonto nur verwenden, um das delegierte Administratorkonto zu ändern oder zu entfernen.

Die Aktivierung von Amazon Inspector scannt nach Mitgliedskonten

Als delegierter Administrator für Ihre Organisation können Sie Amazon EC2-Scanning, Amazon ECR-Scannen oder beides für jedes Mitglied aktivieren, das AWS Organizations mit dem Verwaltungskonto verknüpft ist. Wenn Sie Scans für ein Mitgliedskonto aktivieren, wird dieses Konto dem delegierten Administrator zugeordnet, Amazon Inspector wird automatisch aktiviert und Scans des ausgewählten Typs werden sofort gestartet. Informationen darüber, welche Ressourcen gescannt werden können und wie Scans konfiguriert werden, finden Sie unterAutomatisiertes Scannen von Ressourcen mit Amazon Inspector.

Amazon Inspector bietet mehrere Optionen für die Verwaltung und Aktivierung von Scans für Mitgliedskonten, einschließlich der Möglichkeit, dass Mitgliedskonten Amazon Inspector aktivieren können. Verwenden Sie eine der folgenden Optionen, um Scans für Ihre Mitgliedskonten zu starten.

Um das Scannen für alle Mitgliedskonten automatisch zu aktivieren

1. Melden Sie sich mit dem delegierten Administratorkonto an.
2. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home. Geben Sie dann mit AWS-Region der Auswahl oben rechts die Region an, in der Sie das Scannen für alle Mitgliedskonten aktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus. In der Kontentabelle werden alle Mitgliedskonten angezeigt, die dem AWS Organizations Verwaltungskonto zugeordnet sind.
4. Aktivieren Sie das Kontrollkästchen oben in der Tabelle, um alle Konten auf dieser Seite auszuwählen. Wählen Sie dann Aktivieren und wählen Sie im Menü Ihre bevorzugte Option für den Scantyp aus.

   > **Note**
   >
   > Es werden nur die Konten ausgewählt, die derzeit auf der Seite sichtbar sind. Wenn Sie mehrere Kontoseiten haben, müssen Sie diesen Vorgang auf jeder Seite wiederholen. Um die Anzahl der auf der Seite angezeigten Konten zu ändern, wählen Sie das Zahnradsymbol.

5. Aktivieren Sie die Einstellung Inspector automatisch für neue Mitgliedskonten aktivieren und wählen Sie dann die Scantypen aus, um alle neuen Mitglieder zu aktivieren, die zu Ihrer Organisation hinzugefügt werden.

6. (Empfohlen) Wiederholen Sie diese Schritte in jeder Region, in der Sie Mitgliedskonten scannen möchten.

Die Einstellung Inspector automatisch für neue Mitgliedskonten aktivieren aktiviert Amazon Inspector für alle future Mitglieder Ihrer Organisation. Auf diese Weise kann Ihr delegierter Amazon Inspector-Administrator alle neuen Mitglieder verwalten, die der Organisation hinzugefügt werden. Wenn die Anzahl der Mitgliedskonten das Kontingent von 5.000 erreicht, wird diese Einstellung automatisch deaktiviert. Wenn ein Konto entfernt wird und die Gesamtzahl der Mitglieder auf weniger als 5.000 sinkt, wird die Einstellung automatisch wieder aktiviert.

Um Mitgliedskonten selektiv zu aktivieren

1. Melden Sie sich mit dem delegierten Administratorkonto an.
2. Öffnen Sie die Amazon Inspector AWS-Region Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und geben Sie dann mit der Auswahl oben rechts die Region an, in der Sie das Scannen für bestimmte Mitgliedskonten aktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus.
   In der Kontentabelle werden alle Mitgliedskonten angezeigt, die dem AWS Organizations Verwaltungskonto zugeordnet sind.
4. Aktivieren Sie auf der Seite Kontoverwaltung das Kontrollkästchen für jedes Mitgliedskonto, für das Sie die Suche aktivieren möchten.
5. Wählen Sie Aktivieren aus.
6. Wählen Sie im Menü Aktivieren die Scantypen aus, die für die ausgewählten Konten aktiviert werden sollen. Sie können aus den folgenden Scanoptionen wählen:
   - Gesamtes Scannen — um alle Scanarten zu aktivieren.
   - EC2-Scannen — um Scans von Amazon EC2 EC2-Instances zu aktivieren.
   - ECR-Container-Scanning — um Scans von ECR-Container-Images zu aktivieren.
   - AWS Lambda Standard-Scanning — um Scans von Lambda-Funktionen zu aktivieren.
7. (Empfohlen) Wiederholen Sie diese Schritte in jeder Region, in der Sie Scans für bestimmte Mitglieder aktivieren möchten.

Wenn Ihr AWS Organizations Verwaltungskonto einen Administrator für Amazon Inspector delegiert hat, können Sie Ihr eigenes Konto als Mitglied aktivieren und die Scandetails für Ihr eigenes Konto einsehen.

Um das Scannen als Mitgliedskonto zu aktivieren

1. Loggen Sie sich in Ihr Konto ein.
2. Öffnen Sie die Amazon Inspector AWS-Region Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und geben Sie dann mit der Auswahl oben rechts die Region an, in der Sie das Scannen aktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus.
4. Aktivieren Sie auf der Seite Kontoverwaltung das Kontrollkästchen für Ihr Konto.
5. Wählen Sie im Menü Aktivieren die zu aktivierenden Scantypen aus. Sie können aus den folgenden Scanoptionen wählen:
   - Gesamtes Scannen — um alle Scanarten zu aktivieren.
   - EC2-Scannen — um Scans von Amazon EC2 EC2-Instances zu aktivieren.
   - ECR-Container-Scanning — um Scans von ECR-Container-Images zu aktivieren.
   - AWS Lambda Standard-Scanning — um Scans von Lambda-Funktionen zu aktivieren.
6. (Empfohlen) Wiederholen Sie diese Schritte in jeder Region, in der Sie Scans aktivieren möchten.

Verknüpfung von Mitgliedskonten in Amazon Inspector aufheben

Das folgende Verfahren zeigt, wie die Zuordnung von Mitgliedskonten aufgehoben wird. Getrennte Mitgliedskonten verbleiben in Ihrer AWS Organizations Organisation als eigenständige Amazon Inspector Inspector-Konten. Der delegierte Administrator von Amazon Inspector ist nicht mehr berechtigt, Amazon Inspector für diese Konten zu aktivieren und zu verwalten. Sie können getrennte Konten später wieder als Mitglieder hinzufügen.

> **Note**
>
> Durch das Trennen eines Kontos werden die Amazon Inspector-Scans für dieses Konto nicht deaktiviert.

Console

Um Mitgliedskonten mithilfe der Konsole zu trennen

1. Melden Sie sich mit dem delegierten Administratorkonto an.

2. Öffnen Sie die Amazon Inspector AWS-Region Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und geben Sie dann mit der Auswahl oben rechts die Region an, in der Sie die Zuordnung zu einem oder mehreren Mitgliedskonten aufheben möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus.
4. Aktivieren Sie auf der Seite Kontoverwaltung das Kontrollkästchen für jedes Konto, dessen Verknüpfung Sie aufheben möchten.
5. Wählen Sie im Menü Aktionen die Option Konto trennen aus.
6. (Empfohlen) Wiederholen Sie diese Schritte in jeder Region, in der Sie Konten trennen möchten.

API

So trennen Sie Mitgliedskonten mithilfe der API

Führen Sie den DisassociateMember API-Vorgang aus. Geben Sie in der Anfrage die Konto-IDs an, deren Zuordnung Sie aufheben möchten.

Entfernen eines delegierten Amazon Inspector-Administrators

Wenn Sie einen neuen delegierten Amazon Inspector-Administrator zuweisen müssen, können Sie einen vorhandenen delegierten Administrator als AWS Organizations Verwaltungskonto entfernen.

Wenn Sie einen delegierten Administrator entfernen, wird Amazon Inspector in diesem Konto oder in Mitgliedskonten einer Organisation nicht deaktiviert. Konten innerhalb Ihrer Organisation werden in eigenständige Konten umgewandelt und behalten die Scaneinstellungen bei, die sie hatten, bevor sie von einem delegierten Administrator verwaltet wurden.

Um den delegierten Administrator zu entfernen

1. Melden Sie sich AWS Management Console mit dem AWS Organizations Verwaltungskonto an.
2. Öffnen Sie die Amazon Inspector AWS-Region Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und geben Sie dann mit der Auswahl oben rechts die Region an, aus der Sie den delegierten Administrator entfernen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus.
4. Wählen Sie im Bereich Delegierter Administrator die Option Entfernen aus, und bestätigen Sie dann Ihre Aktion.

5. Wiederholen Sie diese Schritte in jeder Region, in der Sie diesen delegierten Administrator registriert haben.

Wenn Sie einen neuen delegierten Amazon Inspector-Administrator hinzufügen, müssen Sie dem neuen Administratorkonto manuell Organisationsmitglieder zuordnen. Gehen Sie wie folgt vor, um Organisationsmitglieder dem neuen Administratorkonto zuzuordnen.

So ordnen Sie Mitglieder einem neuen delegierten Administrator zu

1. Melden Sie sich AWS Management Console mit dem delegierten Administratorkonto an.
2. Öffnen Sie die Amazon Inspector AWS-Region Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und geben Sie dann mit der Auswahl oben rechts die Region an, in der Sie Mitglieder mit dem neuen delegierten Administrator verknüpfen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus.
4. Wählen Sie alle aufgelisteten Konten in Ihrer Organisation aus, indem Sie das obere Kontrollkästchen verwenden.
5. Wählen Sie im Menü Aktionen die Option Mitglied hinzufügen aus.
6. Wiederholen Sie diese Schritte in jeder Region, in der Sie Mitglieder dem neuen delegierten Administrator zuordnen möchten.

Überwachung von Nutzung und Kosten in Amazon Inspector

Sie können die Amazon Inspector-Konsole und die API-Operationen verwenden, um die monatlichen Kosten für die Nutzung von Amazon Inspector in Ihrer Umgebung zu prognostizieren. Wenn Sie der Amazon Inspector-Administrator für eine Umgebung mit mehreren Konten sind, können Sie die Gesamtkosten für Ihre gesamte Umgebung und die Kostenkennzahlen für jedes Ihrer Mitgliedskonten einsehen.

Verwenden Sie die Nutzungskonsole

Sie können die Nutzung und die voraussichtlichen Kosten für Amazon Inspector von der Konsole aus beurteilen.

Um auf Nutzungsstatistiken zuzugreifen

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Kosten überwachen möchten.
3. Wählen Sie im Navigationsbereich Benutzer.

Auf der Registerkarte „Nach Konto“ finden Sie die voraussichtlichen Gesamtkosten auf der Grundlage des Zeitraums von 30 Tagen, der unter Kontonutzung aufgeführt ist. Wählen Sie in der Tabelle unter der Spalte Voraussichtliche Kosten einen Wert aus, um eine Aufschlüsselung der Nutzung nach Scantyp für dieses Konto anzuzeigen. In diesem Detailbereich können Sie auch sehen, für welche Scantypen eine kostenlose Testversion für dieses Konto aktiv ist.

Wenn Sie der delegierte Administrator für eine Organisation sind, wird in der Tabelle für jedes Konto in Ihrer Organisation eine Zeile angezeigt. Wenn die Zuordnung zu einem Konto in Ihrer Organisation aufgehoben wird, zeigt die Konsole die voraussichtlichen Kosten als - an.

Auf der Registerkarte Nach Scan-Typ finden Sie eine Aufschlüsselung der tatsächlichen Nutzung im aktuellen Zeitraum von 30 Tagen nach Scantyp. Diese Informationen werden zur Berechnung der voraussichtlichen Kosten auf der Registerkarte „Nach Konto“ verwendet.

Wenn Sie der delegierte Administrator einer Organisation sind, können Sie die Nutzung für jedes Konto in Ihrer Organisation einsehen.

Auf dieser Registerkarte können Sie jeden der folgenden Bereiche für Nutzungsstatistiken erweitern:

Amazon EC2-Scannen

Die Amazon Inspector Inspector-Nutzungskonsole verfolgt die folgenden Metriken für agentenbasiertes Scannen und agentenloses Scannen:

- Instances (Durchschnitt) — Amazon Inspector berechnet anhand der Servicezeiten die durchschnittliche Anzahl von Ressourcen für das Scannen von EC2-Instances. Der Durchschnitt ergibt sich aus der Gesamtzahl der abgedeckten Stunden geteilt durch 720 Stunden (die Anzahl der Stunden in einem Zeitraum von 30 Tagen).
- Servicezeiten — für Amazon EC2-Scans ist dies die Gesamtzahl der Stunden innerhalb der letzten 30 Tage, in denen Amazon Amazon Inspector für jede EC2-Instance in einem Konto eine aktive Abdeckung bereitgestellt hat. Bei EC2-Instances sind die Stunden zwischen dem Zeitpunkt, an dem Amazon Inspector die Instance entdeckt hat, bis sie beendet oder gestoppt oder anhand von Tags von Scans ausgeschlossen wird. (Wenn Sie eine gestoppte Instance neu starten oder ein Ausschluss-Tag entfernen, nimmt Amazon Inspector den Versicherungsschutz wieder auf und es fallen weiterhin Versicherungsstunden für diese Instance an).

CIS-Instance-Scans — Die Gesamtzahl der CIS-Scans, die für Instances im Konto durchgeführt wurden.

Amazon ECR-Scannen

Erste Scans — Die Summe der ersten Scans von Bildern im Konto innerhalb der letzten 30 Tage.

Rescans — Die Summe der Rescans von Bildern im Konto innerhalb der letzten 30 Tage. Ein erneuter Scan ist jeder Scan, der an einem ECR-Bild durchgeführt wird, das Amazon Inspector zuvor gescannt hat. Wenn Sie Ihr ECR-Repository für kontinuierliches Scannen konfiguriert haben, werden erneute Scans automatisch durchgeführt, wenn Amazon Inspector seiner Datenbank neue Common Vulnerabilities and Exposures (CVE) hinzufügt.

Lambda-Scannen

Die Amazon Inspector Inspector-Nutzungskonsole verfolgt die folgenden Metriken für Lambda-Standardscans und Lambda-Code-Scans:

- Anzahl der Lambda-Funktionen (Durchschnitt) — Amazon Inspector berechnet anhand der Empfangsstunden die durchschnittliche Anzahl von Funktionen für das Scannen von Lambda-Funktionen. Der Durchschnitt ist die Gesamtzahl der abgedeckten Stunden geteilt durch 720 Stunden (die Anzahl der Stunden in einem Zeitraum von 30 Tagen).

- Servicezeiten — Für Lambda-Funktionsscans ist dies die Gesamtzahl der Stunden innerhalb der letzten 30 Tage, in denen Amazon Amazon Inspector für jede Lambda-Funktion in einem Konto eine aktive Abdeckung bereitgestellt hat. Für AWS Lambda Funktionen werden die Empfangszeiten von dem Zeitpunkt, an dem Amazon Inspector eine Funktion entdeckt, bis zu dem Zeitpunkt berechnet, zu dem sie gelöscht oder von Scans ausgeschlossen wird. Wenn eine ausgeschlossene Funktion erneut aufgenommen wird, fallen die für diese Funktion verfügbaren Stunden weiterhin an.

Verstehen, wie Amazon Inspector die Nutzungskosten berechnet

Bei den von Amazon Inspector angegebenen Kosten handelt es sich um Schätzungen, nicht um tatsächliche Kosten. Sie können daher von denen auf Ihrer AWS Billing Konsole abweichen.

Beachten Sie auf der Seite „Nutzung“ Folgendes zur Berechnung der Kosten durch Amazon Inspector:

- Die Nutzungskosten beziehen sich nur auf die aktuelle Region. Die Preise pro Scantyp variieren je nach AWS Region. Die genauen Preise pro Region finden Sie unter Preise für Amazon Inspector
- Alle Nutzungsprognosen werden auf den nächsten US-Dollar gerundet.
- Rabatte sind nicht in den voraussichtlichen Kosten enthalten.
- Die voraussichtlichen Kosten stellen die Gesamtkosten für den 30-tägigen Nutzungszeitraum pro Scantyp dar. Wenn ein Konto weniger als 30 Tage genutzt wurde, berechnet Amazon Inspector die Kosten nach 30 Tagen so, als ob alle derzeit abgedeckten Ressourcen für den Rest des 30-tägigen Zeitraums abgedeckt bleiben würden.
- Die Kosten pro Scan-Typ werden auf der Grundlage der folgenden Faktoren berechnet:
  - EC2-Scannen: Die Kosten spiegeln die durchschnittliche Anzahl der EC2-Instances wider, die Amazon Inspector in den letzten 30 Tagen abgedeckt hat.
  - Scannen von ECR-Containern: Die Kosten entsprechen der Summe der ersten Bildscans und der erneuten Bildscans in den letzten 30 Tagen.
  - Lambda-Standardscan: Die Kosten spiegeln die durchschnittliche Anzahl der Lambda-Funktionen wider, die Amazon Inspector in den letzten 30 Tagen abgedeckt hat.
  - Lambda-Code-Scanning: Die Kosten spiegeln die durchschnittliche Anzahl der Lambda-Funktionen wider, die Amazon Inspector in den letzten 30 Tagen abgedeckt hat.

Über die kostenlose Testversion von Amazon Inspector

Wenn Sie einen Amazon Inspector-Scantyp aktivieren, werden Sie automatisch für eine 15-tägige kostenlose Testversion für diesen Scantyp angemeldet. Jeder Scantyp hat eine unabhängige freie Spur. Dazu gehören: EC2-Scannen, ECR-Scannen, Lambda-Standardscannen und Lambda-Code-Scannen.

> **Note**
>
> Die kostenlose Testversion gilt nicht für das CIS-Scannen.

Wenn Sie während der kostenlosen Testversion einen Scan-Typ deaktivieren, wird die kostenlose Testversion für diesen Scantyp angehalten. Wenn Sie diesen Service reaktivieren, wird die kostenlose Testversion wieder aufgenommen und Sie erhalten die verbleibenden Tage der kostenlosen Testversion.

Sicherheit in Amazon Inspector

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon Inspector gelten, finden Sie unter AWS Services im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon Inspector anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon Inspector konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie Ihre Amazon Inspector Inspector-Ressourcen überwachen und sichern können.

Themen

Datenschutz in Amazon Inspector

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in Amazon Inspector. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon Inspector oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Themen

Verschlüsselung im Ruhezustand

Amazon Inspector speichert Ihre Daten im Ruhezustand sicher und verwendet standardmäßig AWS Verschlüsselungslösungen. Amazon Inspector verschlüsselt Daten, wie z. B. mit AWS Systems Manager erfasstes Ressourceninventar, anhand von Amazon ECR-Images analysiertes Ressourceninventar und generierte Sicherheitsergebnisse, mithilfe AWS eigener Verschlüsselungsschlüssel von AWS Key Management Service ().AWS KMS Sie können AWS eigene Schlüssel nicht einsehen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme ändern, um die Schlüssel zu schützen, mit denen Ihre Daten verschlüsselt werden. Weitere Informationen finden Sie unter AWS Eigene Schlüssel.

Wenn Sie Amazon Inspector deaktivieren, werden alle Ressourcen, die Amazon Inspector für Sie speichert oder verwaltet, dauerhaft gelöscht, z. B. gesammeltes Inventar und Sicherheitserkenntnisse.

Verschlüsselung im Ruhezustand für den Code in Ihren Ergebnissen

Beim Scannen von Amazon Inspector Lambda-Code arbeitet Amazon Inspector mit Amazon Inspector zusammen, CodeGuru um Ihren Code auf Sicherheitslücken zu scannen. Wenn eine Sicherheitslücke erkannt wird, wird ein Codeausschnitt, der die Sicherheitslücke enthält, CodeGuru extrahiert und gespeichert, bis Amazon Inspector Zugriff anfordert. Standardmäßig wird ein AWS eigener Schlüssel CodeGuru verwendet, um den extrahierten Code zu verschlüsseln. Sie können Amazon Inspector jedoch so konfigurieren, dass Ihr eigener, vom Kunden verwalteter AWS KMS Schlüssel für die Verschlüsselung verwendet wird.

Der folgende Arbeitsablauf erklärt, wie Amazon Inspector den von Ihnen konfigurierten Schlüssel verwendet, um Ihren Code zu verschlüsseln:

1. Sie stellen Amazon Inspector mithilfe der Amazon Inspector UpdateEncryptionKeyInspector-API einen AWS KMS Schlüssel zur Verfügung.
2. Amazon Inspector leitet die Informationen zu Ihrem AWS KMS Schlüssel weiter an CodeGuru. CodeGuru speichert die Informationen für die future Verwendung.

3. CodeGuru fordert ein Zuschussformular AWS KMS für den Schlüssel an, den Sie in Amazon Inspector konfiguriert haben.
4. CodeGuru erstellt aus Ihrem Schlüssel einen verschlüsselten AWS KMS Datenschlüssel und speichert ihn. Dieser Datenschlüssel wird verwendet, um Ihre von CodeGuru gespeicherten Codedaten zu verschlüsseln.
5. Immer wenn Amazon Inspector Daten aus Codescans anfordert, CodeGuru verwendet Amazon Inspector den Grant, um den verschlüsselten Datenschlüssel zu entschlüsseln, und verwendet diesen Schlüssel dann, um die Daten zu entschlüsseln, sodass sie abgerufen werden können.

Wenn Sie das Lambda-Code-Scannen deaktivieren, wird CodeGuru der Grant zurückgezogen und der zugehörige Datenschlüssel gelöscht.

Berechtigungen für die Codeverschlüsselung mit einem vom Kunden verwalteten Schlüssel

Um Verschlüsselung verwenden zu können, benötigen Sie eine Richtlinie, die den Zugriff auf AWS KMS Aktionen ermöglicht, sowie eine Erklärung, die Amazon Inspector die CodeGuru Erlaubnis erteilt, diese Aktionen über Bedingungsschlüssel zu verwenden.

Wenn Sie den Verschlüsselungsschlüssel für Ihr Konto einrichten, aktualisieren oder zurücksetzen, müssen Sie eine Amazon Inspector-Administratorrichtlinie verwenden, wie z. AWS verwaltete Richtlinie: AmazonInspector2FullAccess Außerdem müssen Sie Benutzern mit Lesezugriff, die Codefragmente aus Ergebnissen oder Daten über den für die Verschlüsselung ausgewählten Schlüssel abrufen müssen, die folgenden Berechtigungen gewähren.

Für KMS muss die Richtlinie es Ihnen ermöglichen, die folgenden Aktionen auszuführen:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

Sobald Sie überprüft haben, dass Sie in Ihrer Richtlinie über die richtigen AWS KMS Berechtigungen verfügen, müssen Sie eine Erklärung beifügen, die Amazon Inspector und CodeGuru die

Verwendung Ihres Schlüssels für die Verschlüsselung gestattet. Fügen Sie die folgende Grundsatzerklärung bei:

> **Note**
>
> Ersetzen Sie Region durch die AWS Region, in der Sie das Amazon Inspector Lambda-Code-Scannen aktiviert haben.

```
{
            "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
         "Effect": "Allow",
         "Action": "kms:CreateGrant",
         "Resource": "*",
         "Condition": {
          "ForAllValues:StringEquals": {
           "kms:GrantOperations": [
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "Encrypt",
            "Decrypt",
            "RetireGrant",
            "DescribeKey"
           ]
          },
          "StringEquals": {
           "kms:ViaService": [
            "codeguru-security.Region.amazonaws.com"
           ]
          }
         }
        },
        {
         "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
         "Effect": "Allow",
         "Action": [
          "kms:Encrypt",
          "kms:Decrypt",
          "kms:RetireGrant",
          "kms:DescribeKey",
          "kms:GenerateDataKeyWithoutPlaintext"
```

```
        ],
        "Resource": "*",
        "Condition": {
         "StringEquals": {
          "kms:ViaService": [
           "inspector2.Region.amazonaws.com",
           "codeguru-security.Region.amazonaws.com"
          ]
         }
        }
       }
```

> **Note**
>
> Wenn Sie die Anweisung hinzufügen, stellen Sie sicher, dass die Syntax gültig ist. Richtlinien verwenden das JSON-Format. Das bedeutet, dass Sie vor oder nach der Anweisung ein Komma hinzufügen müssen, je nachdem, wo Sie die Anweisung zur Richtlinie hinzufügen. Wenn Sie die Anweisung als letzte Anweisung hinzufügen, fügen Sie hinter der schließenden Klammer für die vorherige Anweisung ein Komma hinzu. Wenn Sie sie als erste Anweisung oder zwischen zwei vorhandenen Anweisungen hinzufügen, fügen Sie hinter der schließenden Klammer für die Anweisung ein Komma ein.

Konfiguration der Verschlüsselung mit einem vom Kunden verwalteten Schlüssel

Um die Verschlüsselung für Ihr Konto mit einem vom Kunden verwalteten Schlüssel zu konfigurieren, müssen Sie ein Amazon Inspector-Administrator mit den unter beschriebenen Berechtigungen seinBerechtigungen für die Codeverschlüsselung mit einem vom Kunden verwalteten Schlüssel. Darüber hinaus benötigen Sie einen AWS KMS Schlüssel in derselben AWS Region wie Ihre Ergebnisse oder einen Schlüssel für mehrere Regionen. Sie können einen vorhandenen symmetrischen Schlüssel in Ihrem Konto verwenden oder mithilfe der AWS Managementkonsole oder der APIs einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen. AWS KMS Weitere Informationen finden Sie im Benutzerhandbuch unter Erstellen symmetrischer AWS KMSAWS KMS Verschlüsselungsschlüssel.

Verwenden der Amazon Inspector API zur Konfiguration der Verschlüsselung

Um einen Schlüssel für die Verschlüsselung für den UpdateEncryptionKeyBetrieb der Amazon Inspector-API festzulegen, während Sie als Amazon Inspector-Administrator angemeldet sind.

Verwenden Sie in der API-Anfrage das `kmsKeyId` Feld, um den ARN des AWS KMS Schlüssels anzugeben, den Sie verwenden möchten. Für `scanType` Enter `CODE` und für `resourceType` Enter`AWS_LAMBDA_FUNCTION`.

Sie können die UpdateEncryptionKeyAPI verwenden, um zu überprüfen, welchen AWS KMS Schlüssel Amazon Inspector für die Verschlüsselung verwendet.

> **Note**
>
> Wenn Sie versuchen zu verwenden, `GetEncryptionKey` obwohl Sie keinen vom Kunden verwalteten Schlüssel eingerichtet haben, gibt der Vorgang einen `ResourceNotFoundException` Fehler zurück, was bedeutet, dass ein AWS eigener Schlüssel für die Verschlüsselung verwendet wird.

Wenn Sie den Schlüssel löschen oder seine Richtlinie ändern, sodass der Zugriff auf Amazon Inspector verweigert wird, können CodeGuru Sie andernfalls nicht auf Ihre gefundenen Sicherheitslücken zugreifen und der Lambda-Code-Scan schlägt für Ihr Konto fehl.

Sie können `ResetEncryptionKey` damit fortfahren, einen AWS eigenen Schlüssel zur Verschlüsselung von Code zu verwenden, der im Rahmen Ihrer Amazon Inspector Inspector-Ergebnisse extrahiert wurde.

Verschlüsselung während der Übertragung

AWS verschlüsselt alle Daten, die zwischen AWS internen Systemen und anderen AWS Diensten übertragen werden.

Für die Inventarerfassung sammelt Systems Manager Telemetriedaten von kundeneigenen EC2-Instances, die zur Bewertung AWS über einen durch Transport Layer Security (TLS) geschützten Kanal zurückgesendet werden. Unter Datenschutz in Systems Manager erfahren Sie, wie SSM Daten bei der Übertragung verschlüsselt.

Ebenso werden die Ergebnisse der Amazon ECR- und AWS Lambda-Funktionsscans, die an Security Hub gesendet werden, über einen TLS-geschützten Kanal verschlüsselt.

Identity and Access Management für Amazon Inspector

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon Inspector Inspector-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Amazon Inspector ausführen.

Servicebenutzer — Wenn Sie den Amazon Inspector-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Funktionen von Amazon Inspector verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Amazon Inspector nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Identität und Zugriff auf Amazon Inspector.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon Inspector-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon Inspector. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon Inspector Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Amazon Inspector verwenden kann, finden Sie unterSo arbeitet Amazon Inspector mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon Inspector zu verwalten. Beispiele für identitätsbasierte Amazon Inspector Inspector-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center -Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-

Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer

gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den

Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-

Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So arbeitet Amazon Inspector mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon Inspector zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Amazon Inspector verwendet werden können.

IAM-Funktionen, die Sie mit Amazon Inspector verwenden können

IAM-Feature	Unterstützung für Amazon Inspector
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Amazon Inspector und andere AWS-Services mit den meisten IAM-Funktionen funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für Amazon Inspector

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen

ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

Ressourcenbasierte Richtlinien in Amazon Inspector

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben

Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Politische Maßnahmen für Amazon Inspector

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Amazon Inspector-Aktionen finden Sie unter Von Amazon Inspector definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in Amazon Inspector verwenden das folgende Präfix vor der Aktion:

```
inspector2
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "inspector2:action1",
      "inspector2:action2"
         ]
```

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

Richtlinienressourcen für Amazon Inspector

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der Amazon Inspector-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon Inspector definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon Inspector definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

Schlüssel für Richtlinienbedingungen für Amazon Inspector

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Amazon Inspector-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon Inspector in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Inspector definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

ACLs in Amazon Inspector

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Amazon Inspector

Unterstützt ABAC (Tags in Richtlinien)	Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit Amazon Inspector verwenden

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn

Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Hauptberechtigungen für Amazon Inspector

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Amazon Inspector

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Amazon Inspector beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon Inspector Sie dazu anleitet.

Servicebezogene Rollen für Amazon Inspector

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS-Services Diese Rollen funktionieren mit IAM. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon Inspector Inspector-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon Inspector definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Inspector in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon Inspector Inspector-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation

B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Amazon Inspector Inspector-Konsole

Um auf die Amazon Inspector Inspector-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon Inspector Inspector-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Amazon Inspector-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch den Amazon Inspector `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder 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": "*"
        }
    ]
}
```

Nur-Lese-Zugriff auf alle Amazon Inspector Inspector-Ressourcen zulassen

Dieses Beispiel zeigt eine Richtlinie, die nur Lesezugriff auf alle Amazon Inspector Inspector-Ressourcen ermöglicht.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector2:Describe*",
                "inspector2:Get*",
                "inspector2:BatchGet*",
                "inspector2:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Vollzugriff auf alle Amazon Inspector Inspector-Ressourcen zulassen

Dieses Beispiel zeigt eine Richtlinie, die vollen Zugriff auf alle Amazon Inspector Inspector-Ressourcen ermöglicht.

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

```
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinien für Amazon Inspector

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar

sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AmazonInspector2FullAccess

Sie können die `AmazonInspector2FullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Zugriff auf Amazon Inspector ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `inspector2`— Ermöglicht vollen Zugriff auf die Funktionen von Amazon Inspector.
- `iam`— Ermöglicht Amazon Inspector, die serviceverknüpfte Rolle zu erstellen,`AmazonInspector2AgentlessServiceRole`. Dies ist erforderlich, damit Amazon Inspector beispielsweise Informationen über Ihre Amazon EC2-Instances und Amazon ECR-Repositorys und Container-Images abrufen, Ihr VPC-Netzwerk analysieren und Konten beschreiben kann, die mit Ihrer Organisation verknüpft sind. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Inspector.
- `organizations`— Ermöglicht Administratoren die Verwendung von Amazon Inspector für eine Organisation in AWS Organizations. Nach der Aktivierung des vertrauenswürdigen Zugriffs für

Amazon Inspector in AWS Organizations können Mitglieder des delegierten Administratorkontos Einstellungen verwalten und Ergebnisse in ihrer gesamten Organisation einsehen.

- `codeguru-security`— Ermöglicht Administratoren, Amazon Inspector zu verwenden, um Informationscodefragmente abzurufen und die Verschlüsselungseinstellungen für den von CodeGuru Security gespeicherten Code zu ändern. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand für den Code in Ihren Ergebnissen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:UpdateAccountConfiguration"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "inspector2.amazonaws.com"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
```

```
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS verwaltete Richtlinie: AmazonInspector2ReadOnlyAccess

Sie können die `AmazonInspector2ReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Berechtigungen, die nur Lesezugriff auf Amazon Inspector ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `inspector2`— Ermöglicht den schreibgeschützten Zugriff auf die Funktionen von Amazon Inspector.
- `organizations`— Ermöglicht die Anzeige von Details zum Versicherungsschutz durch Amazon Inspector für ein Unternehmen. AWS Organizations
- `codeguru-security`— Ermöglicht das Abrufen von Codefragmenten aus CodeGuru der Sicherheitsabteilung. Ermöglicht auch das Einsehen der Verschlüsselungseinstellungen für Ihren in CodeGuru Security gespeicherten Code.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
```

```
    "inspector2:BatchGet*",
    "inspector2:List*",
    "inspector2:Describe*",
    "inspector2:Get*",
    "inspector2:Search*",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS verwaltete Richtlinie: AmazonInspector2ManagedCisPolicy

Sie können die `AmazonInspector2ManagedCisPolicy`-Richtlinie auch Ihren IAM-Entitäten anfügen. Diese Richtlinie sollte einer Rolle zugeordnet werden, die Ihren Amazon EC2 EC2-Instances die Erlaubnis erteilt, CIS-Scans der Instance auszuführen. Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie all ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `inspector2`— Ermöglicht den Zugriff auf Aktionen, die zur Ausführung von CIS-Scans verwendet werden.

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

```
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
            ],
            "Resource": "*",
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonInspector2ServiceRolePolicy

Sie können die `AmazonInspector2ServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Amazon Inspector ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Inspector.

AWS verwaltete Richtlinie: AmazonInspector2AgentlessServiceRolePolicy

Sie können die `AmazonInspector2AgentlessServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es Amazon Inspector ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Inspector.

Amazon Inspector aktualisiert AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon Inspector an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Amazon Inspector Document History-Seite.

Änderung	Beschreibung	Datum
AmazonInspector2 ManagedCisPolicy — Neue Richtlinie	Amazon Inspector hat eine neue verwaltete Richtlini e hinzugefügt, die Sie als Teil eines Instance-Profils	23. Januar 2024

Änderung	Beschreibung	Datum
	verwenden können, um CIS-Scans auf einer Instance zuzulassen.	
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, CIS-Scans auf Ziel-Instances zu starten.	23. Januar 2024
AmazonInspector2 AgentlessServiceRolePolicy — Neue Richtlinie	Amazon Inspector hat eine neue servicebezogene Rollenrichtlinie hinzugefügt, um das agentenlose Scannen von EC2-Instances zu ermöglichen.	8. November 2023
AmazonInspector2 ReadOnlyAccess — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Benutzern mit Lesezugriff ermöglichen, Informationen zu Sicherheitslücken für gefundene Sicherheitslücken in Paketen abzurufen.	22. September 2023
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, Netzwerkkonfigurationen von Amazon EC2 EC2-Instances zu scannen, die Teil der Elastic Load Balancing Balancing-Zielgruppen sind.	31. August 2023

Änderung	Beschreibung	Datum
AmazonInspector2 ReadOnlyAccess — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Benutzern mit Lesezugriff ermöglichen, Software Bill of Materials (SBOM) für ihre Ressourcen zu exportieren.	29. Juni 2023
AmazonInspector2 ReadOnlyAccess — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Benutzern mit Lesezugriff ermöglichen, Details der Verschlüsselungseinstellungen für Lambda-Code-Scanergebnisse für ihr Konto abzurufen.	13. Juni 2023
AmazonInspector2 FullAccess — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, mit denen Benutzer einen vom Kunden verwalteten KMS-Schlüssel konfigurieren können, um Code in Ergebnissen aus Lambda-Code-Scans zu verschlüsseln.	13. Juni 2023
AmazonInspector2 ReadOnlyAccess — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Benutzern mit Lesezugriff ermöglichen, Details zum Status und zu den Ergebnissen des Lambda-Code-Scans für ihr Konto abzurufen.	02. Mai 2023

Änderung	Beschreibung	Datum
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, AWS CloudTrail serviceverknüpfte Kanäle in Ihrem Konto zu erstellen, wenn Sie Lambda-Scanning aktivieren. Dadurch kann Amazon Inspector CloudTrail Ereignisse in Ihrem Konto überwachen.	30. April 2023
AmazonInspector2 FullAccess — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Benutzern ermöglichen, Details zu den beim Lambda-Code-Scannen gefundenen Sicherheitslücken abzurufen.	21. April 2023
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, Informationen über die benutzerdefinierten Pfade, die ein Kunde für Amazon EC2 Deep Inspection definiert hat, an Amazon EC2 Systems Manager zu senden.	17. April 2023

Änderung	Beschreibung	Datum
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, AWS CloudTrail serviceverknüpfte Kanäle in Ihrem Konto zu erstellen, wenn Sie Lambda-Scanning aktivieren. Dadurch kann Amazon Inspector CloudTrail Ereignisse in Ihrem Konto überwachen.	30. April 2023
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, Scans des Entwicklercodes in AWS Lambda Funktionen anzufordern und Scandaten von Amazon CodeGuru Security zu empfangen. Darüber hinaus hat Amazon Inspector Berechtigungen zur Überprüfung von IAM-Richtlinien hinzugefügt. Amazon Inspector verwendet diese Informationen, um Lambda-Funktionen auf Code-Schwachstellen zu überprüfen.	28. Februar 2023

Änderung	Beschreibung	Datum
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat eine neue Anweisung hinzugefügt, die es Amazon Inspector ermöglicht, Informationen CloudWatch darüber abzurufen, wann eine AWS Lambda Funktion zuletzt aufgerufen wurde. Amazon Inspector verwendet diese Informationen, um Scans auf die Lambda-Funktionen in Ihrer Umgebung zu konzentrieren, die in den letzten 90 Tagen aktiv waren.	20. Februar 2023
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat eine neue Anweisung hinzugefügt, die es Amazon Inspector ermöglicht, Informationen über AWS Lambda Funktionen abzurufen, einschließlich jeder Layer-Version, die jeder Funktion zugeordnet ist. Amazon Inspector verwendet diese Informationen, um Lambda-Funktionen auf Sicherheitslücken zu überprüfen.	28. November 2022

Änderung	Beschreibung	Datum
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat eine neue Aktion hinzugefügt, mit der Amazon Inspector die Ausführung von SSM-Verknüpfungen beschreiben kann. Darüber hinaus hat Amazon Inspector zusätzlichen Ressourcenbereich hinzugefügt, damit Amazon Inspector SSM-Verknüpfungen mit `AmazonInspector2` eigenen SSM-Dokumenten erstellen, aktualisieren, löschen und starten kann.	31. August 2022
AmazonInspector2 ServiceRolePolicy Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat den Ressourcenbereich der Richtlinie aktualisiert, sodass Amazon Inspector Softwareinventar in anderen AWS Partitionen erfassen kann.	12. August 2022
AmazonInspector2 ServiceRolePolicy — Aktualisierungen einer bestehenden Richtlinie	Amazon Inspector hat den Ressourcenbereich der Aktionen neu strukturiert, sodass Amazon Inspector SSM-Verknüpfungen erstellen, löschen und aktualisieren kann.	10. August 2022
AmazonInspector2 — Neue Richtlinie ReadOnlyAccess	Amazon Inspector hat eine neue Richtlinie hinzugefügt, die den schreibgeschützten Zugriff auf die Funktionen von Amazon Inspector ermöglicht.	21. Januar 2022

Änderung	Beschreibung	Datum
AmazonInspector2 FullAccess — Neue Richtlinie	Amazon Inspector hat eine neue Richtlinie hinzugefügt, um vollen Zugriff auf die Funktionen von Amazon Inspector zu ermöglichen.	29. November 2021
AmazonInspector2 ServiceRolePolicy — Neue Richtlinie	Amazon Inspector hat eine neue Richtlinie hinzugefügt, die es Amazon Inspector ermöglicht, in Ihrem Namen Aktionen in anderen Diensten durchzuführen.	29. November 2021
Amazon Inspector hat begonnen, Änderungen nachzuverfolgen	Amazon Inspector hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	29. November 2021

Verwenden von serviceverknüpften Rollen für Amazon Inspector

Amazon Inspector verwendet eine AWS Identity and Access Management (IAM) -Serviceverknüpfte Rolle mit dem Namen. `AWSServiceRoleForAmazonInspector2` Bei dieser serviceverknüpften Rolle handelt es sich um eine IAM-Rolle, die direkt mit Amazon Inspector verknüpft ist. Es ist von Amazon Inspector vordefiniert und beinhaltet alle Berechtigungen, die Amazon Inspector benötigt, um andere in AWS-Services Ihrem Namen anzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon Inspector, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon Inspector definiert die Berechtigungen seiner serviceverknüpften Rolle. Sofern nicht anders definiert, kann nur Amazon Inspector die Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. eine Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden

Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch. Sie können eine dienstverknüpfte Rolle erst löschen, nachdem Sie die zugehörigen Ressourcen gelöscht haben. Dadurch werden Ihre Amazon Inspector Inspector-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie Ja mit einem Link, um die mit dem Service verknüpfte Rollendokumentation für diesen Service zu lesen.

Servicebezogene Rollenberechtigungen für Amazon Inspector

Amazon Inspector verwendet die mit dem Service verknüpfte Rolle namens`AWSServiceRoleForAmazonInspector2`. Diese dienstbezogene Rolle vertraut darauf, dass der `inspector2.amazonaws.com` Service die Rolle übernimmt.

Die Berechtigungsrichtlinie für die Rolle, die benannt ist`AmazonInspector2ServiceRolePolicy`, ermöglicht es Amazon Inspector, Aufgaben wie die folgenden auszuführen:

- Verwenden Sie Amazon Elastic Compute Cloud (Amazon EC2) -Aktionen, um Informationen über Ihre Instances und Netzwerkpfade abzurufen.
- Verwenden Sie AWS Systems Manager Aktionen, um Inventar von Ihren Amazon EC2 EC2-Instances abzurufen und Informationen über Pakete von Drittanbietern aus benutzerdefinierten Pfaden abzurufen.
- Verwenden Sie die AWS Systems Manager `SendCommand` Aktion, um CIS-Scans für Ziel-Instances aufzurufen.
- Verwenden Sie Amazon Elastic Container Registry-Aktionen, um Informationen über Ihre Container-Images abzurufen.
- Verwenden Sie AWS Lambda Aktionen, um Informationen über Ihre Lambda-Funktionen abzurufen.
- Verwenden Sie AWS Organizations Aktionen, um zugehörige Konten zu beschreiben.
- Verwenden Sie CloudWatch Aktionen, um Informationen darüber abzurufen, wann Ihre Lambda-Funktionen zuletzt aufgerufen wurden.
- Verwenden Sie ausgewählte IAM-Aktionen, um Informationen über Ihre IAM-Richtlinien abzurufen, die zu Sicherheitslücken in Ihrem Lambda-Code führen könnten.

- Verwenden Sie CodeGuru Sicherheitsaktionen, um den Code in Ihren Lambda-Funktionen zu scannen. Amazon Inspector verwendet die folgenden CodeGuru Sicherheitsaktionen:
  - codeguru-security: CreateScan — Erteilt die Erlaubnis, einen Sicherheitsscan zu erstellen CodeGuru .
  - codeguru-security: GetScan — Erteilt die Erlaubnis, Metadaten des Sicherheitsscans abzurufen. CodeGuru
  - codeguru-security: ListFindings — Erteilt die Erlaubnis, von Security generierte Ergebnisse abzurufen. CodeGuru
  - codeguru-security: DeleteScansByCategory — Erteilt der Sicherheitsabteilung die Erlaubnis, von Amazon CodeGuru Inspector initiierte Scans zu löschen.
  - codeguru-security: BatchGetFindings — Erteilt die Erlaubnis, eine Reihe von spezifischen Ergebnissen abzurufen, die von Security generiert wurden. CodeGuru
- Verwenden Sie ausgewählte Elastic Load Balancing Balancing-Aktionen, um Netzwerkscans von EC2-Instances durchzuführen, die Teil der Elastic Load Balancing Balancing-Zielgruppen sind.

Die Rolle ist mit der folgenden Berechtigungsrichtlinie konfiguriert.

```
    {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "TirosPolicy",
  "Effect": "Allow",
  "Action": [
   "directconnect:DescribeConnections",
   "directconnect:DescribeDirectConnectGatewayAssociations",
   "directconnect:DescribeDirectConnectGatewayAttachments",
   "directconnect:DescribeDirectConnectGateways",
   "directconnect:DescribeVirtualGateways",
   "directconnect:DescribeVirtualInterfaces",
   "ec2:DescribeAvailabilityZones",
   "ec2:DescribeCustomerGateways",
   "ec2:DescribeInstances",
   "ec2:DescribeInternetGateways",
   "ec2:DescribeManagedPrefixLists",
   "ec2:DescribeNatGateways",
   "ec2:DescribeNetworkAcls",
   "ec2:DescribeNetworkInterfaces",
```

```
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "PackageVulnerabilityScanning",
```

```
    "Effect": "Allow",
    "Action": [
     "ecr:BatchGetImage",
     "ecr:BatchGetRepositoryScanningConfiguration",
     "ecr:DescribeImages",
     "ecr:DescribeRegistry",
     "ecr:DescribeRepositories",
     "ecr:GetAuthorizationToken",
     "ecr:GetDownloadUrlForLayer",
     "ecr:GetRegistryScanningConfiguration",
     "ecr:ListImages",
     "ecr:PutRegistryScanningConfiguration",
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization",
     "organizations:ListAccounts",
     "ssm:DescribeAssociation",
     "ssm:DescribeAssociationExecutions",
     "ssm:DescribeInstanceInformation",
     "ssm:ListAssociations",
     "ssm:ListResourceDataSync"
    ],
    "Resource": "*"
   },
   {
    "Sid": "LambdaPackageVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "lambda:ListFunctions",
     "lambda:GetFunction",
     "lambda:GetLayerVersion",
     "cloudwatch:GetMetricData"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GatherInventory",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateAssociation",
     "ssm:StartAssociationsOnce",
     "ssm:DeleteAssociation",
     "ssm:UpdateAssociation"
    ],
    "Resource": [
```

```
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ssm:*:*:document/AmazonInspector2-*",
    "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
    "arn:aws:ssm:*:*:managed-instance/*",
    "arn:aws:ssm:*:*:association/*"
   ]
  },
  {
   "Sid": "DataSyncCleanup",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateResourceDataSync",
    "ssm:DeleteResourceDataSync"
   ],
   "Resource": [
    "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
   ]
  },
  {
   "Sid": "ManagedRules",
   "Effect": "Allow",
   "Action": [
    "events:PutRule",
    "events:DeleteRule",
    "events:DescribeRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": [
    "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
   ]
  },
  {
   "Sid": "LambdaCodeVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "codeguru-security:CreateScan",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:GetFindings",
    "codeguru-security:GetScan",
    "codeguru-security:ListFindings",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:DeleteScansByCategory"
```

```
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Sid": "CodeGuruCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:GetRolePolicy",
     "iam:GetPolicy",
     "iam:GetPolicyVersion",
     "iam:ListAttachedRolePolicies",
     "iam:ListPolicies",
     "iam:ListPolicyVersions",
     "iam:ListRolePolicies",
     "lambda:ListVersionsByFunction"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "codeguru-security.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "Ec2DeepInspection",
    "Effect": "Allow",
    "Action": [
     "ssm:PutParameter",
     "ssm:GetParameters",
     "ssm:DeleteParameter"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
```

```
      }
     }
    },
    {
     "Sid": "AllowManagementOfServiceLinkedChannel",
     "Effect": "Allow",
     "Action": [
      "cloudtrail:CreateServiceLinkedChannel",
      "cloudtrail:DeleteServiceLinkedChannel"
     ],
     "Resource": [
      "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
     ],
     "Condition": {
      "StringEquals": {
       "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
     }
    },
    {
     "Sid": "AllowListServiceLinkedChannels",
     "Effect": "Allow",
     "Action": [
      "cloudtrail:ListServiceLinkedChannels"
     ],
     "Resource": [
      "*"
     ],
     "Condition": {
      "StringEquals": {
       "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
     }
    },
    {
     "Sid": "AllowToRunInvokeCisSpecificDocuments",
     "Effect": "Allow",
     "Action": [
      "ssm:SendCommand",
      "ssm:GetCommandInvocation"
     ],
     "Resource": [
      "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
     ]
```

```
  },
  {
   "Sid": "AllowToRunCisCommandsToSpecificResources",
   "Effect": "Allow",
   "Action": [
    "ssm:SendCommand"
   ],
   "Resource": [
    "arn:aws:ec2:*:*:instance/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "AllowToPutCloudwatchMetricData",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": "AWS/Inspector2"
    }
   }
  }
 ]
}
```

Eine serviceverknüpfte Rolle für Amazon Inspector erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Amazon Inspector in der AWS Management Console, der oder der AWS API aktivieren AWS CLI, erstellt Amazon Inspector die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon Inspector

Amazon Inspector erlaubt Ihnen nicht, die `AWSServiceRoleForAmazonInspector2` serviceverknüpfte Rolle zu bearbeiten. Nachdem eine serviceverknüpfte Rolle erstellt wurde, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten möglicherweise auf die Rolle verweisen. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon Inspector

Wenn Sie Amazon Inspector nicht mehr verwenden müssen, empfehlen wir Ihnen, die `AWSServiceRoleForAmazonInspector2` serviceverknüpfte Rolle zu löschen. Bevor Sie die Rolle löschen können, müssen Sie Amazon Inspector in allen Bereichen deaktivieren, in AWS-Region denen sie aktiviert ist. Wenn Sie Amazon Inspector deaktivieren, wird die Rolle nicht für Sie gelöscht. Wenn Sie Amazon Inspector erneut aktivieren, kann Amazon Inspector daher die bestehende Rolle verwenden. Auf diese Weise können Sie vermeiden, dass eine ungenutzte Entität nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Wenn Sie diese serviceverknüpfte Rolle löschen und dann erneut erstellen müssen, können Sie die Rolle in Ihrem Konto mit demselben Verfahren neu anlegen. Wenn Sie Amazon Inspector aktivieren, erstellt Amazon Inspector die serviceverknüpfte Rolle für Sie neu.

> **Note**
>
> Wenn der Amazon Inspector-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Warten Sie in diesem Fall einige Minuten und führen Sie den Vorgang dann erneut aus.

Sie können die IAM-Konsole, die oder die AWS API verwenden AWS CLI, um die `AWSServiceRoleForAmazonInspector2` serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Servicebezogene Rollenberechtigungen für agentenlose Amazon Inspector-Scans

Das agentenlose Scannen von Amazon Inspector verwendet die angegebene, mit dem Service verknüpfte Rolle. `AWSServiceRoleForAmazonInspector2Agentless` Mit dieser Spiegelreflexkamera kann Amazon Inspector einen Amazon EBS-Volume-Snapshot in Ihrem Konto

erstellen und dann auf die Daten aus diesem Snapshot zugreifen. Diese dienstbezogene Rolle vertraut darauf, dass der `agentless.inspector2.amazonaws.com` Service die Rolle übernimmt.

> **Important**
>
> Die Anweisungen in dieser servicebezogenen Rolle verhindern, dass Amazon Inspector agentenlose Scans auf allen EC2-Instances durchführt, die Sie mithilfe des Tags von Scans ausgeschlossen haben. `InspectorEc2Exclusion` Darüber hinaus verhindern die Anweisungen, dass Amazon Inspector auf verschlüsselte Daten von einem Volume zugreift, wenn der für die Verschlüsselung verwendete KMS-Schlüssel das `InspectorEc2Exclusion` Tag trägt. Weitere Informationen finden Sie unter Instances von Amazon Inspector-Scans ausschließen.

Die Berechtigungsrichtlinie für die Rolle, die benannt ist`AmazonInspector2AgentlessServiceRolePolicy`, ermöglicht es Amazon Inspector, Aufgaben wie die folgenden auszuführen:

- Verwenden Sie Amazon Elastic Compute Cloud (Amazon EC2) -Aktionen, um Informationen über Ihre EC2-Instances, Volumes und Snapshots abzurufen.
  - Verwenden Sie Amazon EC2-Tagging-Aktionen, um Schnappschüsse für Scans mit dem `InspectorScan` Tag-Schlüssel zu taggen.
  - Verwenden Sie Amazon EC2-Snapshot-Aktionen, um Snapshots zu erstellen, sie mit dem `InspectorScan` Tag-Schlüssel zu kennzeichnen und anschließend Snapshots von Amazon EBS-Volumes zu löschen, die mit dem Tag-Schlüssel gekennzeichnet wurden. `InspectorScan`
- Verwenden Sie Amazon EBS-Aktionen, um Informationen aus Snapshots abzurufen, die mit dem `InspectorScan` Tag-Schlüssel gekennzeichnet sind.
- Verwenden Sie ausgewählte AWS KMS Entschlüsselungsaktionen, um Snapshots zu entschlüsseln, die mit vom Kunden verwalteten Schlüsseln verschlüsselt wurden. AWS KMS Amazon Inspector entschlüsselt keine Snapshots, wenn der KMS-Schlüssel, mit dem sie verschlüsselt wurden, mit dem Tag gekennzeichnet ist. `InspectorEc2Exclusion`

Die Rolle ist mit der folgenden Berechtigungsrichtlinie konfiguriert.

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

```
 "Statement": [
  {
   "Sid": "InstanceIdentification",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetSnapshotData",
   "Effect": "Allow",
   "Action": [
    "ebs:ListSnapshotBlocks",
    "ebs:GetSnapshotBlock"
   ],
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "aws:ResourceTag/InspectorScan": "*"
    }
   }
  },
  {
   "Sid": "CreateSnapshotsAnyInstanceOrVolume",
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshots",
   "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
   ]
  },
  {
   "Sid": "DenyCreateSnapshotsOnExcludedInstances",
   "Effect": "Deny",
   "Action": "ec2:CreateSnapshots",
   "Resource": "arn:aws:ec2:*:*:instance/*",
   "Condition": {
    "StringEquals": {
     "ec2:ResourceTag/InspectorEc2Exclusion": "true"
    }
   }
```

```
  },
  {
   "Sid": "CreateSnapshotsOnAnySnapshotOnlyWithTag",
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshots",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "Null": {
     "aws:TagKeys": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": "InspectorScan"
    }
   }
  },
  {
   "Sid": "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
   "Effect": "Allow",
   "Action": "ec2:CreateTags",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "ec2:CreateAction": "CreateSnapshots"
    },
    "Null": {
     "aws:TagKeys": "false"
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": "InspectorScan"
    }
   }
  },
  {
   "Sid": "DeleteOnlySnapshotsTaggedForScanning",
   "Effect": "Allow",
   "Action": "ec2:DeleteSnapshot",
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "ec2:ResourceTag/InspectorScan": "*"
    }
   }
  },
  {
```

```
    "Sid": "DenyKmsDecryptForExcludedKeys",
    "Effect": "Deny",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksVolContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "vol-*"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksSnapContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "snap-*"
     }
    }
   },
   {
    "Sid": "DescribeKeysForEbsOperations",
    "Effect": "Allow",
    "Action": "kms:DescribeKey",
```

```
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ListKeyResourceTags",
    "Effect": "Allow",
    "Action": "kms:ListResourceTags",
    "Resource": "arn:aws:kms:*:*:key/*"
   }
  ]
}
```

Erstellung einer dienstbezogenen Rolle für agentenloses Scannen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Amazon Inspector in der AWS Management Console, der oder der AWS API aktivieren AWS CLI, erstellt Amazon Inspector die serviceverknüpfte Rolle für Sie.

Bearbeitung einer serviceverknüpften Rolle für agentenloses Scannen

Amazon Inspector erlaubt Ihnen nicht, die `AWSServiceRoleForAmazonInspector2Agentless` serviceverknüpfte Rolle zu bearbeiten. Nachdem eine serviceverknüpfte Rolle erstellt wurde, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten möglicherweise auf die Rolle verweisen. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für das Scannen ohne Agenten

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Um die `AWSServiceRoleForAmazonInspector2Agentless` Rolle zu löschen, müssen Sie Ihren Scanmodus in allen Regionen, in denen agentenloses Scannen verfügbar ist, auf agentenbasiert einstellen. Weitere Informationen finden Sie unter [Link zur Einstellung des Scanmodus wird noch bekannt gegeben].

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForAmazonInspector2Agentless serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Fehlerbehebung bei Identität und Zugriff auf Amazon Inspector

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Inspector und IAM auftreten können.

Themen

Ich bin nicht berechtigt, eine Aktion in Amazon Inspector durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `inspector2:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector2:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `inspector2:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon Inspector übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon Inspector auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon Inspector Inspector-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon Inspector diese Funktionen unterstützt, finden Sie unterSo arbeitet Amazon Inspector mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Überwachung von Amazon Inspector

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Inspector und Ihren anderen AWS Lösungen. AWS bietet Überwachungstools, um Amazon Inspector zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, oftware-as-a S-Service (SaaS) -Anwendungen und AWS Diensten und leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können Sie Ereignisse überwachen, die in Diensten auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihrer AWS-Konto. CloudTrail übermittelt dann die Protokolldateien an einen Amazon S3 S3-Bucket, den Sie angeben. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Protokollieren Amazon Inspector Inspector-API-Aufrufen mit AWS CloudTrail

Amazon Inspector ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem IAM-Benutzer oder einer IAM-Rolle oder einem AWS-Service in Amazon Inspector ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Amazon Inspector als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon Inspector Inspector-Konsole und Aufrufe der Amazon Inspector Inspector-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon Inspector. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie Folgendes ermitteln:

- Die Anfrage, die an Amazon Inspector gestellt wurde.
- Die IP-Adresse, von der die Anforderung erfolgt ist.
- Wer die Anfrage gestellt hat.
- Wann die Anfrage gestellt wurde.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zu Amazon Inspector in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Amazon Inspector eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Amazon Inspector, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter den folgenden Themen:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien von mehreren Konten
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen

Alle Amazon Inspector Inspector-Aktionen werden von protokolliert CloudTrail. Alle Aktionen, die Amazon Inspector ausführen kann, sind in der Amazon Inspector API-Referenz dokumentiert. Aufrufe von, und `UpdateOrganizationConfiguration` Aktionen generieren beispielsweise Einträge in den CloudTrail Protokolldateien. `CreateFindingsReport` `ListCoverage`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Stammbenutzers oder des IAM-Benutzers gestellt wurde.
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter dem CloudTrail UserIdentity-Element.

Grundlegendes zu Amazon Inspector Inspector-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Ereignisse enthalten unter anderem Informationen über die angeforderte Aktion, etwaige Anforderungsparameter und das Datum und die Uhrzeit der Aktion. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Amazon Inspector Scaninformationen in CloudTrail

Amazon Inspector Scan ist in integriert CloudTrail. Alle Amazon Inspector Scan API-Operationen werden als Verwaltungsereignisse protokolliert. Eine Liste der Amazon Inspector Scan API-

Operationen, bei denen Amazon Inspector protokolliert CloudTrail, finden Sie unter Amazon Inspector Scan in der Amazon Inspector API-Referenz.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ScanSbom` Aktion demonstriert:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:akua_mansa",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/akua_mansa",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-17T15:22:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-17T16:02:34Z",
    "eventSource": "gamma-inspector-scan.amazonaws.com",
    "eventName": "ScanSbom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "aws-sdk-java/2.20.162 Mac_OS_X/13.5.2 OpenJDK_64-
Bit_Server_VM/17.0.8+7-LTS Java/17.0.8 vendor/Amazon.com_Inc. io/sync http/
UrlConnection cfg/retry-mode/legacy",
    "requestParameters": {
        "sbom": {
            "specVersion": "1.5",
            "metadata": {
                "component": {
                    "name": "debian",
                    "type": "operating-system",
```

```
                    "version": "9"
                }
            },
            "components": [
                {
                    "name": "packageOne",
                    "purl": "pkg:deb/debian/packageOne@1.0.0?arch=x86_64&distro=9",
                    "type": "application"
                }
            ],
            "bomFormat": "CycloneDX"
        }
    },
    "responseElements": null,
    "requestID": "f041a27f-f33e-4f70-b09b-5fbc5927282a",
    "eventID": "abc8d1e4-d214-4f07-bc56-8a31be6e36fe",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Konformitätsvalidierung für Amazon Inspector

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in Amazon Inspector

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz,

hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Infrastruktursicherheit in Amazon Inspector

Als verwalteter Service ist Amazon Inspector durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon Inspector zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Reaktion auf Vorfälle in Amazon Inspector

Sicherheit hat bei uns höchste Priorität AWS. AWS Verwaltet im Rahmen des Modells der gemeinsamen Verantwortung in der AWS Cloud eine Rechenzentrums-, Netzwerk- und Softwarearchitektur, die die Anforderungen der sicherheitssensibelsten Unternehmen erfüllt. AWS ist verantwortlich für jegliche Reaktion auf Vorfälle in Bezug auf den AWS Config Service selbst. Außerdem tragen Sie als AWS Kunde gemeinsam die Verantwortung für die Aufrechterhaltung der Sicherheit in der Cloud. Das bedeutet, dass Sie anhand der AWS Tools und Funktionen, auf die Sie Zugriff haben, die Sicherheit kontrollieren, die Sie implementieren möchten, und dass Sie im Rahmen des Modells der gemeinsamen Verantwortung für die Reaktion auf Vorfälle verantwortlich sind.

Indem Sie eine Sicherheitsbasis einrichten, die den Zielen Ihrer in der Cloud ausgeführten Anwendungen entspricht, können Sie Abweichungen erkennen, auf die Sie reagieren können. Da die Reaktion auf Sicherheitsvorfälle ein komplexes Thema sein kann, empfehlen wir Ihnen, die folgenden Ressourcen zu lesen, damit Sie besser verstehen, welche Auswirkungen Incident Response (IR) und Ihre Entscheidungen auf Ihre Unternehmensziele haben: Leitfaden zur Reaktion auf AWS Sicherheitsvorfälle, Whitepaper zu bewährten AWS Sicherheitsmethoden und das Whitepaper Security Perspective of the AWS Cloud Adoption Framework (CAF).

Amazon Inspector Inspector-Integrationen

Amazon Inspector lässt sich in andere AWS Dienste integrieren. Diese Dienste können Daten von Amazon Inspector aufnehmen, sodass Sie Ihre Ergebnisse auf neue Weise betrachten können. Sehen Sie sich die folgenden Integrationsoptionen an, um mehr darüber zu erfahren, wie dieser Service für die Zusammenarbeit mit Amazon Inspector eingerichtet ist.

Integration von Amazon Inspector mit Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) ist eine vollständig verwaltete Docker-Container-Registry, die das Speichern, Teilen und Bereitstellen von Container-Images vereinfacht. Private Registrys von Amazon ECR hosten Ihre Container-Images in einer hochverfügbaren und skalierbaren Architektur. Sie können Amazon Inspector verwenden, um Container-Images, die sich in Ihren Amazon ECR-Repositorys befinden, nach anfälligen Betriebssystempaketen und Programmiersprachenpaketen zu durchsuchen.

Weitere Informationen zur Verwendung von Amazon ECR mit Amazon Inspector finden Sie unterIntegration von Amazon Inspector mit Amazon Elastic Container Registry (Amazon ECR).

Amazon Inspector Inspector-Integration mit AWS Security Hub

AWS Security Hubsammelt Sicherheitsdaten aus all Ihren AWS Konten, Diensten und anderen unterstützten Produkten, um den Sicherheitsstatus Ihrer Umgebung gemäß Industriestandards und Best Practices zu bewerten. Security Hub bewertet nicht nur Ihren Sicherheitsstatus, sondern bietet auch einen zentralen Ort für Erkenntnisse aus all Ihren integrierten AWS Services und AWS Partnernetzwerk-Produkten. Durch die Aktivierung von Security Hub mit Amazon Inspector kann Security Hub automatisch Amazon Inspector-Ergebnisdaten aufnehmen.

Weitere Informationen zur Verwendung von Security Hub mit Amazon Inspector finden Sie unterAmazon Inspector Inspector-Integration mit AWS Security Hub.

Integration von Amazon Inspector mit Amazon Elastic Container Registry (Amazon ECR)

Amazon ECR ist eine vollständig verwaltete Container-Registry, die Docker- und OCI-Images und -Artefakte unterstützt. AWS Wenn Sie Amazon ECR verwenden, können Sie Enhanced Scanning für

Ihre Registrierung aktivieren, damit Amazon Inspector Ihre Container-Images automatisch erkennt und sie nach anfälligen Betriebssystempaketen und Programmiersprachenpaketen durchsucht.

Diese Integration ermöglicht es Ihnen, die Ergebnisse von Amazon Inspector für Container-Images in der Amazon ECR-Konsole anzuzeigen. Darüber hinaus können Sie von der Amazon ECR-Konsole aus die Scan-Häufigkeit verwalten und den Umfang der Scans verfeinern, indem Sie Einschlussfilter erstellen.

Aktivierung der Integration

Sie können die Integration aktivieren, indem Sie das Amazon Inspector-Scannen über die Amazon Inspector-Konsole oder API aktivieren oder indem Sie Ihr Repository so konfigurieren, dass es Enhanced Scanning mit Amazon Inspector über die Amazon ECR-Konsole oder API verwendet.

Weitere Informationen zur Aktivierung der Integration über Amazon Inspector finden Sie unterAutomatisiertes Scannen von Ressourcen mit Amazon Inspector.

Informationen zur Aktivierung und Konfiguration von Enhanced Scanning in Amazon ECR finden Sie unter Enhanced Scanning im Amazon ECR-Benutzerhandbuch.

Verwendung der Integration in einer Umgebung mit mehreren Konten

Wenn Sie Mitglied in einer Umgebung mit mehreren Konten sind, können Sie das erweiterte Scannen über Amazon ECR aktivieren. Nach der Aktivierung kann es jedoch nur von Ihrem delegierten Amazon Inspector-Administrator deaktiviert werden. Wenn es deaktiviert ist, kehrt es zum normalen Scannen zurück. Weitere Informationen finden Sie unter Amazon Inspector deaktivieren.

Amazon Inspector Inspector-Integration mit AWS Security Hub

Security Hub bietet einen umfassenden Überblick über Ihren Sicherheitsstatus AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Security Hub sammelt Sicherheitsdaten von AWS Konten, Diensten und weiteren unterstützten Produkten. Sie können die bereitgestellten Informationen verwenden, um Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

Die Integration von Amazon Inspector mit Security Hub ermöglicht es Ihnen, Ergebnisse von Amazon Inspector an Security Hub zu senden. Der Security Hub kann diese Erkenntnisse dann in die Analyse Ihres Sicherheitsniveaus einbeziehen.

In AWS Security Hub werden Sicherheitsprobleme als Ergebnisse nachverfolgt. Einige Ergebnisse resultieren aus Problemen, die von anderen AWS Diensten oder Produkten von Drittanbietern entdeckt wurden. Security Hub verwendet ebenfalls verschiedene Regeln, um Sicherheitsprobleme zu erkennen und Ergebnisse zu generieren. Security Hub bietet Tools zur Verwaltung von Erkenntnissen aus all diesen Quellen. Sie können Ergebnislisten und Ergebnisdetails anzeigen und filtern. Weitere Informationen zu Ergebnissen in Security Hub finden Sie unter Ergebnisse anzeigen im AWS Security Hub Benutzerhandbuch. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Siehe Ergreifen von Maßnahmen zu Ergebnissen im AWS Security Hub -Leitfaden.

Alle Ergebnisse in Security Hub verwenden ein standardmäßiges JSON-Format, das AWS Security Finding Format (ASFF). Das ASFF enthält Details über die Ursache des Problems, die betroffenen Ressourcen und den aktuellen Status der Erkenntnis. Siehe AWS -Security Finding-Format (ASFF) im AWS Security Hub -Leitfaden.

Security Hub archiviert die Ergebnisse von Amazon Inspector, sobald diese Ergebnisse in Amazon Inspector behoben und geschlossen wurden.

Ergebnisse von Amazon Inspector anzeigen in AWS Security Hub

Die Ergebnisse von Amazon Inspector Classic und dem neuen Amazon Inspector sind im selben Bereich in Security Hub verfügbar. Sie können jedoch Ergebnisse aus dem neuen Amazon Inspector filtern, indem Sie der Filterleiste eine `"aws/inspector/ProductVersion": "2"` hinzufügen. Durch das Hinzufügen dieses Filters werden Ergebnisse von Amazon Inspector Classic aus dem Security Hub-Dashboard ausgeschlossen.

Beispiel für ein Ergebnis von Amazon Inspector

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "ProductName": "Inspector",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "AWSInspector",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ],
  "FirstObservedAt": "2023-01-31T20:25:38Z",
```

```
  "LastObservedAt": "2023-05-04T18:18:43Z",
  "CreatedAt": "2023-01-31T20:25:38Z",
  "UpdatedAt": "2023-05-04T18:18:43Z",
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "CVE-2022-34918 - kernel",
  "Description": "An issue was discovered in the Linux kernel through 5.18.9. A type
 confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a
 local attacker to escalate privileges, a different vulnerability than CVE-2022-32250.
 (The attacker can obtain root access, but must start with an unprivileged user
 namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data
 in net/netfilter/nf_tables_api.c.",
  "Remediation": {
    "Recommendation": {
      "Text": "Remediation is available. Please refer to the Fixed version in the
 vulnerability details section above. For detailed remediation guidance for each of the
 affected packages, refer to the vulnerabilities section of the detailed finding JSON."
    }
  },
  "ProductFields": {
    "aws/inspector/FindingStatus": "ACTIVE",
    "aws/inspector/inspectorScore": "7.8",
    "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform":
 "AMAZON_LINUX_2",
    "aws/inspector/ProductVersion": "2",
    "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Patch Group": "SSM",
        "Name": "High-SEv-Test"
      },
      "Details": {
```

```
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-0cff7528ff583bf9a",
          "IpV4Addresses": [
            "52.87.229.97",
            "172.31.57.162"
          ],
          "KeyName": "ACloudGuru",
          "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-9c934cb1",
          "LaunchedAt": "2022-07-26T21:49:46Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "Vulnerabilities": [
    {
      "Id": "CVE-2022-34918",
      "VulnerablePackages": [
        {
          "Name": "kernel",
          "Version": "5.10.118",
          "Epoch": "0",
          "Release": "111.515.amzn2",
          "Architecture": "X86_64",
          "PackageManager": "OS",
          "FixedInVersion": "0:5.10.130-118.517.amzn2",
          "Remediation": "yum update kernel"
        }
      ],
      "Cvss": [
        {
          "Version": "2.0",
          "BaseScore": 7.2,
          "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
          "Source": "NVD"
        },
```

```
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD",
          "Adjustments": []
        }
      ],
      "Vendor": {
        "Name": "NVD",
        "Url": "https://nvd.nist.gov/vuln/detail/CVE-2022-34918",
        "VendorSeverity": "HIGH",
        "VendorCreatedAt": "2022-07-04T21:15:00Z",
        "VendorUpdatedAt": "2022-10-26T17:05:00Z"
      },
      "ReferenceUrls": [
        "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?
id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6",
        "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-
d86f4869f452@randorisec.fr/T/",
        "https://www.debian.org/security/2022/dsa-5191"
      ],
      "FixAvailable": "YES"
    }
  ],
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
  },
  "ProcessedAt": "2023-05-05T20:28:38.822Z"
}
```

Aktivierung und Konfiguration der Integration

Um die Amazon Inspector Inspector-Integration mit verwenden zu können AWS Security Hub, müssen Sie Security Hub aktivieren. Informationen zur Aktivierung von Security Hub finden Sie unter Security Hub einrichten im AWS Security Hub Benutzerhandbuch.

Wenn Sie sowohl Amazon Inspector als auch Security Hub aktivieren, wird die Integration automatisch aktiviert und Amazon Inspector beginnt, Ergebnisse an Security Hub zu senden. Amazon Inspector sendet alle von ihm generierten Ergebnisse mithilfe des AWS Security Finding Formats (ASFF) an Security Hub.

Stoppt die Veröffentlichung der Ergebnisse an AWS Security Hub

Wie kann ich das Senden von Ergebnissen beenden

Um keine Ergebnisse mehr an Security Hub zu senden, können Sie entweder die Security Hub-Konsole oder die API verwenden.

Weitere Informationen finden Sie unter Deaktivierung und Aktivierung des Ergebnisflusses aus einer Integration (Konsole) oder Deaktivierung des Ergebnisflusses aus einer Integration (Security Hub Hub-API AWS CLI) im AWS Security Hub Benutzerhandbuch.

Von Amazon Inspector unterstützte Betriebssysteme und Programmiersprachen

Amazon Inspector kann Softwareanwendungen scannen, die auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances installiert sind, Container-Images, die in Amazon Elastic Container Registry (Amazon ECR) -Repositorys gespeichert sind, und Funktionen. AWS Lambda Bei ECR-Container-Images kann Amazon Inspector sowohl nach Sicherheitslücken im Betriebssystem als auch in Programmiersprachenpaketen suchen. Bei Lambda-Funktionen kann Amazon Inspector nach Code-Schwachstellen suchen. Wenn Amazon Inspector Ressourcen scannt, verwendet es seine eigene, speziell entwickelte Scan-Engine und bezieht mehr als 50 Datenfeeds, um Ergebnisse für Common Vulnerabilities and Exposures (CVEs) zu generieren. Zu den Quellen gehören Sicherheitsempfehlungen von Anbietern, NVD, MITRE, Open-Source-Feeds, interne Recherchen und lizenzierte Datenfeeds.

Damit Amazon Inspector eine Ressource scannen kann, muss auf der Ressource ein unterstütztes Betriebssystem ausgeführt werden oder eine unterstützte Programmiersprache verwendet werden. In den Themen in diesem Abschnitt sind die Betriebssysteme, Laufzeiten und Programmiersprachen aufgeführt, die Amazon Inspector derzeit für verschiedene Ressourcen und Scantypen unterstützt. Sie listen auch Betriebssysteme auf, die Amazon Inspector zuvor unterstützt hat, die aber inzwischen von Anbietern eingestellt wurden. Amazon Inspector kann nur eingeschränkten Support für ein Betriebssystem anbieten, nachdem ein Anbieter den Support für das Betriebssystem eingestellt hat.

Themen

Unterstützte Betriebssysteme: Amazon EC2-Scanning

In der folgenden Tabelle sind die Betriebssysteme aufgeführt, die Amazon Inspector derzeit für Scans von Amazon EC2 EC2-Instances unterstützt. Außerdem wird die Quelle der Sicherheitsempfehlungen des jeweiligen Anbieters aufgeführt und angegeben, ob das jeweilige Betriebssystem mit der agentenbasierten oder agentenlosen Scanmethode gescannt werden kann. Weitere Informationen zu Suchmethoden finden Sie unter und. Agentengestütztes Scannen Scannen ohne Agenten

> **Note**
>
> Erkennungen von Linux-Betriebssystemen werden nur für das Standard-Paketmanager-Repository unterstützt und schließen keine Anwendungen von Drittanbietern, Repositorys mit erweitertem Support (z. B. BYOS RHEL, PAYG RHEL und RHEL für SAP) und optionale Repositorys wie Red Hat Application Streams ein.

Betriebssystem	Version	Sicherheitsempfehlungen von Anbietern	Unterstützung für agentenloses Scannen	Unterstützung für agentengestütztes Scannen
AlmaLinux	8	ALSA	Ja	Ja
AlmaLinux	9	ALSA	Ja	Ja
Amazon Linux (AL2)	AL 2	LEIDER	Ja	Ja
Amazon Linux 2023 (AL2023)	AL2023	LEIDER	Ja	Ja
Bottlerocket	1.7.0 und später	GHSA, CVE	Nein	Ja
CentOS Linux (CentOS)	7	CESA	Ja	Ja
Debian-Server (Buster)	10	DSA	Ja	Ja

Betriebssystem	Version	Sicherheitsempfehlungen von Anbietern	Unterstützung für agentenloses Scannen	Unterstützung für agentengestütztes Scannen
Debian-Server (Bullseye)	11	DSA	Ja	Ja
Debian-Server (Bücherwurm)	12	DSA	Ja	Ja
Fedora	38	CVE	Ja	Ja
Fedora	39	CVE	Ja	Ja
OpenSUSE	15,5	CVE	Ja	Ja
Oracle Linux (Oracle)	7	ELSA	Ja	Ja
Oracle Linux (Oracle)	8	ELSA	Ja	Ja
Oracle Linux (Oracle)	9	ELSA	Ja	Ja
Red Hat Enterprise Linux (RHEL)	7	RHSA	Ja	Ja
Red Hat Enterprise Linux (RHEL)	8	RHSA	Ja	Ja
Red Hat Enterprise Linux (RHEL)	9	RHSA	Ja	Ja
Rocky Linux	8	RLSA	Ja	Ja
Rocky Linux	9	RLSA	Ja	Ja

Betriebssystem	Version	Sicherheitsempfehlungen von Anbietern	Unterstützung für agentenloses Scannen	Unterstützung für agentengestütztes Scannen
SUSE Linux Enterprise Server (SLES)	12.4	SUSE-HÖHLE	Ja	Ja
SUSE Linux Enterprise Server (SLES)	12,5	SUSIE CVE	Ja	Ja
SUSE Linux Enterprise Server (SLES)	15,3	HÖHLE SUES	Ja	Ja
SUSE Linux Enterprise Server (SLES)	15,4	SUSE-HÖHLE	Ja	Ja
SUSE Linux Enterprise Server (SLES)	15,5	SUSE-HÖHLE	Ja	Ja
Ubuntu (vertrauenswürdig)	14.04 (ESM)	USB, Ubuntu Pro	Ja	Ja
Ubuntu (Xenial)	16,04 (ESM)	USB, Ubuntu Pro	Ja	Ja
Ubuntu (Bionisch)	18,04 (ESM)	USB, Ubuntu Pro	Ja	Ja
Ubuntu (fokal)	20.04 (LTS)	SONNE	Ja	Ja
Ubuntu (Jammy)	22,04 (LTS)	SONNE	Ja	Ja
Ubuntu (Mantischer Minotaurus)	23,10	SONNE	Ja	Ja

Betriebssystem	Version	Sicherheitsempfehlungen von Anbietern	Unterstützung für agentenloses Scannen	Unterstützung für agentengestütztes Scannen
Windows Server	2016	MSKB	Nein	Ja
Windows Server	2019	MSKB	Nein	Ja
Windows Server	2022	MSKB	Nein	Ja
macOS (Mojave)	10.14	APPLE-SA	Nein	Ja
macOS (Catalina)	10.15	APPLE-SA	Nein	Ja
macOS (Big Sur)	11	APPLE-SA	Nein	Ja
macOS (Monterey)	12	APPLE-SA	Nein	Ja
macOS (Ventura)	13	APPLE-SA	Nein	Ja

Unterstützte Programmiersprachen: Amazon EC2 Deep Inspection

Amazon Inspector unterstützt derzeit die folgenden Programmiersprachen beim Scannen von Amazon EC2 EC2-Linux-Instances auf Sicherheitslücken in Softwarepaketen von Drittanbietern:

- Java
- JavaScript
- Python

Amazon Inspector verwendet Systems Manager Distributor, um das für die Tiefeninspektion verwendete Plugin in Ihrer Amazon EC2 EC2-Instance bereitzustellen. Systems Manager Distributor unterstützt die Betriebssysteme, die im Systems Manager-Handbuch als Unterstützte Paketplattformen und Architekturen aufgeführt sind. Das Betriebssystem Ihrer Amazon EC2 EC2-

Instance muss von Systems Manager Distributor und Amazon Inspector für Amazon Inspector unterstützt werden, um Deep Inspection-Scans durchführen zu können.

> **Note**
>
> Deep Inspection wird für Bottlerocket-Betriebssysteme nicht unterstützt.

Unterstützte Betriebssysteme: CIS-Scanning

In der folgenden Tabelle sind die Betriebssysteme aufgeführt, die Amazon Inspector derzeit für CIS-Scans unterstützt. Die Tabelle enthält auch die CIS-Benchmark-Version, die für die Durchführung von Scans dieses Betriebssystems verwendet wurde.

Betriebssystem	Version	CIS-Benchmark-Version
Amazon Linux 2	AL2	2.0.0
Amazon Linux 2023	AL2023	1.0.0
Windows Server	2019	2.0.0
Windows Server	2022	2.0.0

Unterstützte Betriebssysteme: Amazon ECR-Scannen mit Amazon Inspector

Amazon Inspector unterstützt derzeit das Scannen der folgenden Betriebssysteme beim Scannen von Container-Images in Amazon ECR-Repositorys:. In der Tabelle ist auch die Quelle der Sicherheitsempfehlungen des Anbieters für jedes Betriebssystem aufgeführt.

Betriebssystem	Version	Sicherheitsempfehlungen der Anbieter
Alpine Linux (Alpine)	3.16	Alpine SecDB

Betriebssystem	Version	Sicherheitsempfehlungen der Anbieter
Alpine Linux (Alpine)	3.17	Alpine SecDB
Alpine Linux (Alpine)	3.18	Alpine SecDB
Alpine Linux (Alpine)	3.19	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
CentOS Linux (CentOS)	7	CESA
Debian Server (Buster)	10	DSA
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA
Fedora	38	CVE
Fedora	39	CVE
OpenSUSE	15.5	CVE
Oracle Linux (Oracle)	7	ELSA
Oracle Linux (Oracle)	8	ELSA
Oracle Linux (Oracle)	9	ELSA
Photon OS	3	PHSA
Photon OS	4	PHSA
Photon OS	5	PHSA

Betriebssystem	Version	Sicherheitsempfehlungen der Anbieter
Red Hat Enterprise Linux (RHEL)	7	RHSA
Red Hat Enterprise Linux (RHEL)	8	RHSA
Red Hat Enterprise Linux (RHEL)	9	RHSA
Rocky Linux	8	RLSA
Rocky Linux	9	RLSA
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12.5	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE
Ubuntu (Trusty)	14.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Focal)	20.04 (LTS)	USN
Ubuntu (Jammy)	22.04 (LTS)	USN

Betriebssystem	Version	Sicherheitsempfehlungen der Anbieter
Ubuntu (Mantic Minotaur)	23.10	USN

Unterstützte Programmiersprachen: Amazon ECR Scanning

Amazon Inspector unterstützt derzeit die folgenden Programmiersprachen beim Scannen von Container-Images in Amazon ECR-Repositorys:

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

Unterstützte Laufzeiten: Amazon Inspector Lambda Standard-Scanning

Das Standard-Scannen von Amazon Inspector Lambda unterstützt derzeit die folgenden Programmiersprachen beim Scannen von Lambda-Funktionen auf Sicherheitslücken in Softwarepaketen von Drittanbietern:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x

  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

Unterstützte Laufzeiten: Amazon Inspector Lambda-Code-Scanning

Das Scannen von Lambda-Code mit Amazon Inspector unterstützt derzeit die folgenden Programmiersprachen beim Scannen von Lambda-Funktionen auf Sicherheitslücken im Code:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x

  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Ruby
  - ruby2.7
  - ruby3.2

Nicht mehr erhältliche Betriebssysteme

Der standardmäßige Herstellersupport für die in den folgenden Tabellen aufgeführten Betriebssysteme wurde vom Anbieter eingestellt. In den Tabellen gibt die Spalte Nicht mehr an, wann der Hersteller den Standardsupport für ein Betriebssystem eingestellt hat.

Amazon Inspector bot zuvor volle Unterstützung für diese Betriebssysteme und wird weiterhin Amazon EC2 EC2-Instances und Amazon ECR-Container-Images scannen, auf denen sie ausgeführt werden. Gemäß den Herstellerrichtlinien werden die Betriebssysteme jedoch nicht mehr mit Patches aktualisiert, und in vielen Fällen werden keine neuen Sicherheitsempfehlungen mehr für sie veröffentlicht. Darüber hinaus entfernen einige Anbieter bestehende Sicherheitsempfehlungen und Sicherheitswarnungen aus ihren Feeds, wenn für ein betroffenes Betriebssystem der Standardsupport ausläuft. Infolgedessen generiert Amazon Inspector möglicherweise keine Ergebnisse mehr für bekannte CVEs. Alle Ergebnisse, die Amazon Inspector für ein eingestelltes Betriebssystem generiert, sollten nur zu Informationszwecken verwendet werden.

Aus Sicherheitsgründen und zur kontinuierlichen Berichterstattung über Amazon Inspector empfehlen wir Ihnen, zu einer aktuellen, unterstützten Version eines Betriebssystems zu wechseln.

Eingestellte Betriebssysteme: Amazon EC2-Scannen

Betriebssystem	Version	Nicht mehr angeboten
Amazon Linux (AL1)	2012	31. Dezember 2021
CentOS Linux (CentOS)	8	31. Dezember 2021
Debian-Server (Stretch)	9	30. Juni 2022
Fedora	35	13. Dezember 2022
Fedora	36	16. Mai 2023
Fedora	37	05. Dezember 2023
OpenSUSE	15.3	01. Dezember 2022
OpenSUSE	15.4	07. Dezember 2023
openSUSE Leap (SUSE Leap)	15.2	1. Dezember 2021
Oracle Linux (Oracle)	6	1. März 2021
SUSE Linux Enterprise Server (SLES)	12	1. Juli 2019
SUSE Linux Enterprise Server (SLES)	12.1	31. Mai 2020
SUSE Linux Enterprise Server (SLES)	12.2	31. März 2021
SUSE Linux Enterprise Server (SLES)	12.3	30. Juni 2022
SUSE Linux Enterprise Server (SLES)	15	31. Dezember 2019
SUSE Linux Enterprise Server (SLES)	15,1	31. Januar 2021

Betriebssystem	Version	Nicht mehr angeboten
SUSE Linux Enterprise Server (SLES)	15.2	31. Dezember 2021
Ubuntu (Groovy)	20,10	22. Juli 2021
Ubuntu (Hirsute)	21,04	20. Januar 2022
Ubuntu (Impish)	21.10	31. Juli 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024
Windows Server	2012	10. Oktober 2023
Windows Server	2012 R2	10. Oktober 2023

Eingestellte Betriebssysteme: Amazon ECR Scanning

Betriebssystem	Version	Nicht mehr angeboten
Alpine Linux (Alpine)	3.12	01.Mai 2022
Alpines Linux (Alpin)	3.13	1. November 2022
Alpine Linux (Alpine)	3.14	May 1, 2023
Alpine Linux (Alpine)	3.15	November 1, 2023
Amazon Linux (AL1)	2012	31. Dezember 2021
CentOS Linux (CentOS)	8	31. Dezember 2021
Debian-Server (Stretch)	9	30. Juni 2022
Fedora	35	13. Dezember 2022
Fedora	36	16. Mai 2023

Betriebssystem	Version	Nicht mehr angeboten
OpenSUSE	15.3	01. Dezember 2022
OpenSUSE	15.4	December 7, 2023
openSUSE Leap (SUSE Leap)	15.2	1. Dezember 2021
Oracle Linux (Oracle)	6	1. März 2021
SUSE Linux Enterprise Server (SLES)	12	1. Juli 2019
SUSE Linux Enterprise Server (SLES)	12.1	31. Mai 2020
SUSE Linux Enterprise Server (SLES)	12.2	31. März 2021
SUSE Linux Enterprise Server (SLES)	12.3	30. Juni 2022
SUSE Linux Enterprise Server (SLES)	15	31. Dezember 2019
SUSE Linux Enterprise Server (SLES)	15,1	31. Januar 2021
SUSE Linux Enterprise Server (SLES)	15.2	31. Dezember 2021
Ubuntu (Groovy)	20,10	22. Juli 2021
Ubuntu (Hirsute)	21,04	20. Januar 2022
Ubuntu (Impish)	21.10	31. Juli 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024

Amazon Inspector deaktivieren

Sie können Amazon Inspector in jedem Fall deaktivieren, AWS-Region indem Sie die Amazon Inspector Inspector-Konsole oder API verwenden. Folgen Sie den Anweisungen am Ende dieses Themas, um Amazon Inspector zu deaktivieren. Wenn Sie alle Amazon Inspector-Scans für einen deaktivieren AWS-Konto, wird Amazon Inspector für dieses Konto automatisch deaktiviert. Informationen zur Deaktivierung von Scantypen für verschiedene Ressourcen finden Sie unter. Automatisiertes Scannen von Ressourcen mit Amazon Inspector

Nachdem Amazon Inspector für ein Konto deaktiviert wurde, werden alle Scantypen für dieses Konto in dieser Region deaktiviert. Darüber hinaus werden alle Amazon Inspector-Scaneinstellungen, Unterdrückungsregeln sowie Filter und Ergebnisse für das Konto in dieser Region gelöscht.

Die Nutzung von Amazon Inspector wird Ihnen nicht in Rechnung gestellt, solange Amazon Inspector für Ihr Konto in dieser Region deaktiviert ist. Nachdem Sie Amazon Inspector deaktiviert haben, können Sie ihn zu einem späteren Zeitpunkt erneut aktivieren.

> **Note**
>
> Bevor Sie Amazon Inspector deaktivieren, empfehlen wir Ihnen, Ihre Ergebnisse zu exportieren. Weitere Informationen finden Sie unter Ergebnisberichte aus Amazon Inspector exportieren.

Wenn Sie das Amazon Inspector Amazon EC2-Scannen deaktivieren, werden die folgenden von Amazon Inspector verwendeten SSM-Verknüpfungen gelöscht:

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`. Darüber hinaus wird das Amazon Inspector SSM-Plugin, das über diese Verknüpfung installiert wurde, von all Ihren Windows Hosts entfernt. Weitere Informationen finden Sie unter Instanzen scannen Windows.

Voraussetzungen

Abhängig von Ihrem Kontotyp müssen Sie möglicherweise zusätzliche Schritte ausführen, bevor Sie Amazon Inspector wie folgt deaktivieren:

- Wenn Sie ein eigenständiges Amazon Inspector Inspector-Konto haben, können Sie es jederzeit deaktivieren.
- Wenn Sie ein Mitgliedskonto in einer Amazon Inspector Inspector-Umgebung mit mehreren Konten sind, können Sie Ihren eigenen Service nicht deaktivieren. Sie müssen sich an den delegierten Administrator Ihrer Organisation wenden, um Ihren Service zu deaktivieren.
- Wenn Sie ein delegierter Administrator sind, müssen Sie alle Ihre Mitgliedskonten trennen, bevor Sie Amazon Inspector deaktivieren können. Weitere Informationen finden Sie unter Verknüpfung von Mitgliedskonten in Amazon Inspector aufheben.

> **Note**
>
> Durch das Trennen eines Kontos wird Amazon Inspector für dieses Konto nicht deaktiviert. Stattdessen wird ein getrenntes Mitgliedskonto zu einem eigenständigen Konto.

> **Note**
>
> Wenn Sie Amazon Inspector als delegierter Administrator deaktivieren, ist die Funktion zur automatischen Aktivierung für Ihre Organisation deaktiviert.

Amazon Inspector deaktivieren

Console

Um Amazon Inspector zu deaktivieren

1. Öffnen Sie die Amazon Inspector Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Amazon Inspector deaktivieren möchten.
3. Wählen Sie im Navigationsbereich Allgemeine Einstellungen aus.
4. Wählen Sie „Inspector deaktivieren“.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie in das Textfeld deaktivieren ein und wählen Sie dann Inspector deaktivieren.

6. (Empfohlen) Wiederholen Sie diese Schritte in jeder Region, für die Sie Amazon Inspector deaktivieren möchten.

API

Führen Sie den Vorgang „API deaktivieren“ aus. Geben Sie in der Anfrage die Konto-IDs an, die Sie deaktivieren, und `EC2, ECR, LAMBDA` für `resourceTypes` die Deaktivierung aller Scans, wodurch das Konto deaktiviert wird.

Kontingente für Amazon Inspector

Ihr AWS Konto hat die folgenden Kontingente für Amazon Inspector pro Region.

Ressource	Standard	Kommentare
Unterdrückungsregeln	500	Die maximale Anzahl an gespeicherten Unterdrückungsregeln pro AWS Konto und Region. Sie können keine Kontingenterhöhung beantragen.
Ergebnisse Amazon EC2 EC2-Netzwerks	10.000	Die maximale Anzahl von Amazon EC2 EC2-Netzwerkergebnissen pro AWS Konto. Sie können keine Kontingenterhöhung beantragen.
Mitgliedskonten	10000	Die maximale Anzahl von Mitgliedskonten, die einem delegierten Administratorkonto von Amazon Inspector zugeordnet sind. Dieses Limit basiert auf AWS Organizations, siehe Kontingente für AWS Organizations.

Ressource	Standard	Kommentare
CIS-Scan-Konfigurationen	500	Die maximale Anzahl von CIS-Scan-Konfigurationen. Sie können keine Kontingenterhöhung beantragen.

Eine Liste der mit Amazon Inspector Classic verknüpften Kontingente finden Sie unter Amazon Inspector-Servicekontingente in der Allgemeine AWS-Referenz.

Eine Liste der mit Organizations verknüpften Kontingente finden Sie unter Dienstkontingente für Organizations in der Allgemeine AWS-Referenz.

Regionen und Endpunkte

Das agentenlose Scannen von Amazon Inspector für Amazon EC2 befindet sich in der Vorschauversion. Ihre Nutzung der Amazon EC2-Scanfunktion ohne Agenten unterliegt Abschnitt 2 der AWS Servicebedingungen („Betas und Vorschauen“).

Informationen darüber, AWS-Regionen wo Amazon Inspector verfügbar ist, finden Sie unter Amazon Inspector Inspector-Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Endpunkte für die Amazon Inspector Scan API

Die folgende Tabelle zeigt die regionalen Endpunkte, die beim Aufrufen der Amazon Inspector Scan API verwendet werden können. Wenn Sie die API verwenden, müssen Sie den Endpunkt und die entsprechende Region für die AWS Region angeben, in der Sie derzeit authentifiziert sind.

Die Namenskonvention für Amazon Inspector Scan-Endpunkte lautet`inspector-scan.`*`region`*`.amazonaws.com`. Wenn Sie beispielsweise authentifiziert sind, würden Sie den Endpunkt verwenden`us-west-2`, `inspector-scan.us-west-2.amazonaws.com` um die API aufzurufen. `inspector-scan`

Name der Region	Region	Endpunkt	Protokoll
USA Ost (Ohio)	us-east-2	inspector-scan.us-east-2.amazonaws.com inspector-scan-fips.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	inspector-scan.us-east-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protokoll
		inspector-scan-fips.us-east-1.amazonaws.com	
USA West (Nordkalifornien)	us-west-1	inspector-scan.us-west-1.amazonaws.com inspector-scan-fips.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	inspector-scan.us-west-2.amazonaws.com inspector-scan-fips.us-west-2.amazonaws.com	HTTPS
Afrika (Kapstadt)	af-south-1	inspector-scan.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	inspector-scan.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	inspector-scan.ap-southeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	inspector-scan.ap-south-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protokoll
Asien-Pazifik (Osaka)	ap-northeast-3	inspector-scan.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	inspector-scan.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	inspector-scan.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	inspector-scan.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	inspector-scan.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	inspector-scan.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	inspector-scan.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	inspector-scan.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	inspector-scan.eu-west-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protokoll
Europa (Mailand)	eu-south-1	inspector-scan.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	inspector-scan.eu-west-3.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	inspector-scan.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	inspector-scan.eu-central-2.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	inspector-scan.me-south-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	inspector-scan.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	Inspektor-Scan. us-gov-east-1.amazonaws.com inspector-scan-fips. us-gov-east-1. amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protokoll
AWS GovCloud (US-West)	us-gov-west-1	Inspektor-Scan. us-gov-west-1.amazonaws.com inspector-scan-fips. us-gov-west-1. amazonaws.com	HTTPS

Verfügbarkeit regionsspezifischer Feature

In diesem Abschnitt wird die Verfügbarkeit der Amazon Inspector Inspector-Funktionen von beschrieben AWS-Region.

Agentenloses EC2-Scannen für Amazon EC2 EC2-Regionen

Die folgende Tabelle zeigt, AWS-Regionen wo agentenloses Scannen für Amazon EC2 derzeit verfügbar ist.

Name der Region	Regionscode
USA Ost (Nord-Virginia)	us-east-1
USA West (Oregon)	us-west-2
Europa (Irland)	eu-west-1

Lambda-Code-Scanning-Regionen

Die folgende Tabelle zeigt, AWS-Regionen wo Lambda-Code-Scanning derzeit verfügbar ist.

Name der Region	Regionscode
USA Ost (Nord-Virginia)	us-east-1
USA West (Oregon)	us-west-2

Name der Region	Regionscode
USA Ost (Ohio)	us-east-2
Asien-Pazifik (Sydney)	ap-southeast-2
Asien-Pazifik (Tokio)	ap-northeast-1
Europa (Frankfurt)	eu-central-1
Europa (Irland)	eu-west-1
Europa (London)	eu-west-2
Europa (Stockholm)	eu-north-1
Asien-Pazifik (Singapur)	ap-southeast-1

AWS GovCloud (US) Regionen

Die neuesten Informationen finden Sie unter Amazon Inspector im AWS GovCloud (US) Benutzerhandbuch.

Dokumentenverlauf für das Amazon Inspector Inspector-Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version von Amazon Inspector beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Aktualisierte Funktionalität	Amazon Inspector aktualisiert die Aufbewahrungsfrist für abgeschlossene Ergebnisse von 30 Tagen auf 7 Tage. Weitere Informationen finden Sie unter Grundlegendes zu den Ergebnissen in Amazon Inspector.	12. Februar 2024
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicyRichtlinie eine neue Erklärung hinzugefügt. Die neue Anweisung ermöglicht es Amazon Inspector, CIS-Scans für Ihre Instance zu starten.	23. Januar 2024
Neue Richtlinie	Amazon Inspector hat eine neue Richtlinie, AmazonInspector2ManagedCisPolicyPolicy, hinzugefügt, die Sie als Teil eines Instance-Profils verwenden können, um CIS-Scans auf einer Instance zuzulassen.	23. Januar 2024

Neue Funktion	Amazon Inspector aktualisiert jetzt die Dauer des ECR-Rescans von Container-Images, wenn Sie sie abrufen. Informationen zum Ändern der Dauer des erneuten Scans auf der Grundlage von Push- oder Pull-Daten finden Sie unter Konfiguration der ECR-Rescan-Dauer.	23. Januar 2024
Neue Funktion	Amazon Inspector kann jetzt Center for Internet Security (CIS) -Scans auf EC2-Instances ausführen. Weitere Informationen finden Sie unter Amazon Inspector CIS-Scans.	23. Januar 2024
Neue Funktion	Amazon Inspector kann jetzt Container-Images in Ihren CI/CD-Pipelines scannen. Weitere Informationen finden Sie unter CI/CD-Integration mit Amazon Inspector.	30. November 2023
Neue Richtlinie	Amazon Inspector hat eine neue Richtlinie hinzugefügt, die es Amazon Inspector ermöglicht, Amazon EBS-Snapshots von Ihrer EC2-Instance für agentenloses Scannen zu scannen. Weitere Informationen zu dieser Richtlinie finden Sie unter Agentloses Scannen.	8. November 2023

Neue Funktion	Amazon Inspector unterstützt jetzt das Scannen unterstützter Linux-Amazon-EC2-Instances ohne SSM-Agenten durch agentenloses Scannen. Weitere Informationen finden Sie unter Agentloses Scannen.	8. November 2023
Neue unterstützte Ressourcen	Amazon Inspector unterstützt jetzt das Scannen von macOS Amazon EC2 EC2-Instances. Siehe Unterstützte Betriebssysteme: Amazon EC2 scannt nach unterstützten macOS-Versionen.	05. Oktober 2023
Neue Regionen	Amazon Inspector ist jetzt in Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Osaka) und Europa (Zürich) verfügbar.	29. September 2023
Neues Feature	Sie können jetzt EC2-Instances mithilfe von Ausschluss-Tags von Amazon Inspector-Scans ausschließen.	14. September 2023
Neues Feature	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, Netzwerkkonfigurationen von Amazon EC2 EC2-Instances zu scannen, die Teil der Elastic Load Balancing Balancing-Zielgruppen sind.	31. August 2023

Neues Feature	Amazon Inspector bietet jetzt Informationen zu Sicherheitslücken für gefundene Sicherheitslücken in Paketen.	31. Juli 2023
Aktualisierte Funktionalität	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Benutzern mit Lesezugriff ermöglichen, Software Bill of Materials (SBOM) für ihre Ressourcen zu exportieren.	29. Juni 2023
Neues Feature	Sie können jetzt SBOM für Ressourcen exportieren, die von Amazon Inspector gescannt werden.	13. Juni 2023
Neues Feature	Das Scannen von Lambda-Code ist jetzt allgemein verfügbar. Es wurden neue Funktionen hinzugefügt, mit denen Sie Code verschlüsseln können, der in Ihren Ergebnissen beim Lambda-Code-Scannen identifiziert wurde. Darüber hinaus bietet das Lambda-Code-Scannen jetzt Vorschläge zur Behebung von Neuschreibungen Ihres Codes.	13. Juni 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ReadOnlyAccessRichtlinie eine neue Erklärung hinzugefügt. Die neuen Anweisungen ermöglichen es Benutzern, die nur lesen können, Details zum Status und zu den Ergebnissen des Lambda-Code-Scans für ihr Konto abzurufen.	2. Mai 2023
Neues Feature	Amazon Inspector hat die Suche nach Sicherheitslücken in der Datenbank hinzugefügt, mit der Sie überprüfen können, ob Amazon Inspector ein bestimmtes CVE abdeckt.	1. Mai 2023
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicyRichtlinie neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, AWS CloudTrail serviceverknüpfte Kanäle in Ihrem Konto zu erstellen, wenn Sie Lambda-Scanning aktivieren. Dadurch kann Amazon Inspector CloudTrail Ereignisse in Ihrem Konto überwachen.	30. April 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2FullAccessRichtlinie eine neue Erklärung hinzugefügt. Die neue Erklärung ermöglicht es Benutzern, Details zu den beim Lambda-Code-Scannen gefundenen Sicherheitslücken abzurufen.	17. April 2023
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicyRichtlinie eine neue Erklärung hinzugefügt. Die neue Erklärung ermöglicht es Amazon Inspector, Informationen über die benutzerdefinierten Pfade, die Sie für Amazon EC2 Deep Inspection definiert haben, an Amazon EC2 Systems Manager zu senden.	17. April 2023
Neues Feature	Amazon Inspector bietet zusätzliche Unterstützung für Linux EC2-Instances in Form von Amazon Inspector Deep Inspection, die Ihre Instances auf Paketschwachstellen in Programmiersprachenpaketen für Anwendungen scannt.	17. April 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicyRichtlinie eine neue Erklärung hinzugefügt. Die neuen Anweisungen ermöglichen es Amazon Inspector, Scans des Entwicklercodes in AWS Lambda Funktionen anzufordern und Scandaten von Amazon CodeGuru Security zu empfangen. Darüber hinaus hat Amazon Inspector Berechtigungen zur Überprüfung von IAM-Richtlinien hinzugefügt. Amazon Inspector verwendet diese Informationen, um Lambda-Funktionen auf Code-Schwachstellen zu überprüfen.	28. Februar 2023
Neues Feature	Amazon Inspector bietet zusätzliche Unterstützung für Lambda-Funktionen in Form von Lambda-Code-Scans, die den Entwicklercode Ihrer Lambda-Funktionen auf Sicherheitslücken scannen.	28. Februar 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicyRichtlinie eine neue Erklärung hinzugefügt. Die neue Anweisung ermöglicht es Amazon Inspector, Informationen CloudWatch darüber abzurufen, wann eine AWS Lambda Funktion zuletzt aufgerufen wurde. verwendet diese Informationen, um Scans auf die Lambda-Funktionen in Ihrer Umgebung zu konzentrieren, die in den letzten 90 Tagen aktiv waren.	20. Februar 2023
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicyRichtlinie eine neue Erklärung hinzugefügt. Die neue Erklärung ermöglicht es Amazon Inspector, Informationen über Ihre AWS Lambda Funktionen abzurufen. Amazon Inspector verwendet diese Informationen, um Ihre Lambda-Funktionen auf Sicherheitslücken zu überprüfen.	28. November 2022
Neues Feature	Amazon Inspector bietet Unterstützung für AWS Lambda Scanfunktionen.	28. November 2022

Aktualisierter Inhalt	Es wurden Verfahren, Richtlinienbeispiele und Tipps für den Export von Ergebnisberichten aus Amazon Inspector in einen Amazon Simple Storage Service (Amazon S3) -Bucket hinzugefügt.	14. Oktober 2022
Neuer Inhalt	Es wurden Informationen zur Bewertung der Amazon Inspector Inspector-Abdeckung Ihrer AWS Umgebung mithilfe der Amazon Inspector Inspector-Konsole hinzugefügt. Die Informationen umfassen Beschreibungen der Statuswerte für einzelne Ressourcen in Ihrer Umgebung.	7. Oktober 2022

Neues Feature	Amazon Inspector bietet jetzt zusätzliche Informationen zur Behebung von Sicherheitslücken in Paketen. Zu den Suchdetails wurden neue Felder hinzugefügt. Die neuen Felder geben Aufschluss darüber, ob ein Update im Rahmen eines Paket-Updates verfügbar ist. Wenn ein Update verfügbar ist, werden im Abschnitt „Vorgeschlagene Abhilfemaßnahmen“ eines Ergebnisses die Befehle angezeigt, die Sie ausführen können, um das Problem zu beheben.	02. September 2022
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicyRichtlinie eine neue Aktion hinzugefügt. Die neue Aktion ermöglicht es Amazon Inspector, SSM-Zuordnungsausführungen zu beschreiben. Amazon Inspector hat außerdem zusätzlichen Ressourcenbereich hinzugefügt, damit Amazon Inspector SSM-Verknüpfungen mit `AmazonInspector2` eigenen SSM-Dokumenten erstellen, aktualisieren, löschen und starten kann.	31. August 2022

Neues Feature	Amazon Inspector unterstützt jetzt Scans für Windows Instances. Amazon Inspector kann jetzt SSM-verwaltete Instances scannen, auf denen unterstützte Windows Betriebssysteme ausgeführt werden. Scans von Windows Hosts werden vom Amazon Inspector SSM-Plugin durchgeführt, das über neue SSM-Verknüpfungen installiert und aufgerufen wird, die automatisch von Amazon Inspector erstellt werden.	31. August 2022
Aktualisierte Funktionalität	Amazon Inspector hat den Ressourcenbereich der AmazonInspector2ServiceRolePolicyRichtlinie aktualisiert, sodass Amazon Inspector Softwareinventar in anderen AWS Partitionen erfassen kann.	12. August 2022
Aktualisierte Funktionalität	In der AmazonInspector2ServiceRolePolicyRichtlinie hat Amazon Inspector den Ressourcenbereich der Aktionen neu strukturiert, sodass Amazon Inspector SSM-Verknüpfungen erstellen, löschen und aktualisieren kann.	10. August 2022

Neues Feature	Amazon Inspector unterstützt jetzt die Änderung Ihrer Einstellung für die Dauer Ihres automatisierten ECR-Rescans. Die Einstellung für die Dauer des automatischen erneuten Scans in Amazon ECR bestimmt, wie lange Amazon Inspector kontinuierlich Bilder überwacht, die in Repositorys übertragen werden. Wenn ein Bild älter als die Scandauer ist, scannt Amazon Inspector das Bild nicht mehr und schließt alle vorhandenen Ergebnisse dafür. Bei allen neuen Konten wird die Dauer des automatischen ECR-Wiederholungsscans automatisch auf „Lebenszeit“ gesetzt. Zuvor erstellte Konten hatten eine Dauer von 30 Tagen für den automatischen ECR-Rescan, aber Sie können jetzt zwischen einer Dauer von 30 Tagen, 180 Tagen oder lebenslangen Scans wählen.	25. Juni 2022

Neue Funktionalität	Amazon Inspector hat eine neue AWS verwaltete Richtlinie, die AmazonInspector2ReadOnlyAccessRichtlinie, hinzugefügt, um den schreibgeschützten Zugriff auf die Funktionen von Amazon Inspector zu ermöglichen.	21. Januar 2022
Allgemeine Verfügbarkeit	Dies ist die erste öffentliche Version des Amazon Inspector Inspector-Benutzerhandbuchs.	29. November 2021

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.