aws

Benutzerhandbuch

Amazon Inspector

Amazon Inspector: Benutzerhandbuch

Table of Contents

Was ist Amazon Inspector?

Amazon Inspector Inspector-Management ist ein Schwachstellen-Management-Service, der Ihre AWS Workloads kontinuierlich auf Softwareschwachstellen und unbeabsichtigte Netzwerkfreigabe durchsucht. Amazon Inspector erkennt und scannt automatisch laufende Amazon EC2 EC2-Instances, Container-Images in Amazon Elastic Container Registry (Amazon ECR) und sucht nach bekannten Softwareschwachstellen und AWS Lambda unbeabsichtigten Netzwerkangriffen.

Amazon Inspector erstellt eine Feststellung, wenn es eine Software-Schwachstelle oder ein Problem mit der Netzwerkkonfiguration entdeckt. Ein Ergebnis beschreibt die Sicherheitsanfälligkeit, identifiziert die betroffene Ressource, bewertet den Schweregrad der Sicherheitslücke und gibt Hinweise zur Behebung. Sie können die Ergebnisse mithilfe der Amazon Inspector Inspector-Konsole analysieren oder Ihre Ergebnisse über eine andere Konsole anzeigen und verarbeitenAWS-Services. Weitere Informationen finden Sie unter Erkenntnisse in Amazon Inspector verstehen.

Themen

Funktionen von Amazon Inspector

Zentrale Verwaltung mehrerer Amazon Inspector Inspector-Konten

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie Ihre Umgebung mithilfe von AWS Organizations zentral über ein einziges Konto 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, wenn 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 AWS Organisation.

Scannen Sie Ihre Umgebung kontinuierlich auf Schwachstellen und Netzwerkrisiken

Mit Amazon Inspector Inspector-Inspector-Zeichens müssen Sie die Bewertungs-Scans nicht manuell planen oder konfigurieren. Amazon Inspector erkennt Ihre berechtigten Ressourcen automatisch und beginnt mit dem Scannen. Amazon Inspector bewertet Ihre Umgebung während des gesamten Lebenszyklus Ihrer Ressourcen, indem es Ressourcen automatisch erneut scannt, um auf Änderungen zu reagieren, die zu einer neuen Sicherheitslücke führen könnten, wie z. B. die Installation eines neuen Pakets in einer EC2-Instance, die Installation eines Patches und die Veröffentlichung eines neuen Common Vulnerabilities and Exposures (CVE), das sich auf die Ressource auswirkt. Im Gegensatz zu herkömmlicher Sicherheitsscanning-Software hat Amazon Inspector nur minimale Auswirkungen auf die Leistung Ihrer Flotte.

Wenn Sicherheitslücken oder offene Netzwerkpfade identifiziert werden, erstellt Amazon Inspector einen Befund, den Sie untersuchen können. Das Ergebnis enthält umfassende Informationen zur Sicherheitsanfälligkeit, der betroffenen Ressource und Empfehlungen zur Behebung. Wenn Sie einen Befund angemessen korrigieren, erkennt Amazon Inspector die Korrektur automatisch und schließt den Befund ab.

Beurteilen Sie Sicherheitslücken mit dem Amazon Inspector Risk Score genau

Amazon Inspector sammelt im Rahmen von Scans Informationen über Ihre Umgebung und stellt Schweregradwerte bereit, die speziell auf Ihre Umgebung zugeschnitten sind. Amazon Inspector untersucht die Sicherheitsmetriken, aus denen sich der Basiswert der National Vulnerability Database (NVD) für eine Schwachstelle zusammensetzt, und passt sie an Ihre Computerumgebung an. Beispielsweise kann der Service den Amazon Inspector-Score eines Funds für eine Amazon EC2 EC2-Instance senken, wenn die Sicherheitsanfälligkeit über das Netzwerk ausgenutzt werden kann, von der Instance aus jedoch kein offener Netzwerkpfad zum Internet verfügbar ist. Dieser Score liegt im CVSS-Format vor und ist eine Modifikation des von NVD bereitgestellten Basiswerts für das Common Vulnerability Scoring System (CVSS).

Identifizieren Sie wichtige Ergebnisse mit dem Amazon Inspector-Dashboard

Das Amazon Inspector-Dashboard bietet einen umfassenden Überblick über Ergebnisse aus Ihrer gesamten Umgebung. Über das Dashboard können Sie die Details eines Befundes auf die Details auf unterer Ebene aufrufen. Das Dashboard enthält optimierte Informationen zur Scanabdeckung in Ihrer Umgebung, zu Ihren wichtigsten Ergebnissen und zu den Ressourcen mit den meisten Ergebnissen. Das Panel zur risikobasierten Problembehebung im Amazon Inspector-Dashboard enthält die Ergebnisse, die die meisten Instances und Images betreffen. Dieses Panel erleichtert es Ihnen, die Ergebnisse mit den größten Auswirkungen auf Ihre Umgebung zu identifizieren, die Einzelheiten der Ergebnisse zu überprüfen und Lösungsvorschläge zu überprüfen.

Verwalte deine 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 die Details der einzelnen Ergebnisse. Sie können die Ergebnisse nach Kategorie oder Schwachstellentyp gruppiert anzeigen. In jeder Ansicht können Sie Ihre Ergebnisse mithilfe von Filtern weiter anpassen. Sie können auch Filter verwenden, um Unterdrückungsregeln zu erstellen, die unerwünschte Ergebnisse vor Ihren Ansichten verbergen.

Sie können Filter und Unterdrückungsregeln verwenden, um Suchberichte 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 Ergebnisse EventBridge als Auffindungsereignisse bei Amazon. EventBridgeist ein serverloser Event-Bus-Service, der die Ergebnisdaten an Ziele, wie beispielsweise die AWS Lambda Funktionen und Amazon Simple Notification Service (Amazon SNS) -Themen. Mit EventBridge können Sie Ergebnisse im Rahmen Ihrer bestehenden Sicherheits- und Compliance-Workflows nahezu in Echtzeit überwachen und verarbeiten.

Wenn Sie es aktiviert haben AWS Security Hub, veröffentlicht Amazon Inspector die Ergebnisse auch im Security Hub. Security Hub ist ein Service, der einen umfassenden Überblick über Ihre Sicherheitslage in Ihrer AWS Umgebung liefert und Sie dabei unterstützt, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu überprüfen. Mit Security Hub können Sie Ihre Ergebnisse im Rahmen einer umfassenderen Analyse der Sicherheitslage Ihrer Organisation in einfacher verfolgen und verarbeitenAWS.

Auf Amazon Inspector

Amazon Inspector ist in den meisten verfügbarAWS-Regionen. Eine Liste der Regionen, in denen Amazon Inspector Inspector-Endpunkte und Kontingente verfügbar ist, finden Sie unter Amazon Inspector Inspector-Endpunkte und Kontingente in der Amazon Web Services General Reference. Weitere Informationen AWS-Regionen finden Sie unter Managing AWS-Regionen in der Amazon Web Services General Reference. In jeder Region können Sie Amazon Inspector Inspector-Inspector-Zeichens wie folgt nutzen:

AWSManagement-Konsole

AWS Management ConsoleEs ist eine browserbasierte Schnittstelle, mit der Sie -Ressourcen erstellen und verwalten AWS 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 über die Amazon Inspector Inspector-Konsole ausführen.

AWSBefehlszeilen-Tools

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

AWS bietet zwei Sätze an Befehlszeilen-Tools: AWS Command Line Interface (AWS CLI) und AWS Tools for PowerShell. Weitere Informationen zur Installation und Verwendung der AWS CLI finden Sie AWSim -CLI-Benutzerhandbuch. Weitere Informationen zur Installation und Verwendung der Tools for PowerShell finden Sie im AWS Tools for PowerShell-Benutzerhandbuch.

AWS-SDKs

AWSstellt SDKs zur Verfügung, die aus Bibliotheken und Beispiel-Codes für verschiedene Programmiersprachen und Plattformen bestehen, einschließlich Java, Go, Python, C++ und .NET. Die SDKs bieten bequemen, programmatischen Zugriff auf Amazon Inspector und andere. AWS-Services Sie behandeln auch Aufgaben wie das kryptografische Signieren, die Fehlerbehandlung und das Erstellen von Anforderungen. Informationen zur Installation und Verwendung der AWS SDKs finden Sie unter Tools, auf AWS denen Sie aufbauen können.

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 Befehlszeilen-Tools und -SDKs muss Ihre Anwendung Details auf unterer Ebene behandeln, z. B. die Generierung eines Hash-Zeichens zum Signieren einer Anforderung.

Erste Schritte mit Amazon Inspector

Dieses Tutorial bietet eine praktische Einführung in Amazon Inspector .

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

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

> **Note**
>
> In diesem Tutorial führen Sie Aufgaben in Ihrem aktuellen aus 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 Schwachstellenverwaltungsservice, der Ihre Amazon EC2-Instances, Amazon-ECR-Container-Images und - AWS Lambda Funktionen kontinuierlich auf Softwareschwachstellen und unbeabsichtigte Netzwerkrisiken scannt.

Beachten Sie Folgendes, bevor Sie Amazon Inspector aktivieren:

- Amazon Inspector ist ein regionaler Service und die Daten werden in der gespeichert AWS-Region , in der Sie den Service verwenden. Alle Konfigurationsverfahren, die Sie in diesem Tutorial durchführen, müssen in jedem wiederholt werden AWS-Region , das Sie mit Amazon Inspector überwachen möchten.
- Amazon Inspector bietet Ihnen die Flexibilität, Amazon EC2-Instance, Amazon-ECR-Container-Image und AWS Lambda Funktionsscan zu aktivieren. Sie können die Scantypen auf der

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

- Amazon Inspector kann Common Vulnerabilities and Exposures (CVE)-Daten 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, aber Sie müssen ihn möglicherweise manuell aktivieren. Unabhängig vom Status des SSM-Agenten werden alle Ihre EC2-Instances auf Probleme mit der Netzwerkrisiken gescannt. Weitere Informationen zum Konfigurieren von Scans für Amazon EC2 finden Sie unter Scannen von Amazon EC2. Das Scannen von Amazon ECR und AWS Lambda Funktionen erfordert nicht die Verwendung eines Agenten.
- Eine IAM-Benutzeridentität mit Administratorberechtigungen in einem 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 zum Verwalten von Amazon Inspector erforderlich sind. Informationen zu den erforderlichen Berechtigungen zum Aktivieren von Amazon Inspector finden Sie unter AWS Von verwaltete Richtlinie: AmazonInspector2FullAccess.
- Wenn Sie Amazon Inspector zum ersten Mal in einer beliebigen Region aktivieren, wird global eine serviceverknüpfte Rolle für Ihr Konto namens erstelltAWSServiceRoleForAmazonInspector2. Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es Amazon Inspector ermöglichen, Softwarepaketdetails zu sammeln und Amazon-VPC-Konfigurationen zu analysieren, um Schwachstellen zu generieren. 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: Aktivieren von Amazon Inspector

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

Wenn Sie Amazon Inspector für mehrere Konten in 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-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie Get Started.
3. Wählen Sie Amazon Inspector aktivieren aus.

Wenn Sie Amazon Inspector in einem eigenständigen Konto aktivieren, werden alle Scantypen standardmäßig aktiviert. Sie können aktivierte Scantypen auf der Kontoverwaltungsseite in der Amazon Inspector-Konsole oder mithilfe von Amazon Inspector-APIs verwalten. Nachdem Amazon Inspector aktiviert wurde, erkennt es automatisch alle berechtigten Ressourcen und beginnt mit dem Scannen. Lesen Sie die folgenden Scantypinformationen, um zu verstehen, welche Ressourcen standardmäßig berechtigt sind:

Amazon EC2-Scan

Um Common Vulnerabilities and Exposures (CVE)-Daten für Ihre EC2-Instance bereitzustellen, verlangt Amazon Inspector, dass der AWS Systems Manager (SSM)-Agent installiert und aktiviert wird. Dieser Agent ist auf vielen EC2-Instances vorinstalliert, aber Sie müssen ihn möglicherweise manuell aktivieren. Unabhängig vom Status des SSM-Agenten werden alle Ihre EC2-Instances auf Probleme mit der Netzwerkrisiken gescannt. Weitere Informationen zum Konfigurieren von Scans für Amazon EC2 finden Sie unter Scannen von Amazon EC2-Instances mit Amazon Inspector.

Amazon-ECR-Scan

Wenn Sie das Amazon-ECR-Scannen aktivieren, konvertiert Amazon Inspector alle Container-Repositorys in Ihrer privaten Registrierung, die für das von Amazon ECR bereitgestellte Standard-Basisscan konfiguriert sind, mit kontinuierlichem Scannen in Erweitertes Scannen. Sie können diese Einstellung optional auch so konfigurieren, dass nur per Push gescannt wird oder ausgewählte Repositorys über Einschlussregeln gescannt werden. Alle Images, 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 zum Konfigurieren von Scans für Amazon ECR finden Sie unter Scannen von Amazon-ECR-Container-Images mit Amazon Inspector.

AWS Lambda Scannen von -Funktionen

Wenn Sie das Scannen von AWS Lambda Funktionen aktivieren, erkennt Amazon Inspector die Lambda-Funktionen in Ihrem Konto und beginnt sofort mit dem Scannen auf Schwachstellen. Amazon Inspector scannt neue Lambda-Funktionen und -Ebenen, 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 Ebenen des Scannens von Lambda-Funktionen. Wenn Sie Amazon Inspector zum ersten Mal aktivieren, ist standardmäßig das Lambda-Standardscannen aktiviert, das Paketabhängigkeiten in Ihren Funktionen scannt. Sie können zusätzlich das Scannen von Lambda-Code aktivieren, um den Entwicklercode in Ihren Funktionen auf Code-Schwachstellen zu scannen. Weitere Informationen zum Konfigurieren des Scannens von Lambda-Funktionen finden Sie unter Scannen von AWS Lambda Funktionen mit Amazon Inspector.

Multi-account environment

Important

Um diese Schritte auszuführen, müssen Sie sich in derselben Organisation wie alle Konten befinden, die Sie verwalten möchten, und Zugriff auf das AWS Organizations Verwaltungskonto haben, um einen Administrator für Amazon Inspector innerhalb Ihrer Organisation zu delegieren. Möglicherweise sind zusätzliche Berechtigungen erforderlich, um einen Administrator zu delegieren. Weitere Informationen finden Sie unter Erforderliche Berechtigungen zum designieren eines delegierten Administrators.

Note

Um Amazon Inspector für mehrere Konten in mehreren Regionen programmgesteuert zu aktivieren, können Sie ein von Amazon Inspector entwickeltes Shell-Skript verwenden. Weitere Informationen zur Verwendung dieses Skripts finden Sie unter Inspector2-enablement-with-cli auf GitHub.

Delegieren eines Administrators für Amazon Inspector

1. Melden Sie sich beim AWS Organizations Verwaltungskonto an.

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

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

Hinzufügen von Mitgliedskonten

Als delegierter Administrator können Sie das Scannen für jedes Mitglied aktivieren, das dem Verwaltungskonto von Organizations zugeordnet ist. Dieser Workflow aktiviert alle Scantypen für alle Mitgliedskonten. Mitglieder können Amazon Inspector jedoch auch für ihre eigenen Konten aktivieren oder Scans nach einem 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-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
3. Wählen Sie im Navigationsbereich Kontoverwaltung aus. In der Tabelle Konten werden alle Mitgliedskonten angezeigt, die dem Verwaltungskonto von Organizations zugeordnet sind.
4. Auf der Seite Kontoverwaltung können Sie im oberen Banner die Option Scan für alle Konten aktivieren auswählen, um EC2-Instances, ECR-Container-Images und AWS Lambda Funktionsscan für alle Konten in Ihrer Organisation zu aktivieren. Alternativ können Sie die Konten auswählen, die Sie als Mitglieder hinzufügen möchten, 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 Scantypen aus, die Sie einbeziehen möchten, um diese Scans für alle neuen Mitgliedskonten zu aktivieren, die Ihrer Organisation hinzugefügt werden.

Amazon Inspector bietet derzeit Scans nach EC2-Instances, ECR-Container-Images und - AWS Lambda Funktionen an. Nachdem Sie Amazon Inspector aktiviert haben, beginnt es automatisch mit der Erkennung und dem Scannen aller berechtigten Ressourcen. Lesen Sie die folgenden Scantypinformationen, um zu verstehen, welche Ressourcen standardmäßig berechtigt sind:

Amazon EC2-Scan

Um CVE-Schwachstellendaten für Ihre EC2-Instances bereitzustellen, verlangt Amazon Inspector, dass der AWS Systems Manager (SSM)-Agent installiert und aktiviert wird. Dieser Agent ist auf vielen EC2-Instances vorinstalliert, aber Sie müssen ihn möglicherweise manuell aktivieren. Unabhängig vom Status des SSM-Agenten werden alle Ihre EC2-Instances auf Probleme mit der Netzwerkrisiken gescannt. Weitere Informationen zum Konfigurieren von Scans für Amazon EC2 finden Sie unter Scannen von Amazon EC2-Instances mit Amazon Inspector.

Amazon-ECR-Scan

Wenn Sie das Amazon-ECR-Scannen aktivieren, konvertiert Amazon Inspector alle Container-Repositorys in Ihrer privaten Registrierung, die für das von Amazon ECR bereitgestellte Standard-Basisscan konfiguriert sind, mit kontinuierlichem Scannen in Erweitertes Scannen. Sie können diese Einstellung optional auch so konfigurieren, dass nur per Push gescannt wird oder ausgewählte Repositorys über Einschlussregeln gescannt werden. Alle Images, die innerhalb der letzten 30 Tage übertragen wurden, sind für das Scannen während der Lebensdauer geplant. Diese Amazon-ECR-Scaneinstellung kann vom delegierten Administrator jederzeit geändert werden. Weitere Informationen zum Konfigurieren von Scans für Amazon ECR finden Sie unter Scannen von Amazon-ECR-Container-Images mit Amazon Inspector.

AWS Lambda Scannen von -Funktionen

Wenn Sie das Scannen von AWS Lambda Funktionen aktivieren, erkennt Amazon Inspector die Lambda-Funktionen in Ihrem Konto und beginnt sofort mit dem Scannen auf Schwachstellen. Amazon Inspector scannt neue Lambda-Funktionen und -Ebenen, wenn sie bereitgestellt werden, und scannt sie erneut, wenn sie aktualisiert werden oder wenn neue Common Vulnerabilities and Exposures (CVEs) veröffentlicht werden. Weitere Informationen zum Konfigurieren des Scannens von Lambda-Funktionen finden Sie unter Scannen von AWS Lambda Funktionen mit Amazon Inspector.

Schritt 2: Anzeigen von Amazon Inspector-Ergebnissen

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

Die Amazon 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 Erkenntnisse die Details einer bestimmten Erkenntnis anzeigen können.

In diesem Schritt untersuchen Sie die Details eines Ergebnisses mithilfe der Tabelle Erkenntnisse und des Ergebnisse-Dashboards. Weitere Informationen zum Amazon Inspector-Dashboard finden Sie unter Erklärung des -Dashboards.

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

1. Öffnen Sie die Amazon 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-Konsole mit weiteren Details zu diesem Element zu navigieren.
3. Wählen Sie im Navigationsbereich Erkenntnisse aus.
4. Standardmäßig wird die Registerkarte Alle Ergebnisse angezeigt, auf der alle EC2-Instances, ECR-Container-Images und AWS Lambda Funktionsergebnisse für Ihre Umgebung angezeigt werden.
5. Wählen Sie in der Liste Erkenntnis einen Erkenntnisnamen in der Spalte Titel aus, um den Detailbereich für diese Erkenntnis zu öffnen. Alle Ergebnisse verfügen über eine Registerkarte mit den Erkenntnisdetails. Sie können wie folgt mit der Registerkarte Erkenntnisdetails interagieren:

   - Weitere Informationen zur Schwachstelle finden Sie unter dem Link im Abschnitt Details zur Schwachstelle, um die Dokumentation zu dieser Schwachstelle zu öffnen.
   - Um Ihre Ressource weiter zu untersuchen, folgen Sie dem Ressourcen-ID-Link im Abschnitt Betroffene Ressource, um die Servicekonsole für die betroffene Ressource zu öffnen.

   Die Ergebnisse des Paketschwachstellentyps verfügen auch über eine Registerkarte Inspector Score und Schwachstelleninformationen, auf der erklärt wird, wie der Amazon Inspector-Score

für diese Erkenntnis berechnet wurde, und Informationen zu Common Vulnerability and Exploits (CVE), die mit der Erkenntnis verbunden sind. Weitere Informationen zu Suchtypen finden Sie unter Typen in Amazon Inspector finden.

Das Amazon Inspector-Dashboard verstehen

Das Amazon Inspector-Dashboard bietet einen Überblick über aggregierte Statistiken für Ihre AWS Ressourcen in der aktuellen AWS Region. Diese Statistiken beinhalten wichtige Kennzahlen für die Ressourcenabdeckung und aktive Sicherheitslücken. Das Dashboard zeigt auch Gruppen aggregierter 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. Um eine eingehendere Analyse durchzuführen, können Sie sich die unterstützenden Daten für Dashboard-Elemente ansehen.

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

Anzeigen des -Dashboards

Das Dashboard zeigt einen Überblick über Ihre Umgebungsabdeckung und wichtige Ergebnisse.

Um das Dashboard anzuzeigen:

1. Öffnen Sie die Amazon-Inspector-Konsole https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Sie können folgendermaßen mit dem Dashboard interagieren:

   - Das Dashboard wird automatisch alle fünf Minuten aktualisiert. Sie können die Daten jedoch manuell aktualisieren, indem Sie in der oberen rechten Ecke der Seite auf das Aktualisierungssymbol klicken.
   - 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 Daten zu aktiven Ergebnissen, anhand derer Sie die aktuelle Sicherheitslage Ihrer AWS Ressourcen nachvollziehen könnenAWS-Region.

Berichterstattung über die Umwelt

Der Abschnitt „Umweltabdeckung“ enthält Statistiken zu den Ressourcen, die von Amazon Inspector gescannt wurden. In diesem Abschnitt sehen Sie die Anzahl und den Prozentsatz der Amazon EC2-Instances, Amazon ECR-Images und AWS Lambda Funktionen, die von Amazon Inspector gescannt wurden. Wenn Sie AWS Organizations als delegierter Administrator von Amazon Inspector mehrere Konten verwalten, sehen Sie auch die Gesamtzahl der Organisationskonten, die Anzahl der Konten, bei denen Amazon Inspector aktiviert ist, und den daraus resultierenden Deckungsprozentsatz für die Organisation. Sie können diesen Abschnitt auch verwenden, um festzustellen, welche Ressourcen nicht von Amazon Inspector abgedeckt werden. Diese Ressourcen können Sicherheitslücken enthalten, die ausgenutzt werden könnten, um Ihr Unternehmen einem Risiko auszusetzen. 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 ausgewählte Gruppierung. Auf der Kontoverwaltungsseite finden Sie Informationen 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 Anzahlen pro Ressource und Bewertungstyp angezeigt. Weitere Informationen zu

wichtigen Ergebnissen und zur Bestimmung der Wichtigkeit durch Amazon Inspector finden Sie unterErkenntnisse in Amazon Inspector verstehen.

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

Die folgenden kritischen Ergebnisgruppen sind verfügbar:

- Ergebnisse mit ECR-Container-Images
- Amazon EC2 EC2-Ergebnisse
- Ergebnisse zur Netzwerkerreichbarkeit
- AWS LambdaFunktionsergebnisse

Risikobasierte Abhilfemaßnahmen

Im Abschnitt Risikobasierte Abhilfemaßnahmen werden die fünf wichtigsten Softwarepakete mit kritischen Sicherheitslücken aufgeführt, die die meisten Ressourcen in Ihrer Umgebung betreffen. 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 einzusehen.

Konten mit den kritischsten Ergebnissen

Im Abschnitt Konten mit den kritischsten Ergebnissen werden die fünf wichtigsten 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

Der Abschnitt Elastic Container Registry (ECR) Repositories mit den kritischsten Ergebnissen zeigt die fünf wichtigsten Amazon ECR-Repositorys in Ihrer Umgebung mit den wichtigsten Container-Image-Ergebnissen. 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 Namen des Repositorys, um weitere Informationen über das betroffene Repository zu erhalten.

Container-Images mit den wichtigsten Ergebnissen

Der Abschnitt Container-Images mit den kritischsten Ergebnissen zeigt die fünf wichtigsten Container-Images in Ihrer Umgebung mit den kritischsten Ergebnissen. In der Ansicht werden Image-Tag-Daten, Repository-Name, Image-Digest, AWS Konto-ID, Anzahl der kritischen Sicherheitslücken und Gesamtzahl der Sicherheitslücken angezeigt. Diese Ansicht hilft Anwendungsbesitzern zu 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 wichtigsten Amazon EC2 EC2-Instances mit den kritischsten Ergebnissen. Die Ansicht zeigt die Instance-ID, die AWS Konto-ID, die Amazon Machine Image (AMI) -Kennung, die Anzahl der kritischen Sicherheitslücken und die Gesamtzahl der Sicherheitslücken. Diese Ansicht hilft Infrastrukturbesitzern zu erkennen, welche Instanzen 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

Der Abschnitt Amazon Machine Images (AMIs) mit den kritischsten Ergebnissen zeigt die fünf wichtigsten AMIs in Ihrer Umgebung mit den kritischsten Ergebnissen. 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. Diese Ansicht hilft Infrastrukturbesitzern zu erkennen, welche AMIs möglicherweise neu erstellt werden müssen.

Wählen Sie Betroffene Instances aus, um weitere Informationen zu den Instances zu erhalten, die vom betroffenen AMI aus gestartet wurden.

AWS LambdaFunktionen mit den kritischsten Ergebnissen

Der Abschnitt AWS LambdaFunktionen mit den kritischsten Ergebnissen enthält die fünf wichtigsten Lambda-Funktionen in Ihrer Umgebung mit den kritischsten Ergebnissen. Die Ansicht

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

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

Erkenntnisse in Amazon Inspector verstehen

Eine Erkenntnis ist ein detaillierter Bericht über eine Schwachstelle, die sich auf eine Ihrer AWS Ressourcen auswirkt. Die Erkenntnisse werden nach erkannten Schwachstellen benannt und stellen Schweregrade, Informationen zu betroffenen Ressourcen und Details zur Behebung gemeldeter Schwachstellen bereit.

Amazon Inspector generiert ein Ergebnis, wenn es eine Schwachstelle in einer Amazon EC2-Instance, ein Container-Image in einem Amazon-ECR-Repository oder eine - AWS Lambda Funktion erkennt. Amazon Inspector scannt kontinuierlich Ihre Datenverarbeitungsumgebung und speichert alle Ihre aktiven Erkenntnisse, bis Sie sie beheben.

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 verbundenen Erkenntnisse nach 30 Tagen.

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

Die Ergebnisse sind in einen der folgenden Zustände unterteilt:

Aktiv

Amazon Inspector identifiziert Erkenntnisse, die nicht als Aktiv behoben wurden.

Unterdrückt

Amazon Inspector identifiziert Erkenntnisse, die einer oder mehreren Unterdrückungsregeln unterliegen, als Unterdrückt. Unterdrückte Ergebnisse finden Sie in der Liste Unterdrückte Ergebnisse. Weitere Informationen finden Sie unter Unterdrücken von Amazon Inspector-Ergebnissen mit Unterdrückungsregeln.

Closed (Abgeschlossen)

Nachdem Sie eine Schwachstelle behoben haben, erkennt Amazon Inspector dies automatisch und ändert den Status der Erkenntnis in Geschlossen. Geschlossene Ergebnisse werden nach 7 Tagen gelöscht.

Themen

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 verwendenAmazon Inspector Schwachstellendatenbanksuche, 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 Codescan von Amazon Inspector Lambda aktiviert haben.

Codefragmente, die im Zusammenhang mit einer Code-Schwachstelle erkannt wurden, werden vom Service gespeichert. CodeGuru Standardmäßig wird zur Verschlüsselung Ihres Codes ein AWSeigener 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 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 von Amazon Inspector-Ergebnissen

Die Verfahren in diesem Abschnitt beschreiben, wie Sie Ergebnisse in Amazon Inspector über die Amazon Inspector-Konsole und API finden und anzeigen. Die Erkenntnisdetails variieren je nach Erkenntnistyp, Schwachstellentyp und betroffenen Ressourcen. Weitere Informationen finden Sie unter Details zu den Erkenntnissen in Amazon Inspector .

Console

So zeigen Sie Ergebnisse in der Konsole an

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

Erkenntnisse können Sie ein Ergebnis auswählen, indem Sie den Namen des Ergebnisses in der Spalte Titel auswählen.

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

   - Nach Schwachstelle
   - Nach Instance

   > **Note**
   >
   > Erkenntnisse, die nach Instances gruppiert sind, enthalten keine Informationen zur Netzwerkverfügbarkeit.

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

API

Führen Sie die ListFindings -API-Operation aus. In der Anforderung können Sie angeben, `filterCriteria` um bestimmte Ergebnisse zurückzugeben.

Details zu den Erkenntnissen in Amazon Inspector

In der Amazon Inspector-Konsole können Sie Details zu den einzelnen Erkenntnissen anzeigen. Die Erkenntnisdetails variieren je nach Erkenntnistyp.

So zeigen Sie die Details für ein Ergebnis an

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home
2. Wählen Sie die Region aus, in der die Ergebnisse angezeigt werden sollen.
3. Wählen Sie im Navigationsbereich Erkenntnisse aus, um die Liste der Erkenntnisse anzuzeigen
4. (Optional) Verwenden Sie die Filterleiste, um ein bestimmtes Ergebnis auszuwählen. Weitere Informationen finden Sie unter Filtern von Amazon Inspector-Ergebnissen.
5. Wählen Sie eine Erkenntnis aus, um ihren Detailbereich anzuzeigen.

Der Bereich Erkenntnisdetails enthält die grundlegenden identifizierenden Features der Erkenntnis. Dazu gehören der Titel der Erkenntnis sowie eine grundlegende Beschreibung der identifizierten Schwachstelle, Vorschläge zur Behebung und ein Schweregrad. Weitere Informationen zur Punktzahl finden Sie unter Schweregrade für Erkenntnisse von Amazon Inspector .

Die für eine Erkenntnis verfügbaren Details variieren je nach Erkenntnistyp und der betroffenen Ressource .

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

Der Erkenntnistyp bestimmt die für die Erkenntnis verfügbaren Informationen zur Behebung und Schwachstelleninformation. Je nach Erkenntnistyp sind unterschiedliche Erkenntnisdetails verfügbar.

Paketschwachstelle

Die Ergebnisse der Paketschwachstelle sind für EC2-Instances, ECR-Container-Images und Lambda-Funktionen verfügbar. Weitere Informationen finden Sie unter Sicherheitslücke im Package.

Zu den Erkenntnissen zur Paketschwachstelle gehören auch Amazon Inspector-Score und Schwachstelleninformationen.

Dieser Erkenntnistyp hat die folgenden Details:

- Korrektur verfügbar – Gibt an, ob die Schwachstelle in einer neueren Version der betroffenen Pakete behoben ist. 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 ein oder mehrere (aber nicht alle) der betroffenen Pakete eine feste Version haben.
- Ausnutzen verfügbar – Zeigt an, dass die Schwachstelle einen bekannten Ausnutzen aufweist.
  - `YES`, was bedeutet, dass die in Ihrer -Umgebung erkannte Schwachstelle einen bekannten Exploit hat. Amazon Inspector hat keinen Einblick in die Verwendung von Exploits in einer Umgebung.
  - `NO`, was bedeutet, dass diese Schwachstelle keinen bekannten Exploit hat.
- Betroffene Pakete – Listet jedes Paket auf, das in der Erkenntnis als anfällig identifiziert wurde, sowie die Details jedes Pakets:

- Dateipfad – Die EBS-Volume-ID und Partitionsnummer, die einem Ergebnis zugeordnet sind. Dieses Feld ist in den Ergebnissen für EC2-Instances vorhanden, die mit gescannt wurdenAgentless-Scan.
- Installierte Version/Fixierte Version – Die Versionsnummer des aktuell installierten Pakets, für das eine Schwachstelle erkannt wurde. Vergleichen Sie die installierte Versionsnummer mit dem Wert nach dem Schrägstrich (/). Der zweite Wert ist die Versionsnummer des Pakets, das die erkannte Schwachstelle behebt, wie sie von der Common Vulnerabilities and Exposures (CVEs) oder der mit der Erkenntnis verbundenen Beratung bereitgestellt wird. Wenn die Schwachstelle in mehreren Versionen behoben wurde, listet dieses Feld die neueste Version auf, die den Fix enthält. Wenn kein Fix verfügbar ist, ist dieser Wert `None available`.

  > **Note**
  >
  > Wenn eine Erkenntnis erkannt wurde, bevor Amazon Inspector mit der Aufnahme dieses Felds in Erkenntnisse begann, ist der Wert für dieses Feld leer. Möglicherweise ist jedoch ein Fix verfügbar.

- Paketmanager – Der Paketmanager, der zur Konfiguration dieses Pakets verwendet wurde.
- Abhilfe – Wenn ein Fix 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**
  >
  > Korrekturbefehle werden aus Anbieterdaten-Feeds bereitgestellt und können je nach Systemkonfiguration variieren. Spezifischere Anleitungen finden Sie in den Erkenntnisreferenzen oder in der Betriebssystemdokumentation.

- Details zur Schwachstellen – bietet einen Link zur bevorzugten Quelle von Amazon Inspector für das in der Erkenntnis identifizierte CVE, z. B. National Vulnerability Database (NVD), REDHAT oder einen anderen Betriebssystemanbieter. Darüber hinaus finden Sie die Schweregrade für die Erkenntnis. Weitere Informationen zu Schweregraden wie finden Sie unter Schweregrade für Erkenntnisse von Amazon Inspector . Die folgenden Punktzahlen sind enthalten, einschließlich der jeweiligen Bewertungsvektoren:
  - EPSS-Score
  - Inspector-Score

- CVSS 3.1 von Amazon CVE
- CVSS 3.1 von NVD
- CVSS 2.0 von NVD (falls zutreffend, für ältere CVEs)

- Verwandte Schwachstellen – Gibt andere Schwachstellen im Zusammenhang mit der Erkenntnis an. In der Regel handelt es sich dabei um andere CVEs, die sich auf dieselbe Paketversion auswirken, oder um andere CVEs innerhalb derselben Gruppe wie das Ergebnis-CVE, wie vom Anbieter festgelegt.

Code-Schwachstelle

Code-Schwachstellenergebnisse sind nur für Lambda-Funktionen verfügbar. Weitere Informationen finden Sie unter Sicherheitslücke im Code. Dieser Erkenntnistyp hat die folgenden Details:

- Behebung verfügbar – Bei Code-Schwachstellen ist dieser Wert immer `YES`.
- Name des Detectors – Der Name des CodeGuru Detectors, der zur Erkennung der Code-Schwachstelle verwendet wurde. Eine Liste möglicher Erkennungen finden Sie in der CodeGuru Detector Library.
- Detector-Tags – Die CodeGuru dem Detektor zugeordneten Tags CodeGuru verwenden Tags, um Erkennungen zu kategorisieren.
- Relevante CWE – IDs der Common Weakness Enumeration (CWE), die der Code-Schwachstelle zugeordnet sind.
- Dateipfad – Der Dateispeicherort der Code-Schwachstelle.
- Speicherort der Schwachstellen – Bei Schwachstellen im Code für Lambda-Codescan zeigt dieses Feld genau die Codezeilen an, in denen Amazon Inspector die Schwachstelle gefunden hat.
- Vorgeschlagene Behebung – Dies schlägt vor, wie der Code bearbeitet werden kann, um das Ergebnis zu beheben.

Erreichbarkeit des Netzwerks

Ergebnisse zur Netzwerkerreichbarkeit sind nur für EC2-Instances verfügbar. Weitere Informationen finden Sie unter Erreichbarkeit über das Netzwerk. Dieser Erkenntnistyp 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.
- Abhilfe – Empfohlen eine Methode zum Schließen des offenen Netzwerkpfads.

Amazon Inspector-Score und Schwachstelleninformationen

Wenn Sie in der Amazon Inspector-Konsole eine Erkenntnis auswählen, können Sie die Registerkarte Inspector-Score und Schwachstelleninformationen anzeigen, auf der die Bewertungsdetails für eine Paketschwachstelle sowie Details zu Schwachstelleninformationen angezeigt werden. Diese Details stehen nur für Sicherheitslücke im Package Erkenntnisse zur Verfügung.

Amazon Inspector-Score

Der Amazon Inspector-Score ist ein kontextualisierter Score, den Amazon Inspector für jede EC2-Instance-Erkenntnis erstellt. Der Amazon Inspector-Score wird durch die Korrelation der Basis-CVSS-v3.1-Score-Informationen mit Informationen bestimmt, die während Scans von Ihrer Datenverarbeitungsumgebung gesammelt wurden, z. B. Ergebnisse der Netzwerkerreichbarkeit und Auslastbarkeitsdaten. Beispielsweise kann der Amazon Inspector-Score einer Erkenntnis niedriger sein als der Basiswert, wenn die Schwachstelle über das Netzwerk ausgenutzt werden kann, Amazon Inspector jedoch feststellt, dass kein offener Netzwerkpfad zur anfälligen Instance über das Internet verfügbar ist.

Der Basiswert für eine Erkenntnis ist der vom Anbieter bereitgestellte CVSS v3.1-Basiswert. RHEL-, Debian- oder Amazon-Anbieter-Basiswerte werden für andere Anbieter oder Fälle unterstützt, in denen der Anbieter keinen Wert angegeben hat, verwendet Amazon Inspector den Basiswert aus der National Vulnerability Database (NVD). Amazon Inspector verwendet den Rechner des Common Vulnerability Scoring System Version 3.1, um den Wert zu berechnen. Sie können die Quelle des Basiswerts eines einzelnen Ergebnisses in den Details des Ergebnisses unter Schwachstellendetails, als Schwachstellenquelle (oder packageVulnerabilityDetails.source im Ergebnis-JSON) sehen.

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

Details zur Amazon Inspector-Punktzahl

Wenn Sie die Detailseite eines Ergebnisses öffnen, können Sie die Registerkarte Inspector score und Schwachstelleninformationen auswählen. In diesem Bereich wird der Unterschied zwischen dem Basiswert und dem Inspector-Score angezeigt. In diesem Abschnitt wird erläutert, wie Amazon Inspector den Schweregrad basierend auf einer Kombination aus dem Amazon Inspector-Wert und dem Anbieterwert für das Softwarepaket zugewiesen hat. Wenn sich die Werte unterscheiden, zeigt dieser Bereich eine Erklärung der Gründe.

Im Abschnitt CVSS-Score-Metriken finden Sie eine Tabelle mit Vergleichen zwischen den CVSS-Basisscore-Metriken und dem Inspector-Score . Die verglichenen Metriken sind die Basismetriken, die im von verwalteten CVSS-Spezifikationsdokument definiert sindfirst.org. Im Folgenden finden Sie eine Zusammenfassung der Basismetriken:

Angriffsvektor

Der Kontext, mit dem eine Schwachstelle ausgenutzt werden kann. Für Amazon Inspector-Erkenntnisse kann dies Netzwerk, Gleichzeitiges Netzwerk oder Lokal sein.

Angriffskomplexität

Dies beschreibt den Grad der Schwierigkeiten, die ein Angreifer beim Ausnutzen der Schwachstelle haben wird. Ein niedriger Wert bedeutet, dass der Angreifer nur wenige oder keine zusätzlichen Bedingungen erfüllen muss, um die Schwachstelle auszunutzen. Eine hohe Punktzahl bedeutet, dass ein Angreifer einen beträchtlichen Aufwand investieren muss, um einen erfolgreichen Angriff mit dieser Schwachstelle durchzuführen.

Berechtigung erforderlich

Dies beschreibt die Berechtigungsstufe, die ein Angreifer benötigt, um eine Schwachstelle auszunutzen.

Benutzerinteraktion

Diese Metrik gibt an, ob ein erfolgreicher Angriff, der diese Schwachstelle verwendet, einen menschlichen Benutzer erfordert, außer den Angreifer.

Scope

Dies gibt an, ob sich eine Schwachstelle in einer anfälligen Komponente auf Ressourcen in Komponenten auswirkt, die über den Sicherheitsbereich der anfälligen Komponente hinausgehen. Wenn dieser Wert Unverändert lautet, sind die betroffene Ressource und die betroffene Ressource identisch. Wenn dieser Wert Geändert lautet, kann die anfällige

Komponente ausgenutzt werden, um sich auf Ressourcen auszuwirken, die von verschiedenen Sicherheitsstellen verwaltet werden.

Vertraulichkeit

Dadurch wird der Umfang der Auswirkungen auf die Vertraulichkeit von Daten innerhalb einer Ressource gemessen, wenn die Schwachstelle ausgenutzt wird. Dies reicht von Keine , bei dem keine Vertraulichkeit verloren geht, bis Hoch, bei dem alle Informationen innerhalb einer Ressource unkenntlich sind, oder vertrauliche Informationen wie Passwörter oder Verschlüsselungsschlüssel können unkenntlich gemacht werden.

Integrität

Dadurch wird der Grad der Auswirkungen auf die Integrität der Daten innerhalb der betroffenen Ressource gemessen, wenn die Schwachstelle ausgenutzt wird. Integrität ist gefährdet, wenn der Angreifer Dateien innerhalb der betroffenen Ressourcen ändern kann. Der Wert reicht von Keine, wobei der Exploit es einem Angreifer nicht erlaubt, Informationen zu ändern, bis Hoch, wobei die Schwachstelle es einem Angreifer ermöglicht, einzelne oder alle Dateien zu ändern, oder die Dateien, die geändert werden könnten, schwerwiegende Folgen haben.

Verfügbarkeit

Dadurch wird der Umfang der Auswirkungen auf die Verfügbarkeit der betroffenen Ressource gemessen, wenn die Schwachstelle ausgenutzt wird. Der Wert reicht von Keine, wenn sich die Schwachstelle überhaupt nicht auf die Verfügbarkeit auswirkt, bis Hoch, wobei der Angreifer bei Ausnutzung die Verfügbarkeit der Ressource vollständig verweigern kann oder dazu führt, dass ein Service nicht verfügbar ist.

Schwachstelleninformationen

In diesem Abschnitt werden verfügbare Informationen über das CVE von Amazon sowie branchenübliche 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 Details zu Schwachstelleninformationen in der -Konsole oder mithilfe der BatchGetFindingDetails-API anzeigen. Die folgenden Details sind in der -Konsole verfügbar:

ATT&CK

Dieser Abschnitt zeigt die MITRE-Taktiken, -Techniken und -Verfahren (TTPs), die mit dem CVE verbunden sind. Die zugehörigen TTPs werden angezeigt. Wenn es mehr als zwei entsprechende 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

In diesem Abschnitt werden relevante Daten im Zusammenhang mit der Schwachstelle behandelt. Das Datum der Cybersecurity and Infrastructure Security Agency (CISA) hat die Schwachstelle zum bekannten Katalog für ausgenutzte Schwachstellen hinzugefügt, basierend auf den Beweisen für eine aktive Ausnutzung, und das Konformitätsdatum, nach dem CISA erwartet, dass Systeme gepatcht werden. Diese Informationen stammen aus CISA.

Bekannte Malware

In diesem Abschnitt werden bekannte Exploit-Kits und Tools aufgeführt, die diese Schwachstelle ausnutzen.

Beweise

In diesem Abschnitt werden die wichtigsten Sicherheitsereignisse im Zusammenhang mit dieser Schwachstelle zusammengefasst. Wenn mehr als 3 Ereignisse dieselbe Wichtigkeitsstufe haben, werden die drei letzten Ereignisse angezeigt.

Letzte Meldung

Dieser Abschnitt zeigt das Datum der letzten bekannten öffentlichen Ausnutzung für diese Schwachstelle.

Schweregrade für Erkenntnisse von Amazon Inspector

Wenn Amazon Inspector ein Schwachstellenergebnis generiert, weist es dem Ergebnis automatisch einen Schweregrad zu. Der Schweregrad einer Erkenntnis spiegelt die Hauptmerkmale der Erkenntnis wider und kann Ihnen daher helfen, Ihre Erkenntnisse zu bewerten und zu priorisieren. Der Schweregrad einer Erkenntnis impliziert nicht oder weist anderweitig auf die Wichtigkeit oder Wichtigkeit hin, die eine betroffene Ressource für Ihre Organisation haben könnte.

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, unterscheidet sich je nach Erkenntnistyp. In den folgenden Abschnitten über erfahren Sie mehr darüber, wie Amazon Inspector den Schweregrad für jeden Erkenntnistyp bestimmt.

Schweregrad der Softwarepaketschwachstelle

Amazon Inspector verwendet den NVD/CVSS-Score als Grundlage für die Schweregradbewertung für Softwarepaket-Schwachstellen. Der NVD/CVSS-Score ist der von der NVD veröffentlichte und durch das CVSS definierte Schwachstellenschweregrad. Der NVD/CVSS-Score ist eine Zusammensetzung von Sicherheitsmetriken, wie z. B. Angriffskomplexität, Ausnutzungscodereife und erforderliche Berechtigungen. Amazon Inspector erzeugt einen numerischen Wert von 1 bis 10, der den Schweregrad der Schwachstelle widerspiegelt. Amazon Inspector kategorisiert dies als Basiswert, da es den Schweregrad einer Schwachstelle gemäß ihren intrinsischen Eigenschaften widerspiegelt, die im Laufe der Zeit konstant sind. Dieser Wert geht auch davon aus, dass sich dies in verschiedenen bereitgestellten Umgebungen angemessen auf den schlimmsten Fall auswirkt. Der CVSS v3-Standard ordnet CVSS-Werte den folgenden Schweregraden zu.

Ergebnis	Bewertung
0	Informational
0.1–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10.0	Critical

Die Erkenntnisse zu Paketschwachstellen können auch den Schweregrad Untriaged haben. Das bedeutet, dass der Anbieter noch keinen Schwachstellenwert für die erkannte Schwachstelle festgelegt hat. In diesem Fall empfehlen wir, die Referenz-URLs für die Erkenntnis zu verwenden, um diese Schwachstelle zu untersuchen und entsprechend zu reagieren.

Zu den Ergebnissen der Paketschwachstelle gehören die folgenden Punktzahlen und die zugehörigen Bewertungsvektoren als Teil ihrer Erkenntnisdetails:

- EPSS-Score
- Inspector-Score

- CVSS 3.1 von Amazon CVE
- CVSS 3.1 von NVD
- CVSS 2.0 von NVD (falls zutreffend)

Schweregrad der Code-Schwachstelle

Für Ergebnisse zu Code-Schwachstellen verwendet Amazon Inspector die Schweregrade, die von den Amazon- CodeGuru Detektoren definiert werden, die das Ergebnis generiert haben. Jedem Detektor wird mithilfe des CVSS v3-Scoring-Systems ein Schweregrad zugewiesen. Eine Erläuterung der Schweregrade, die CodeGuru verwendet, finden Sie unter Definitionen des Schweregrads im CodeGuru Handbuch. Eine Liste der Detektoren nach Schweregrad finden Sie unter den unterstützten Programmiersprachen unten:

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

Schweregrad der Netzwerkerreichbarkeit

Amazon Inspector bestimmt den Schweregrad für eine Schwachstelle der Netzwerkerreichbarkeit basierend auf dem Service, den Ports und Protokollen, die verfügbar sind, und dem Typ des offenen Pfads. Die folgende Tabelle definiert diese Schweregrade. Der Wert in der Spalte Bewertung des offenen Pfads stellt offene Pfade von virtuellen Gateways, durch Peering verbundenen VPCs und AWS Direct Connect Netzwerken dar. Alle anderen bereitgestellten Services, Ports und Protokolle haben eine Bewertung des informativen Schweregrads.

Service	TCP-Ports	UDP-Ports	Internetp fadbewertung	Bewertung des offenen Pfads
DHCP	67, 68, 546, 547	67, 68, 546, 547	Medium	Informational
Elasticsearch	9300, 9200	NA	Medium	Informational
FTP	21	21	High	Medium
Global catalog LDAP	3268	NA	Medium	Informational

Global catalog LDAP over TLS	3269	NA	Medium	Informational
HTTP	80	80	Low	Informational
HTTPS	443	443	Low	Informational
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752	Medium	Informational
LDAP	389	389	Medium	Informational
LDAP over TLS	636	NA	Medium	Informational
MongoDB	27017, 27018, 27019, 28017	NA	Medium	Informational
MySQL	3306	NA	Medium	Informational
NetBIOS	137, 139	137, 138	Medium	Informational
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110	Medium	Informational
Oracle	1521, 1630	NA	Medium	Informational
PostgreSQL	5432	NA	Medium	Informational
Print services	515	NA	High	Medium
RDP	3389	3389	Medium	Low
RPC	111, 135, 530	111, 135, 530	Medium	Informational
SMB	445	445	Medium	Informational
SSH	22	22	Medium	Low
SQL Server	1433	1434	Medium	Informational
Syslog	601	514	Medium	Informational

Telnet	23	23	High	Medium
WINS	1512, 42	1512, 42	Medium	Informational

Verwalten von Erkenntnissen in Amazon Inspector

Amazon Inspector bietet mehrere Möglichkeiten, Ihre Ergebnisse zu sortieren, zu gruppieren und zu verwalten. Mit diesen Funktionen können Sie Ergebnisse an Ihre Umgebung anpassen, Ergebnisse nach verschiedenen Ansichten aggregieren 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 zeigt jede Ansicht nur aktive Ergebnisse an. Eine aktive Erkenntnis stellt ein potenzielles Sicherheitsproblem dar, das von Amazon Inspector erkannt wurde und auf eine Schwachstelle oder eine potenzielle Bedrohung hinweist. Unterdrückte Ergebnisse sind aktive Ergebnisse, die Sie mithilfe von Unterdrückungsregeln ausgeschlossen haben. Amazon Inspector setzt den Status einer Erkenntnis automatisch auf „Geschlossen“, wenn es feststellt, dass die Erkenntnis behoben wurde. Sie schließen Ergebnisse nicht manuell.

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

Themen

Anzeigen von Amazon Inspector-Ergebnissen

Die Amazon Inspector-Konsole zeigt Ergebnisse in tabellarischen Ansichten basierend auf verwandten Gruppierungen an. Jede Ansicht enthält Informationen, die Ihnen helfen können, bestimmte Schwachstellen zu analysieren, Ihre anfälligsten Ressourcen zu identifizieren und

die Gesamtauswirkungen von Schwachstellen in Ihrer -Umgebung zu messen. Sie können zu einer anderen Erkenntnisansicht navigieren, indem Sie eine Option im Navigationsseitenbereich Erkenntnisse auswählen. Sie können in jeder Ansicht auch einen Filter erstellen, um sich auf bestimmte Arten von Erkenntnissen zu konzentrieren. Weitere Informationen zur Verwendung von Filtern finden Sie unter Filtern von Amazon Inspector-Ergebnissen.

Die Ergebnisse können nach den folgenden Parametern gruppiert werden:

- Nach Schwachstelle – Listet die kritischsten Schwachstellen auf, die in Ihrer Umgebung erkannt wurden. Wählen Sie in dieser Ansicht einen Schwachstellentitel aus, um einen Detailbereich mit zusätzlichen Informationen zu öffnen.
- Nach Konto – Listet Ihre Konten, den Prozentsatz der Scanabdeckung von Amazon Inspector für jedes Konto und die Gesamtzahl der kritischen und hochgradigen Ergebnisse für jedes Konto auf. Diese Gruppierung ist nur für delegierte Administratoren verfügbar.
- Nach Instance – Listet die anfälligsten Amazon 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 Schwachstellen an.
- Nach Lambda-Funktion – Zeigt die Lambda-Funktionen mit den meisten Schwachstellen an.
- Alle Ergebnisse – Zeigt eine vollständige Liste der Ergebnisse für Ihre Umgebung an. Dies ist die Standardansicht, wenn Sie zur Seite Erkenntnisse navigieren. In dieser Ansicht können Sie nach aktiven, unterdrückten und geschlossenen Ergebnissen filtern.

Sie können Unterdrückungsregeln basierend auf Filtern erstellen, um Ergebnisse aus den Ergebnisansichten auszuschließen. Weitere Informationen finden Sie unter Unterdrücken von Amazon Inspector-Ergebnissen mit Unterdrückungsregeln.

Filtern von Amazon Inspector-Ergebnissen

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

Erstellen von Filtern in der Amazon Inspector-Konsole

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

Ein Filter besteht aus einem Filterkriterium, das aus einem Filterattribut in Kombination mit einem Filterwert besteht. Ergebnisse, die nicht Ihren Filterkriterien entsprechen, werden aus der Liste der Ergebnisse ausgeschlossen. Um beispielsweise alle Erkenntnisse anzuzeigen, die Ihrem Administratorkonto zugeordnet 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 Erkenntnisse, während andere nur für bestimmte Ressourcentypen oder Erkenntnistypen verfügbar sind.

So wenden Sie einen Filter auf die Ergebnisansicht an

1. Öffnen Sie die Amazon 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 Leiste Filter hinzufügen aus, um eine Liste aller geltenden Filterkriterien für diese Ansicht anzuzeigen. Verschiedene Filterkriterien sind in verschiedenen Ansichten verfügbar.
4. Wählen Sie ein Kriterium, nach dem Sie filtern möchten, aus der Liste aus.
5. Geben Sie im Eingabebereich des Kriteriums 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 die Filtereingabeleiste erneut 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.

Unterdrücken von Amazon Inspector-Ergebnissen mit Unterdrückungsregeln

Verwenden Sie Unterdrückungsregeln, um Ergebnisse auszuschließen, die Kriterien entsprechen. Sie können beispielsweise eine Regel erstellen, die alle Erkenntnisse mit niedrigen Schwachstellenwerten unterdrückt, sodass Sie sich nur auf die wichtigsten Erkenntnisse konzentrieren können.

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

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

Amazon Inspector speichert unterdrückte Erkenntnisse, bis sie behoben sind. Amazon Inspector erkennt behobene Erkenntnisse. Wenn Amazon Inspector eine behobene Erkenntnis erkennt, wird die Erkenntnis auf Geschlossen gesetzt und 7 Tage lang gespeichert.

Unterdrückte Ergebnisse werden in AWS Security Hub und Amazon EventBridge als Ereignisse veröffentlicht. Sie können unerwünschte Erkenntnisse in Security Hub automatisch unterdrücken, indem Sie den Status der Erkenntnisse 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 angezeigt werden. Sie können unterdrückte Erkenntnisse jederzeit in der Amazon Inspector-Konsole anzeigen.

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

Erstellen einer Unterdrückungsregel

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

> **Note**
>
> Nur eigenständige Konten und delegierte Administratoren von Amazon Inspector können Unterdrückungsregeln erstellen und verwalten. Mitglieder einer Organisation sehen im Navigationsbereich keine Option für Unterdrückungsregeln.

So erstellen Sie eine Unterdrückungsregel (Konsole)

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich Unterdrückungsregeln 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 der Filterkriterien anzuzeigen, die Sie 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 eine optionale Beschreibung ein.
5. Wählen Sie Save rule (Regel speichern). Amazon Inspector wendet sofort die neue Unterdrückungsregel an und blendet alle Ergebnisse aus, die den Kriterien entsprechen.

Anzeigen unterdrückter Ergebnisse

Standardmäßig zeigt Amazon Inspector keine unterdrückten Ergebnisse in der Amazon Inspector-Konsole an. Sie können jedoch die Ergebnisse anzeigen, die von einer bestimmten Regel unterdrückt werden.

So zeigen Sie unterdrückte Ergebnisse an

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

Ändern von Unterdrückungsregeln

Sie können jederzeit Änderungen an Unterdrückungsregeln vornehmen.

So ändern Sie Unterdrückungsregeln

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home
2. Wählen Sie im Navigationsbereich 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, unterdrückt Amazon Inspector neue und bestehende Erkenntnisse, die die Regelkriterien erfüllen und nicht durch andere Regeln unterdrückt werden.

Nachdem Sie eine Unterdrückungsregel gelöscht haben, haben neue und bestehende Erkenntnisse, die die Kriterien der Regel erfüllt haben, den Status Aktiv . Das bedeutet, dass sie standardmäßig in der Amazon Inspector-Konsole angezeigt werden. Darüber hinaus veröffentlicht Amazon Inspector diese Ergebnisse EventBridge als Ereignisse in AWS Security Hub und Amazon.

So löschen Sie eine Unterdrückungsregel

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie im Navigationsbereich 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 all Ihre Ergebnisse in der aktuellen VersionAWS-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 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 sicherAWS KMS, dass Sie die folgenden Aktionen ausführen dürfen:

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

Mit diesen Aktionen können Sie die Schlüsselrichtlinie für das abrufen und aktualisierenAWS 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 Permissions (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.

   Stellen Sie beim Hinzufügen der Anweisung 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 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.

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 verwendenAWS-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. Beispiele:

  ```
  "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, während andere Aktionen für Ihr Konto ausgeführt werden. 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. Beispiele:

  ```
  "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.

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 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 ServiceEntwicklerhandbuch.

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 keinen vorhandenen Schlüssel haben, 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 die AWS-Region zu ändern, verwenden Sie die Regionenauswahl 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 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.

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 verwendenAWS-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 die Konto-ID für jedes weitere Konto zu dieser Bedingung hinzu. Beispiele:

```
"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. Beispiele:

```
"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 tragen dazu bei, zu verhindern, dass Amazon Inspector bei Transaktionen mit als verwirrter Stellvertreter eingesetzt wirdAWS 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 ErgebnisseAWS-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.

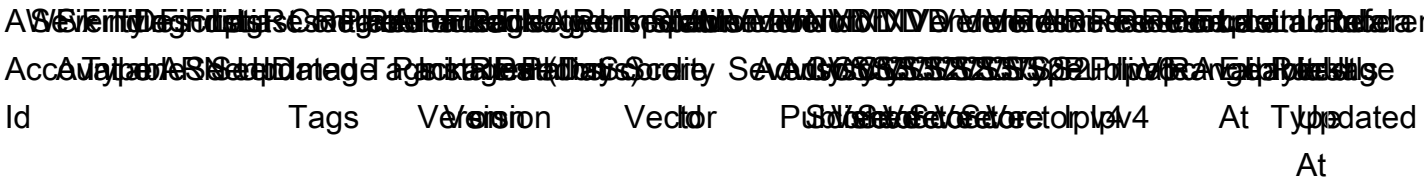
4. Wählen Sie Ergebnisse exportieren aus.
5. Geben Sie im Abschnitt Exporteinstellungen für Exportdateityp ein Dateiformat für den Bericht an:

   - 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, Fix 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:



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 anAWS 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 ServiceEntwicklerhandbuch.

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.

Erstellung benutzerdefinierter Antworten auf die Ergebnisse von Amazon Inspector mit Amazon EventBridge

Amazon Inspector erstellt für Amazon ein Ereignis EventBridge für neu generierte Ergebnisse, neu aggregierte Ergebnisse und Änderungen im Stand der Ergebnisse. Alles andere als eine Änderung der `lastObservedAt` Felder `updatedAt` und führt zur Veröffentlichung einer neuen Veranstaltung. Das bedeutet, dass neue Ereignisse für ein Ergebnis generiert werden, wenn Sie Aktionen wie den Neustart einer Ressource oder das Ändern der mit einer Ressource verknüpften Tags ausführen. Die Finding-ID im `id` Feld bleibt jedoch dieselbe. Ereignisse werden auf die bestmögliche Weise ausgegeben.

> **Note**
>
> Wenn es sich bei Ihrem Konto um einen delegierten Administrator von Amazon Inspector 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 Standardereignisbus in derselben Region. Das bedeutet, dass Sie für jede Region, in der Sie Amazon Inspector ausführen, Veranstaltungsregeln 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 EventBridgeAmazon-Benutzerhandbuch.

Ereignisationsereignis

Im Folgenden finden Sie ein Beispiel für ein Ereignis für ein EC2-Ereignissereignissereignissereignissereignissereignissereignissereignis. Ein Beispiel für ein Schema anderer Findungstypen 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"
    }
}
```


Erstellen einer EventBridge Regel, 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 Warnmeldungen `CRITICAL` und `HIGH` Schweregrad an 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 Eventregel verknüpfen.

Schritt 1. Einrichten eines Amazon-SNS-Themas und Endpoints

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-Leitfaden.

In diesem Beispiel finden Amazon Inspector ein. 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 ein, wie**`Inspector_to_Email`**. Weitere Angaben sind optional.
4. Wählen Sie Create Topic (Thema erstellen) aus. Dadurch wird ein neues Panel 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, für die Sie Benachrichtigungen erhalten möchten.

   > **Note**
   >
   > Nachdem Sie das Abonnement erstellt haben, 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 ein, wie**`Inspector_to_Slack`**. Weitere Angaben sind optional. Wählen Sie Thema erstellen, um die Erstellung des Endpoints abzuschließen.

Einen AWS Chatbot Client konfigurieren

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

> **Note**
>
> Wenn du Slack auswählst, musst du die Berechtigungen für den AWS Chatbot Zugriff auf deinen Channel bestätigen, 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. Wählen Sie für den Slack-Kanal aus, den Sie verwenden möchten.
   c. Kopiere in Slack die Channel-ID des privaten Channels, indem du mit der rechten Maustaste auf den Channel-Namen klickst und Link kopieren auswählst.
   d. Füge im AWS Chatbot Fenster die Channel-ID, die du aus Slack kopiert hast, in das Feld Private Channel-ID ein. AWS Management Console
   e. Wählen Sie unter Berechtigungen aus, eine IAM-Rolle mithilfe einer Vorlage zu erstellen, falls Sie noch keine Rolle haben.
   f. Wählen Sie für Richtlinienvorlagen die Option Benachrichtigungsberechtigungen aus. Dies ist die IAM-Richtlinienvorlage fürAWS 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 ausAmazonInspector. 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 Configure (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 ein, wie**`Inspector_to_Chime`**. Weitere Angaben sind optional. Wählen Sie Thema erstellen, um den Vorgang abzuschließen.

Einen AWS Chatbot Client konfigurieren

1. Navigieren Sie zur AWS Chatbot-Konsole unter https://console.aws.amazon.com/chatbot/.
2. Wählen Sie im Bereich Konfigurierte Clients die Option Neuen Client konfigurieren aus.
3. Wählen Sie Chime und wählen Sie dann 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 aus, um die Webhook-URL in Ihre Zwischenablage zu kopieren.
6. Fügen Sie im AWS Chatbot Fenster die URL, die Sie kopiert haben, in das Feld Webhook-URL ein. AWS Management Console
7. Wählen Sie unter Berechtigungen aus, eine IAM-Rolle mithilfe einer Vorlage zu erstellen, falls Sie noch keine Rolle haben.
8. Wählen Sie für Richtlinienvorlagen die Option Benachrichtigungsberechtigungen aus.
   Dies ist die IAM-Richtlinienvorlage fürAWS 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 Configure (Konfigurieren).

Schritt 2. Erstellen Sie eine EventBridge Regel für die Ergebnisse von Amazon Inspector

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Regeln aus, und wählen Sie 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 Event Pattern die Option Benutzerdefinierte Muster (JSON-Editor) aus.
6. Fügen Sie den folgenden JSON-Text in den Editor ein.

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

> **Note**
>
> Dieses Muster sendet Benachrichtigungen, wenn Amazon Inspector einen aktiven Befund `CRITICAL` oder einen `HIGH` Schweregrad feststellt.

Wählen Sie Weiter, wenn Sie mit der Eingabe des Event-Musters fertig sind.

7. Wählen Sie auf der Seite „Ziele auswählen“ AWS-Service. Wählen Sie dann unter Zieltyp auswählen die Option SNS-Thema aus.
8. Wählen Sie für Thema den Namen des SN-Themas aus, das Sie in Schritt 1 erstellt haben. Wählen Sie anschließend Next (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.

EventBridgefür Amazon Inspector Inspector-Umgebungen mit mehreren Konten

Wenn Sie ein delegierter Administrator von Amazon Inspector sind, werden in Ihrem Konto EventBridge Regeln angezeigt, die auf den entsprechenden Erkenntnissen aus Ihren 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 zusätzlich zu den Ergebnissen und Ereignissen, die von Ihrem eigenen Konto generiert wurden, über Ergebnisse und Ereignisse informiert, die von Ihren Mitgliedskonten generiert wurden.

Sie können die `accountId` JSON-Details des Ergebnisses 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 KMSSchlüssel 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 InterfaceFühren 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.

Amazon Inspector Schwachstellendatenbanksuche

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

In diesem Thema wird beschrieben, wie Sie die Amazon Inspector-Hilfsdatenbank mit einer CVE-ID durchsuchen und die CVE-Detailseite trennen. Weitere Informationen zu Erkenntnissen finden Sie unter Details zu den Erkenntnissen in Amazon Inspector .

> **Note**
>
> Amazon Inspector verfolgt und erzeugt 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 unterstützt die CVE-Suche nichtMicrosoft Windows.

Durchsuchen der Schwachstellendatenbank

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 aktivieren, AWS-Region bevor Sie die Schwachstellendatenbank durchsuchen können.

Console

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/
2. Wählen Sie im Navigationsbereich die Option Schwachstellendatenbanksuche aus.
3. Geben Sie in die Suchleiste eine CVE-ID ein und wählen Sie Suchen aus.

API

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

Grundlegendes zu CVE-Details

In diesem Abschnitt wird beschrieben, wie die CVE-Detailseite unterbrochen wird.

CVE-Details

Der Abschnitt CVE-Details enthält die folgenden Informationen:

- CVE-Beschreibung und -ID
- CVE-Schweregrad
- Common Vulnerability Scoring System (CVSS)- und Exploit Prediction Scoring System (EPSS)-Werte
- Erkennungsplattformen

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

- Common Weakness Enumeration (CWE)
- Vom Anbieter erstellte und aktualisierte Daten

Schwachstelleninformationen

Der Abschnitt Schwachstelleninformationen enthält Bedrohungsdaten wie Ausnutzungsziele und das letzte bekannte öffentliche Ausnutzungsdatum.

Es stellt auch Daten der Cybersecurity and Infrastructure Security Agency (CISA) bereit, die die Abhilfemaßnahme, das Datum, an dem das CVE dem Katalog bekannter ausgelasteter Schwachstellen hinzugefügt wurde, und die Datumszeit, zu der CISA erwartet, dass Bundesbehörden das CVE korrigieren.

Referenzen

Der Abschnitt Referenzen enthält Links zu -Ressourcen für weitere Informationen zum 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 unterErstellung benutzerdefinierter Antworten auf die 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"
    }
}
```

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

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

Die CI/CD-Integration von Amazon Inspector 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 aus einem bereitgestellten Container-Image eine Softwarerechnung (SBOM). Anschließend scannt die Amazon Inspector Scan API diese SBOM und erstellt einen Bericht mit Details zu erkannten Schwachstellen.

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 ihrem Marketplace verfügbar sind, oder Sie können Ihre eigene benutzerdefinierte Scanintegration erstellen.

Themen

Plugin-Integration

Amazon Inspector bietet Plugins für unterstützte CI/CD-Lösungen. Sie können diese Plugins von ihren jeweiligen Marketplaces installieren und sie dann verwenden, um Amazon Inspector Scans als Build-Schritt in Ihrer Pipeline hinzuzufügen. Der Build-Schritt des Plugins führt den Amazon

Inspector-SBOM-Generator auf dem von Ihnen bereitgestellten Image aus und führt dann die Amazon Inspector-Scan-API auf der generierten SBOM aus.

Im Folgenden finden Sie eine Übersicht über die Funktionsweise einer Amazon Inspector CI/CD-Integration über Plugins:

1. Sie konfigurieren einen AWS-Konto , um den Zugriff auf die Amazon Inspector Scan API zu erlauben. Anweisungen finden Sie unter Einrichten eines AWS Kontos für die Verwendung der CI/CD-Integration von Amazon Inspector .
2. Sie installieren das Amazon Inspector-Plugin vom Marketplace aus.
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 Ihrer CI/CD-Pipeline hinzu und konfigurieren den Scan.
5. Wenn Sie einen Build ausführen, nimmt 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 Schwachstellen bewertet.
7. Die Amazon Inspector Scan API-Antwort wird in einen Schwachstellenbericht im CSV-, SBOM JSON- und HTML-Format umgewandelt. Der Bericht enthält Details zu allen Schwachstellen, die Amazon Inspector gefunden hat.

Unterstützte CI/CD-Lösungen

Amazon Inspector unterstützt derzeit die folgenden CI/CD-Lösungen. Vollständige Anweisungen zum Einrichten der CI/CD-Integration mit einem Plugin finden Sie, indem Sie das Plugin für Ihre CI/CD-Lösung auswählen:

- Jenkins-Plugin
- TeamCity-Plugin

Benutzerdefinierte Integration

Wenn Amazon Inspector keine Plugins für Ihre CI/CD-Lösung bereitstellt, können Sie Ihre eigene benutzerdefinierte CI/CD-Integration mit einer Kombination aus dem Amazon Inspector SBOM

Generator und der Amazon Inspector Scan API erstellen. Sie können auch eine benutzerdefinierte Integration verwenden, um Scans mithilfe der über Amazon Inspector SBOM Generator verfügbaren Optionen zu optimieren.

Im Folgenden finden Sie eine Übersicht über die Funktionsweise einer benutzerdefinierten CI/CD-Integration von Amazon Inspector:

1. Sie konfigurieren einen AWS-Konto , um den Zugriff auf die Amazon Inspector Scan API zu erlauben. Anweisungen finden Sie unter Einrichten eines AWS Kontos für die Verwendung der CI/CD-Integration von Amazon Inspector .
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 auf der generierten SBOM, um einen Schwachstellenbericht zu erstellen.

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

Einrichten eines AWS Kontos für die Verwendung der CI/CD-Integration von Amazon Inspector

Sie müssen sich für ein registrieren AWS-Konto , um die CI/CD-Integration von Amazon Inspector verwenden zu können. Der AWS-Konto muss über eine IAM-Rolle verfügen, die Ihrer pipleline Zugriff auf die Amazon Inspector Scan API gewährt.

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

> **Note**
>
> Wenn Sie sich bereits für ein registriert haben AWS-Konto, können Sie mit fortfahrenKonfigurieren einer IAM-Rolle für die CI/CD-Integration.

Themen

Registrieren Sie sich für ein AWS-Konto

Wenn Sie kein haben AWS-Konto, führen Sie die folgenden Schritte aus, um eines zu erstellen.

So registrieren Sie sich für ein 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 ein registrieren AWS-Konto, Root-Benutzer des AWS-Kontos wird ein 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 eine Bestätigungs-E-Mail, nachdem der Registrierungsprozess abgeschlossen ist. 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 ein registriert haben AWS-Konto, sichern Sie Ihr Root-Benutzer des AWS-Kontos, aktivieren Sie AWS IAM Identity Center und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Ihrer Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console als 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 unter Konfigurieren des Benutzerzugriffs mit dem Standard IAM-Identity-Center-Verzeichnis- im AWS IAM Identity Center -Benutzerhandbuch.

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 unter Anmelden beim - AWS Zugriffsportal im AWS-Anmeldung -Benutzerhandbuch.

Konfigurieren einer IAM-Rolle für die CI/CD-Integration

Um das Scannen von Amazon Inspector 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 Softwarerechnung der Materialien (SBOMs) scannt. Anschließend können Sie diese Richtlinie an eine IAM-Rolle anfügen, die Ihr Konto annehmen kann, um die Amazon Inspector Scan API auszuführen.

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 Richtlinien-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 einen Namen, z. B. `InspectorCICDscan-policy`, und fügen Sie eine optionale Beschreibung hinzu. Wählen Sie dann Richtlinie erstellen aus. Diese Richtlinie wird an die 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 für Typ der vertrauenswürdigen Entität 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, und wählen Sie dann Weiter aus.
10. Geben Sie der Rolle einen Namen, z. B. `InspectorCICDscan-role`, und fügen Sie eine optionale Beschreibung hinzu und wählen Sie dann aus`Create Role`.

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 Integrieren 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.txt`Pipfile.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 Ihrer eigenen benutzerdefinierten CI/CD-Pipeline-Integration mit Amazon Inspector Scan

Wir empfehlen, die CI/CD-Plugins von Amazon Inspector zu verwenden, wenn sie auf Ihrem CI/CD-Marketplace verfügbar sind. Eine Liste der verfügbaren Plugins finden Sie unter Unterstützte CI/CD-Lösungen.

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

So richten Sie Ihre eigene benutzerdefinierte Integration ein

1. Konfigurieren Sie einen AWS-Konto , um den Zugriff auf die Amazon Inspector Scan API zu ermöglichen. Anweisungen finden Sie unter Einrichten eines AWS Kontos für die Verwendung der CI/CD-Integration von Amazon Inspector .
2. Installieren und konfigurieren Sie die Binärdatei des Amazon Inspector SBOM Generators. 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, ersetzen Sie durch *`image:id`* den Namen des zu scannenden Images und *`sbom_path.json`* durch den Speicherort für die SBOM-Ausgabe:

   ```
   ./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 bereitzustellen. 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 die , bei der AWS-Region Sie derzeit

authentifiziert sind, und ersetzen Sie *REGION* durch die entsprechende Region. Eine vollständige Liste der Regionen und Endpunkte Endpunkte für die Amazon Inspector Scan API 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 Ergebnis-JSON ausgeben. Die Standardeinstellung kann mit dem `---output-format`Flag 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 die Ausgabe des Inspector-Formats

```
                      {
  "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 InspectorJenkins-Plugins

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

Amazon Inspector ist ein Schwachstellenverwaltungsservice, der Container-Images auf Schwachstellen im Betriebssystem und in Programmiersprachenpaketen basierend auf CVEs scannt. CVEs

Mit dem Amazon InspectorJenkins-Plugin können Sie Ihrer Jenkins Pipeline Amazon-Amazon InspectorSchwachstellenscans hinzufügen.

> **Note**
>
> Amazon-Amazon Inspector-Schwachstellenscans können so konfiguriert werden, dass Pipeline-Ausführungen basierend auf der Anzahl und dem Schweregrad der erkannten Schwachstellen bestanden oder fehlschlagen.

Die neueste Version des Jenkins Plugins finden Sie auf dem Jenkins Marketplace unter https://plugins.jenkins.io/amazon-inspector-image-scanner/.

In den folgenden Schritten wird beschrieben, wie Sie das Amazon Inspector Jenkins-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. Einrichten eines AWS-Konto

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

Schritt 2. Installieren des Amazon Inspector Jenkins-Plugins

Im folgenden Verfahren wird beschrieben, wie Sie das Amazon Inspector-Jenkins-Plugin vom Jenkins Dashboard aus installieren.

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

(Optional) Schritt 3. Hinzufügen von Docker-Anmeldeinformationen zu Jenkins

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

Im folgenden Verfahren wird beschrieben, wie Docker-Anmeldeinformationen aus dem Jenkins Dashboard zu hinzugefügt Jenkins werden.

1. Wählen Sie im Jenkins-Dashboard Jenkins verwalten, Anmeldeinformationen und dann System aus.

2. Wählen Sie Globale Anmeldeinformationen und dann Anmeldeinformationen hinzufügen aus.
3. Wählen Sie für Art die Option Benutzername mit Passwort aus.
4. Wählen Sie für Bereich die Option Global (Jenkins, Knoten, Elemente, alle untergeordneten Elemente usw.) aus.
5. Geben Sie Ihre Details ein und wählen Sie dann OK aus.

(Optional) Schritt 4. Hinzufügen von AWS Anmeldeinformationen

> **Note**
>
> Fügen Sie AWS Anmeldeinformationen nur hinzu, wenn Sie sich basierend auf einem IAM-Benutzer authentifizieren möchten. Andernfalls überspringen Sie diesen Schritt.

Im folgenden Verfahren wird beschrieben, wie Sie AWS Anmeldeinformationen aus dem Jenkins Dashboard hinzufügen.

1. Wählen Sie im Jenkins-Dashboard Jenkins verwalten, Anmeldeinformationen und dann System aus.
2. Wählen Sie Globale Anmeldeinformationen und dann Anmeldeinformationen hinzufügen aus.
3. Wählen Sie für Art die Option AWS-Anmeldeinformationen aus.
4. Geben Sie Ihre Details ein, einschließlich Ihrer Zugriffsschlüssel-ID und Ihres geheimen Zugriffsschlüssels, und wählen Sie dann OK aus.

Schritt 5. Hinzufügen von CSS-Unterstützung in einem JenkinsSkript

Im folgenden Verfahren wird beschrieben, wie Sie CSS-Unterstützung in einem JenkiknsSkript hinzufügen.

1. Starten Sie Jenkins neu.
2. Wählen Sie im Dashboard Jenkins verwalten, Knoten, Integrierter Knoten und dann Skriptkonsole aus.
3. Fügen Sie im Textfeld die Zeile hinzu `System.setProperty("hudson.model.DirectoryBrowserSupport.CSP", "")`und wählen Sie dann Ausführen aus.

Schritt 6: Hinzufügen von Amazon Inspector Scan zu Ihrem Build

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

Amazon Inspector Scan zu Ihrem Build durch Hinzufügen eines Build-Schritts in Ihrem Projekt

1. Scrollen Sie auf der Konfigurationsseite nach unten zu Build-Schritte 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, das das Plugin ausführt.

   b. (Option 2) Wählen Sie Manuell, wenn Sie die Amazon Inspector SBOM Generator-Binärdatei zum 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 Installieren des Amazon Inspector SBOM Generators (Sbomgen) im Amazon Inspector SBOM Generator .
3. Führen Sie die folgenden Schritte aus, um die Konfiguration des Build-Schritts von Amazon Inspector Scan abzuschließen:

   a. Geben Sie Ihre Image-ID ein. Das Image kann lokal, remote oder archiviert sein. Bildnamen sollten der Docker Namenskonvention entsprechen. Wenn Sie ein exportiertes Image analysieren, geben Sie den Pfad zur erwarteten tar-Datei an. Sehen Sie sich die folgenden Beispielpfade für Image-IDs an:

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

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

   b. Wählen Sie einen ausAWS-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 angeben:

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

   ii. (Optional) Wählen Sie für AWS-Anmeldeinformationen die ID aus, die basierend auf einem IAM-Benutzer authentifiziert werden soll.

   iii. (Optional) Geben Sie für AWS Profilname den Namen eines Profils an, das mit einem Profilnamen authentifiziert werden soll.

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

4. Wählen Sie Speichern.

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

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

So laden Sie die deklarative SBOMGen-Pipeline automatisch herunter

- Verwenden Sie die folgende Beispielsyntax, um Amazon Inspector Scan zu einem Build hinzuzufügen. Ersetzen Sie *SBOMGEN_SOURCE* basierend auf Ihrer bevorzugten Betriebssystemarchitektur des Amazon Inspector SBOM Generator-Downloads durch linuxAmd64 oder linuxArm64. Ersetzen Sie *IMAGE_PATH* durch den Pfad zu Ihrem Image (z. B. *al Bol: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 Schwachstellenschwellenwerte 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,
               ])
            }
          }
        }
    }
}
```

So laden Sie die deklarative SBOMGen-Pipeline manuell herunter

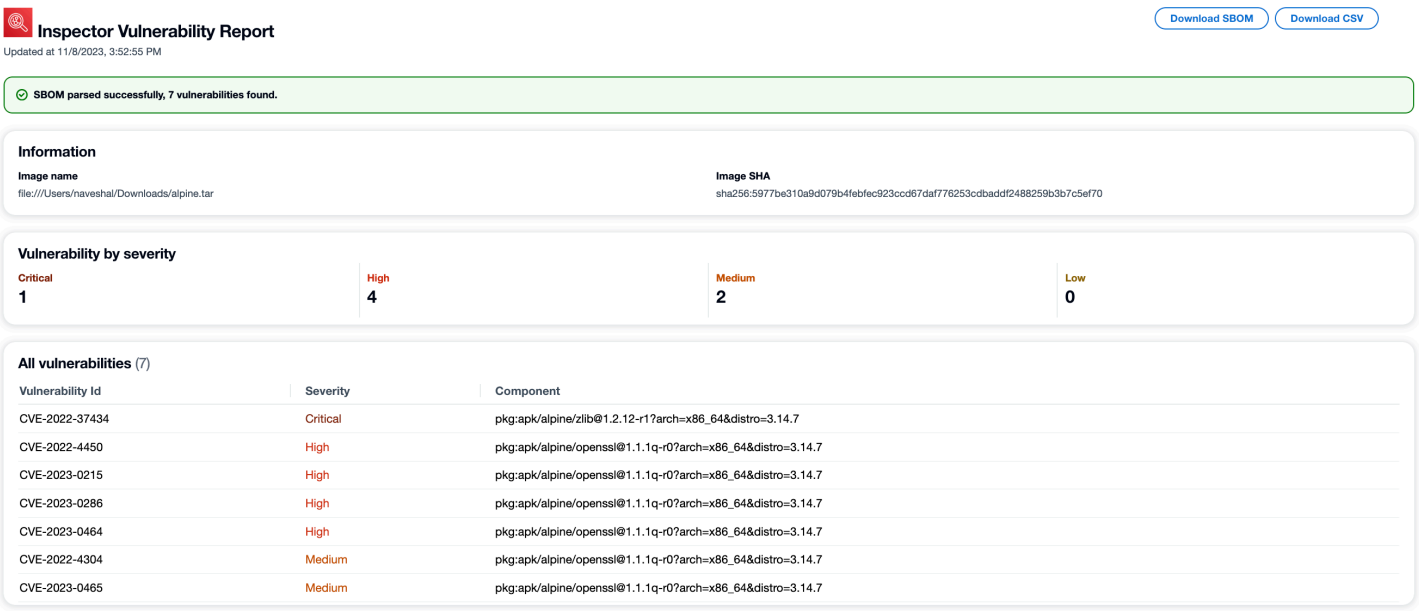
- Verwenden Sie die folgende Beispielsyntax, um Amazon Inspector Scan zu einem Build hinzuzufügen. Ersetzen Sie *SBOMGEN_PATH* durch den Pfad zu dem Amazon Inspector SBOM Generator, den Sie in Schritt 3 installiert haben, *IMAGE_PATH* durch den Pfad zu Ihrem Image (z. B. *alema:latest), IAM_ROLE* durch 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 Schwachstellenschwellenwerte aktivieren und Werte für jeden Schweregrad angeben.

> **Note**
>
> Platzieren Sie 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. Anzeigen Ihres Amazon Inspector-Schwachstellenberichts

1. Schließen Sie einen neuen Build Ihres Projekts ab.
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 sehen Sie ein Beispiel für einen HTML-Bericht:



Fehlerbehebung

Im Folgenden finden Sie häufige Fehler, die bei der Verwendung des Amazon Inspector Scan-Plugins für auftreten könnenJenkins.

Fehler beim Laden von Anmeldeinformationen oder sts-Ausnahme

Fehler:

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

Resoultion

Rufen Sie `aws_access_key_id` und `aws_secret_access_key` für Ihr AWS Konto ab. Richten Sie `aws_access_key_id` und `aws_secret_access_key` in ein`~/.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

Führen Sie das folgende Verfahren aus, 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 der Binärdatei ausführbare Berechtigungen mit dem folgenden Befehl: `chmod +x inspector-sbomgen`.
3. Geben Sie den richtigen Jenkins Maschinenpfad im Plugin an, z. B. `/opt/folder/arm64/inspector-sbomgen`.
4. Speichern Sie die Konfiguration und führen Sie den Jenkins Auftrag aus.

Verwenden des Amazon InspectorTeamCity-Plugins

Mit dem Amazon InspectorTeamCity-Plugin können Sie Ihrer TeamCity Pipeline Amazon Inspector Schwachstellenscans hinzufügen. Das Plugin nutzt die Binär- und Amazon Inspector Scan-API des Amazon Inspector SBOM Generators, um am Ende Ihres Builds detaillierte Berichte zu erstellen, sodass Sie Risiken vor der Bereitstellung untersuchen und beheben können. Die Scans können auch so konfiguriert werden, dass sie Pipeline-Ausführungen basierend auf der Anzahl und dem Schweregrad der erkannten Schwachstellen bestehen oder fehlschlagen.

Amazon Inspector ist ein von angebotener Schwachstellenverwaltungsservice AWS , der Container-Images sowohl auf Betriebssystem- als auch auf Programmiersprachenpaket-Schwachstellen basierend auf CVEs scannt. Weitere Informationen zur CI/CD-Integration von Amazon Inspector finden Sie unter Integrieren 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.

Die neueste Version des Plugins finden Sie auf dem TeamCity Marketplace unter https://plugins.jetbrains.com/plugin/23236-amazon-inspector-scanner. Alternativ können Sie die Schritte in jedem Abschnitt dieses Dokuments ausführen, um das Amazon Inspector TeamCity-Plugin einzurichten:

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

2. Installieren Sie das Amazon InspectorTeamCity-Plugin.

   a. Gehen Sie von Ihrem Dashboard aus 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 Binärdatei des Amazon Inspector SBOM Generators in Ihrem Teamcity-Serververzeichnis. Anweisungen finden Sie unter Amazon Inspector SBOM Generator installieren () Sbomgen.

4. Fügen Sie Ihrem Projekt einen Build-Schritt für Amazon Inspector Scan hinzu.

   a. Scrollen Sie auf der Konfigurationsseite nach unten zu Build-Schritte, wählen Sie Build-Schritt hinzufügen und dann Amazon Inspector Scan aus.

   b. Konfigurieren Sie den Build-Schritt von Amazon Inspector Scan, indem Sie die folgenden Details eingeben:

      - Fügen Sie einen Schrittnamen hinzu.
      - Wählen Sie zwischen zwei Installationsmethoden des Amazon Inspector SBOM Generators: Automatisch oder Manuell.
        - Automatisches Herunterladen der neuesten Version von Amazon Inspector SBOM Generator basierend auf Ihrer System- und CPU-Architektur.
        - Für das manuelle Verfahren müssen Sie einen vollständigen Pfad zu einer zuvor heruntergeladenen Version von Amazon Inspector SBOM Generator angeben.

        Weitere Informationen finden Sie unter Installieren des Amazon Inspector SBOM Generators (Sbomgen) im Amazon Inspector SBOM Generator.
      - Geben Sie Ihre Image-ID ein. Ihr Image kann lokal, remote oder archiviert sein. Bildnamen sollten der Docker Namenskonvention entsprechen. Wenn Sie ein exportiertes Image analysieren, geben Sie den Pfad zur erwarteten tar-Datei an. Sehen Sie sich die folgenden Beispielpfade für Image-IDs 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 ausAWS-Region, über die die Scananforderung gesendet werden soll.

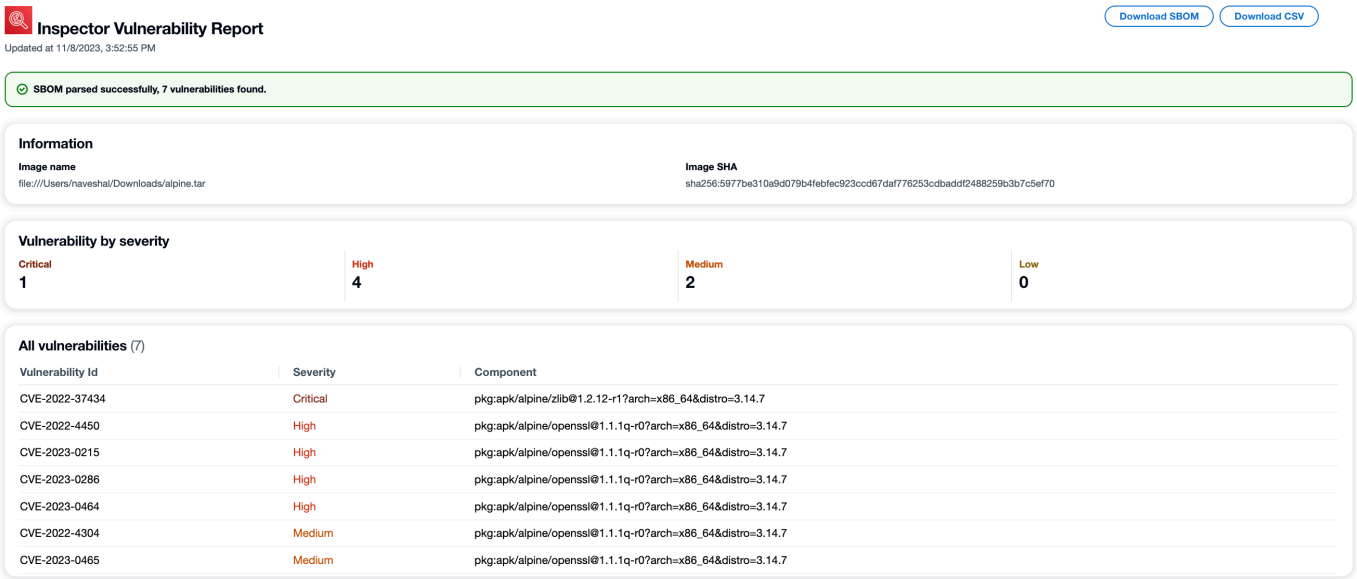
- (Optional) Geben Sie für Docker-Authentifizierung Ihren Docker-Benutzernamen und das Docker-Passwort ein. Tun Sie dies nur, wenn sich Ihr Container-Image in einem privaten Repository befindet.
- (Optional) Geben Sie für AWS Authentifizierung Ihre AWS Zugriffsschlüssel-ID und Ihren AWS geheimen Schlüssel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

c. Wählen Sie Speichern.

5. Sehen Sie sich Ihren Schwachstellenbericht von Amazon Inspector an.

a. Schließen Sie einen neuen Build Ihres Projekts ab.

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 Verwendung der agentenlosen Amazon EC2-Scanfunktion 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 kompromittierten Workloads, böswilliger Nutzung von Ressourcen oder unbefugtem Zugriff auf Ihre Daten führen können. Wenn Amazon Inspector eine Schwachstelle erkennt, wird ein Ergebnis erstellt. Zu den Erkenntnissen gehören Details im Zusammenhang mit der Erkennung, um Ihnen bei der Behebung der Schwachstelle zu helfen. Sie können die Ergebnisse in der Amazon Inspector-Konsole und mithilfe der Amazon Inspector-API überprüfen. Weitere Informationen finden Sie unter Verwalten von Erkenntnissen in Amazon Inspector.

Wenn diese Option aktiviert ist, erkennt Amazon Inspector automatisch alle berechtigten Ressourcen und beginnt mit kontinuierlichen Scans dieser Ressourcen. Amazon Inspector scannt auf Softwareschwachstellen und unbeabsichtigte Netzwerkrisiken. Amazon Inspector führt auch Scans als Reaktion auf Ereignisse aus, z. B. die Installation einer neuen Anwendung oder eines neuen Patches.

Wenn Sie Amazon Inspector zum ersten Mal aktivieren, wird Ihr Konto automatisch bei allen Scantypen registriert. In den folgenden Themen werden spezifische Details zu den Scantypen behandelt, die Amazon Inspector bereitstellt. Amazon Inspector kategorisiert Scantypen basierend auf dem Ressourcentyp, der von einer Schwachstelle 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

- Scannen von AWS Lambda Funktionen mit Amazon Inspector
- Deaktivieren eines Scantyps

Wenn Sie Amazon Inspector zum ersten Mal aktivieren, wird Ihr Konto automatisch bei den folgenden Scantypen registriert: Amazon EC2-Scan, Amazon-ECR-Scan, Lambda-Standardscan. Lambda-Codescan ist eine optionale Ebene des Scannens von Lambda-Funktionen, die Sie jederzeit aktivieren können.

Übersicht über die Scantypen von Amazon Inspector

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

Amazon EC2-Scan

Wenn Sie das Scannen von Amazon EC2 aktivieren, scannt Amazon Inspector Ihre Amazon EC2-Instances auf Schwachstellen im Betriebssystempaket und im Programmiersprachenpaket sowie auf Erreichbarkeit des Netzwerks. Amazon Inspector scannt Ihre EC2-Instance auf Common Vulnerabilities and Exposures (CVE) und Probleme mit Netzwerkrisiken. Amazon Inspector führt Scans durch die Verwendung des auf Ihrer Instance installierten SSM-Agenten oder durch Amazon-EBS-Snapshots von Instances durch. Weitere Informationen zu Scans für Amazon EC2 finden Sie unter Scannen von Amazon EC2-Instances mit Amazon Inspector.

Amazon-ECR-Scan

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

Lambda-Standardscan

Wenn Sie das Lambda-Standardscannen aktivieren, erkennt Amazon Inspector die Lambda-Funktionen in Ihrem Konto und beginnt sofort mit dem Scannen auf Schwachstellen. Amazon

Inspector scannt neue Lambda-Funktionen und -Ebenen, wenn sie bereitgestellt werden, und scannt sie erneut, wenn sie aktualisiert werden oder wenn neue Common Vulnerabilities and Exposures (CVEs) veröffentlicht werden. Weitere Informationen zum Scannen von Lambda-Funktionen finden Sie unter Scannen von AWS Lambda Funktionen mit Amazon Inspector.

Lambda-Standardscan + Lambda-Codescan

Diese Option kann das Scannen des Lambda-Standards mit dem Scannen von Lambda-Code kombinieren. Wenn Lambda-Codescan aktiviert ist, erkennt Amazon Inspector die Lambda-Funktionen und -Ebenen in Ihrem Konto und sucht nach Code-Schwachstellen, die von Ihren Anwendungspaketabhängigkeiten abhängig sind. Lambda-Codescan scannt den benutzerdefinierten Anwendungscode in Ihren Lambda-Funktionen auf Code-Schwachstellen. Diese beiden Scantypen müssen zusammen aktiviert werden. Weitere Informationen finden Sie unter Codescan von Amazon Inspector Lambda.

Aktivieren eines Scantyps

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

- Amazon EC2-Scan – Wenn Sie Amazon Inspector Amazon EC2-Scans für ein Konto aktivieren, scannt Amazon Inspector alle berechtigten Instances in Ihrem Konto auf Paketschwachstellen und Probleme mit der Netzwerkerreichbarkeit. Das Amazon Inspector SSM-Plugin ist auf all Ihren SSM-verwalteten Windows Hosts installiert. Weitere Informationen finden Sie unter Scannen von Windows Instances. Darüber hinaus erstellt Amazon Inspector die folgenden SSM-Zuordnungen 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-Scan – 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

Einfaches Scannen mit Amazon ECR zu Erweitertes Scannen mit Amazon Inspector. Dann werden alle berechtigten 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-Wiederscandauer für Image-Push und Pull-Datum auf 90 Tage festgelegt.

- Lambda-Standardscan – 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 Paketschwachstellen gescannt. Darüber hinaus wird in Ihrem Konto ein CloudTrail serviceverknüpfter Kanal erstellt.
- Lambda-Standardscan + Lambda-Codescan – Diese Scantypen der Lambda-Funktion werden zusammen aktiviert. Wenn Sie das Lambda-Codescannen 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.

Aktivieren von Scans

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

Console

So aktivieren Sie Scans

1. Öffnen Sie die Amazon 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 einen neuen Scantyp aktivieren möchten.
3. Wählen Sie im Navigationsbereich Kontoverwaltung aus.
4. Wählen Sie auf der Seite Kontoverwaltung die Konten aus, für die Sie einen Scantyp aktivieren möchten.
5. Wählen Sie Aktivieren und dann den Scantyp aus, den Sie aktivieren möchten.

6. (Empfohlen) Wiederholen Sie diese Schritte in jeder , AWS-Region für die Sie diesen Scantyp aktivieren möchten.

API

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

Scannen von Amazon EC2-Instances mit Amazon Inspector

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

Amazon Inspector EC2-Scan extrahiert Metadaten aus Ihrer EC2-Instance und vergleicht diese Metadaten dann mit Regeln, die aus Sicherheitsempfehlungen gesammelt wurden, um Ergebnisse zu generieren. Amazon Inspector scannt Instances auf Paketschwachstellen und auf Probleme mit der Netzwerkerreichbarkeit. Informationen zu den Arten von Erkenntnissen, die für diese Probleme erstellt wurden, finden Sie unter Typen in Amazon Inspector finden.

Amazon Inspector führt einmal alle 24 Stunden Scans der Netzwerkerreichbarkeit durch, während Paket-Schwachstellen-Scans in einem variablen Intervall durchgeführt werden, abhängig von der Scanmethode, die der Instance zugeordnet ist.

Scan-Methoden

Paket-Schwachstellenscans können mit einer agentenbasierten oder agentenlosen Scanmethode durchgeführt werden. Diese Scanmethoden bestimmen, wie und wann Amazon Inspector den Softwarebestand von einer EC2-Instance für Paket-Schwachstellenscans sammelt. Die agentenbasierte Methode benötigt den SSM-Agenten, um Softwareinventar zu erfassen, während die agentenlose Methode Amazon-EBS-Snapshots anstelle eines Agenten verwendet.

Die von Amazon Inspector verwendeten Scanmethoden hängen von der Scanmoduseinstellung Ihres Kontos ab. Weitere Informationen finden Sie unter Verwalten des Scanmodus.

Informationen zum Aktivieren von Amazon EC2-Scans finden Sie unter Aktivieren eines Scantyps.

Agentbasiertes Scannen

Agentbasierte Scans werden kontinuierlich mit dem SSM-Agenten auf allen berechtigten Instances durchgeführt. Für agentenbasierte Scans verwendet Amazon Inspector SSM-Zuordnungen und Plugins, die über diese Zuordnungen installiert wurden, um Softwarebestand von Ihren Instances zu erfassen. Zusätzlich zum Scannen von Paketschwachstellen nach Betriebssystempaketen kann das agentenbasierte Scannen von Amazon Inspector auch Paketschwachstellen für Anwendungsprogrammiersprachenpakete in Linux-basierten Instances über erkennenDetaillierte Überprüfung von Amazon Inspector für Amazon EC2-Linux-Instances.

Der folgende Prozess erklärt, wie Amazon Inspector SSM verwendet, um den Bestand zu erfassen und agentenbasierte Scans durchzuführen:

1. Amazon Inspector erstellt SSM-Zuordnungen in Ihrem Konto, um den Bestand von Ihren Instances zu erfassen. Bei einigen Instance-Typen (Windows und Linux) installieren diese Zuordnungen Plugins auf einzelnen Instances, um den Bestand zu erfassen.
2. Mit SSM extrahiert Amazon Inspector den Paketbestand aus einer Instance.
3. Amazon Inspector wertet den extrahierten Bestand aus und generiert Ergebnisse für alle erkannten Schwachstellen.

Zulässige Instances

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

- Die Instance verfügt über ein unterstütztes Betriebssystem. Eine Liste der unterstützten Betriebssysteme finden Sie in der Spalte Agent-basierte Scanunterstützung von 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 von SSM verwaltet. Anweisungen zum Überprüfen und Konfigurieren des Agenten finden Sie unter Konfigurieren des SSM-Agenten.

Kundendienstmitarbeiterbasiertes Scanverhalten

Wenn Sie die agentenbasierte Scanmethode verwenden, 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 Common Vulnerabilities and Exposures (CVE)-Element hinzufügt und dieses CVE für Ihre EC2-Instance (Linux und Mac) relevant ist.

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

Sie können überprüfen, wann eine EC2-Instance zuletzt auf der Registerkarte Instances auf der Kontoverwaltungsseite oder mit dem ListCoverage Befehl auf Schwachstellen gescannt wurde.

Konfigurieren des SSM-Agenten

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

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

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

AmazonSSMManagedInstanceCore ist die empfohlene Richtlinie, die Sie verwenden sollten, wenn Sie ein Instance-Profil anfügen. Diese Richtlinie verfügt über alle Berechtigungen, die für das Scannen von Amazon Inspector EC2 erforderlich sind.

> **Note**
>
> Sie können auch die SSM-Verwaltung all Ihrer EC2-Instances automatisieren, ohne die Verwendung von IAM-Instance-Profilen mithilfe der SSM-Standardkonfiguration für die Host-Verwaltung. Weitere Informationen finden Sie unter Standardkonfiguration für die Host-Verwaltung.

So konfigurieren Sie SSM für eine Amazon EC2-Instance

1. Wenn es noch nicht von Ihrem Betriebssystemanbieter installiert wurde, installieren Sie den SSM Agent. Weitere Informationen finden Sie unter Arbeiten mit SSM Agent.
2. Verwenden Sie die , 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 Berechtigung zum Verwalten Ihrer Instance. Sie können die Berechtigung erteilen, indem Sie ein IAM-Instance-Profil erstellen und es an Ihre Instance anfügen. Wir empfehlen die Verwendung der AmazonSSMManagedInstanceCore Richtlinie, 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 Instance-Profils mit diesen Berechtigungen und zum Anhängen an eine Instance finden Sie unter Konfigurieren von Instance-Berechtigungen für Systems Manager Systems Manager .
4. (Optional) Aktivieren Sie automatische Updates für den SSM-Agenten. Weitere Informationen finden Sie unter Automatisieren von Updates für SSM Agent.
5. (Optional) Konfigurieren Sie Systems Manager für die Verwendung eines Amazon Virtual Private Cloud (Amazon VPC)-Endpunkts. Weitere Informationen finden Sie unter Erstellen von Amazon-VPC-Endpunkten.

> **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 Zuordnung namens `InspectorInventoryCollection-do-not-delete`, wenn noch keine vorhanden ist.
> Amazon Inspector erfordert auch eine Ressourcendatensynchronisierung und erstellt automatisch eine namens `InspectorResourceDataSync-do-not-delete`, wenn noch keine vorhanden ist. Weitere Informationen finden Sie unter

Konfigurieren der Ressourcendatensynchronisierung für Inventory im AWS Systems Manager -Benutzerhandbuch. Jedes Konto kann eine festgelegte Anzahl von Ressourcendatensynchronisierungen pro Region haben. Weitere Informationen finden Sie unter Maximale Anzahl von Ressourcendatensynchronisierungen (pro AWS-Konto und Region) in SSM-Endpunkten und -Kontingenten. Wenn Sie dieses Maximum erreicht haben, müssen Sie eine Ressourcendatensynchronisierung löschen. Weitere Informationen finden Sie unter Verwalten von Ressourcendatensynchronisierungen.

Zum Scannen erstellte SSM-Ressourcen

Amazon Inspector benötigt eine Reihe von SSM-Ressourcen in Ihrem Konto, um Amazon EC2Scans auszuführen. Die folgenden Ressourcen werden erstellt, wenn Sie das Scannen von Amazon Inspector EC2 zum ersten Mal aktivieren:

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

`InspectorInventoryCollection-do-not-delete`

Dies ist eine Systems Manager State Manager (SSM)-Zuordnung, die Amazon Inspector verwendet, um den Bestand an Softwareanwendungen von Ihren Amazon EC2-Instances zu erfassen. Wenn Ihr Konto bereits über eine SSM-Zuordnung zum Erfassen von Inventar aus 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 Bestandsdaten von Ihren Amazon EC2-Instances an einen Amazon S3-Bucket zu senden, der Amazon Inspector gehört. Weitere Informationen finden Sie unter Konfigurieren der Ressourcendatensynchronisierung für Inventory im AWS Systems Manager -Benutzerhandbuch.

`InspectorDistributor-do-not-delete`

Dies ist eine SSM-Zuordnung, die Amazon Inspector zum Scannen von Windows-Instances verwendet. Diese Zuordnung installiert das Amazon Inspector SSM-Plugin auf Ihren Windows-

Instances. Wenn die Plugin-Datei versehentlich gelöscht wird, wird sie von dieser Zuordnung im nächsten Zuordnungsintervall neu installiert.

`InvokeInspectorSsmPlugin-do-not-delete`

Dies ist eine SSM-Zuordnung, die Amazon Inspector zum Scannen von Windows-Instances verwendet. Diese Zuordnung ermöglicht es Amazon Inspector, Scans mit dem Plugin zu initiieren. Sie können damit auch benutzerdefinierte Intervalle für Scans von Windows-Instances festlegen. Weitere Informationen finden Sie unter Festlegen von benutzerdefinierten Zeitplänen für Windows Instance-Scans.

`InspectorLinuxDistributor-do-not-delete`

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

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

Dies ist eine SSM-Zuordnung, die Amazon Inspector für die Amazon EC2-Linux-Deep-Inspection verwendet. Diese Zuordnung ermöglicht es Amazon Inspector, Scans mit dem Plugin zu initiieren.

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

Agentless-Scan

Amazon Inspector verwendet eine agentenlose Scanmethode auf berechtigten Instances, wenn sich Ihr Konto im Hybrid-Scanmodus befindet (dies umfasst sowohl agentenbasierte als auch agentenlose Scans). Für agentenlose Scans verwendet Amazon Inspector EBS-Snapshots, um einen Softwarebestand von Ihren Instances zu erfassen. Instances, die mit der Agentless-Methode gescannt wurden, werden sowohl auf Schwachstellen im Betriebssystempaket als auch im Anwendungsprogrammiersprachenpaket gescannt.

> **Note**
>
> Beim Scannen von Linux-Instances auf Schwachstellen im Programmiersprachenpaket der Anwendung scannt die Agentless-Methode alle verfügbaren Pfade, während das agentenbasierte Scannen nur die Standardpfade und zusätzlichen Pfade scannt, die Sie als Teil von angebenDetaillierte Überprüfung von Amazon Inspector für Amazon EC2-Linux-Instances. Dies kann dazu führen, dass dieselbe Instance unterschiedliche Ergebnisse hat, 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 erfassen und agentenlose Scans durchzuführen:

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

Zulässige Instances

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

- Die Instance verfügt über ein unterstütztes Betriebssystem. Eine Liste der unterstützten Betriebssysteme finden Sie in der Spalte Agent-basierte Scanunterstützung von 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 instance`, `Stale inventory`oder `No inventory`.
- Die Instance ist EBS-gestützt und hat eines der folgenden Dateisystemformate:
  - `ext3`
  - `ext4`

- `xfs`

Agentless-Scanverhalten

Wenn Ihr Konto für Hybrid-Scans konfiguriert ist, führt Amazon Inspector alle 24 Stunden agentenlose Scans auf berechtigten Instances durch. Amazon Inspector erkennt und scannt stündlich neu in Frage kommende Instances. Dazu gehören neue Instances ohne SSM-Agenten oder bereits vorhandene Instances mit Status, die sich in geändert haben`SSM_UNMANAGED`.

Amazon Inspector aktualisiert das Feld Letzter Scan für eine Amazon EC2-Instance, wenn es nach einem Agentless-Scan extrahierte Snapshots aus einer Instance scannt.

Sie können überprüfen, wann eine EC2-Instance zuletzt auf der Registerkarte Instances auf der Kontoverwaltungsseite oder mithilfe des ListCoverage Befehls auf Schwachstellen gescannt wurde.

Verwalten des Scanmodus

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 anzeigen. Eigenständige Konten oder delegierte Administratoren von Amazon Inspector können den Scanmodus ändern. Wenn Sie den Scanmodus als delegierten Amazon Inspector-Administrator festlegen, wird dieser Scanmodus für alle Mitgliedskonten in Ihrer Organisation festgelegt. Amazon Inspector hat die folgenden Scanmodi:

Agentbasiertes Scannen – In diesem Scanmodus verwendet Amazon Inspector ausschließlich die agentenbasierte Scanmethode, wenn auf Paketschwachstellen gescannt wird. Dieser Scanmodus scannt nur SSM-verwaltete Instances in Ihrem Konto, hat jedoch den Vorteil, kontinuierliche Scans als Reaktion auf neue CVE- oder -Änderungen an den Instances bereitzustellen. Agentbasiertes Scannen bietet auch Amazon Inspector Deep Inspector für berechtigte Instances. Dies ist der Standard-Scanmodus für neu aktivierte Konten.

Hybrides Scannen – In diesem Scanmodus verwendet Amazon Inspector eine Kombination aus agentenbasierten und agentenlosen Methoden, um nach Paketschwachstellen 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 von SSM verwaltet werden, verwendet Amazon Inspector die Agentless-Methode für berechtigte EBS-gestützte Instances.

So ändern Sie den Scanmodus

1. Öffnen Sie die Amazon 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 Seitennavigationsbereich 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.

Ausschließen von Instances von Amazon Inspector-Scans

Sie können bestimmte Instances markieren, um sie von Amazon Inspector-Scans auszuschließen. Das Ausschließen von Instances von Scans kann dazu beitragen, nicht umsetzbare Warnungen zu verhindern. Ausgeschlossene Instances werden Ihnen nicht in Rechnung gestellt.

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

- `InspectorEc2Exclusion`

Der Wert ist optional.

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

Darüber hinaus können Sie ein verschlüsseltes EBS-Volume von agentenlosen Scans ausschließen, indem Sie den AWS KMS Schlüssel, der zum Verschlüsseln dieses Volumes verwendet wird, mit dem -`InspectorEc2Exclusion`Tag markieren. Weitere Informationen finden Sie unter Markieren von Schlüsseln

Unterstützte Betriebssysteme

Amazon Inspector scannt unterstützte Mac-, Windows- und Linux-EC2-Instances auf Schwachstellen in Betriebssystempaketen. Für Linux-Instances kann Amazon Inspector Ergebnisse für Anwendungsprogrammiersprachenpakete mit erstellenDetaillierte Überprüfung von Amazon

Inspector für Amazon EC2-Linux-Instances. Bei Mac- und Windows-Instances werden nur Betriebssystempakete gescannt.

Informationen zu unterstützten Betriebssystemen, einschließlich des Betriebssystems, das ohne SSM-Agent gescannt werden kann, finden Sie unter Unterstützte Betriebssysteme für Amazon EC2-Scans.

Detaillierte Überprüfung von Amazon Inspector für Amazon EC2-Linux-Instances

Amazon Inspector erweitert seine Amazon EC2-Scanabdeckung um eine eingehende Überprüfung. Bei eingehender Überprüfung erkennt Amazon Inspector Paketschwachstellen für Anwendungsprogrammiersprachenpakete in Ihren Linux-basierten Amazon EC2-Instances.

Amazon Inspector scannt Standardpfade für Bibliotheken von Programmiersprachenpaketen. Sie können zusätzlich zu den Standardpfaden auch benutzerdefinierte Pfade konfigurieren. Weitere Informationen finden Sie unter Benutzerdefinierte Pfade für Amazon Inspector Deep Inspector.

Amazon Inspector führt Deep-Inspection-Scans mit Daten durch, die mit dem Amazon Inspector-SSM-Plugin erfasst werden. Um das Plugin zu verwalten und eine Deep-Inspection für Linux durchzuführen, erstellt Amazon Inspector automatisch die folgende SSM-Zuordnung `InvokeInspectorLinuxSsmPlugin-do-not-delete` in Ihrem Konto. Dies tritt auf, wenn Amazon Inspector die Deep Inspection aktiviert.

Amazon Inspector sammelt alle 6 Stunden aktualisiertes Anwendungsinventar von Instances zur eingehenden Überprüfung.

Eine Liste der Programmiersprachen, die Amazon Inspector für die detaillierte Überprüfung unterstützt, finden Sie unter Unterstützte Programmiersprachen: Amazon EC2 Deep Inspect.

> **Note**
>
> Eine gründliche Prüfung wird für Windows- oder Mac-Instances nicht unterstützt.

Aktivieren oder Deaktivieren von Deep Inspect

> **Note**
>
> Die detaillierte Überprüfung wird im Rahmen des Amazon EC2-Scans für Konten, die Amazon Inspector nach dem 17. April 2023 aktivieren, automatisch aktiviert.

Sie können überprüfen, ob eine Deep Inspect für ein Konto in der Amazon Inspector-Konsole in der Amazon EC2-Scanspalte auf der Kontoverwaltungsseite aktiv ist. Wenn Deep Inspect nicht aktiv ist, wird in dieser Spalte Aktiviert (Deep Inspect deaktiviert) angezeigt. Um den Aktivierungsstatus programmgesteuert zu überprüfen, verwenden Sie die GetEc2DeepInspectionConfiguration-API. Oder verwenden Sie für mehrere Konten die BatchGetMemberEc2DeepInspectionStatus-API.

Wenn Sie Amazon Inspector vor dem 17. April 2023 aktiviert haben, können Sie die eingehende Überprüfung über das Konsolenbanner oder die UpdateEc2DeepInspectionConfiguration API aktivieren. Wenn Sie der delegierte Administrator für eine Organisation in Amazon Inspector sind, können Sie die BatchUpdateMemberEc2DeepInspectionStatus API verwenden, um sie für sich selbst und Ihre Mitgliedskonten zu aktivieren.

Sie können Deep Inspect über die UpdateEc2DeepInspectionConfiguration API deaktivieren. Mitgliedskonten in einer Organisation können die eingehende Überprüfung nicht deaktivieren. Stattdessen muss das Mitgliedskonto von seinem delegierten Administrator mithilfe der BatchUpdateMemberEc2DeepInspectionStatus API deaktiviert werden.

Informationen zum Amazon Inspector SSM-Plugin für Linux

Amazon Inspector verwendet das Amazon Inspector SSM-Plugin, um eine gründliche Überprüfung 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 EC2Instance bereitzustellen. Systems Manager Distributor unterstützt die Betriebssysteme, die im Systems Manager-Handbuch als Unterstützte Paketplattformen und Architekturen aufgeführt sind. Das Betriebssystem Ihrer Amazon EC2-Instance muss vom Systems

Manager Distributor und Amazon Inspector unterstützt werden, damit Amazon Inspector Deep-Inspection-Scans durchführen kann.

Amazon Inspector erstellt die folgenden Dateiverzeichnisse, um Daten zu verwalten, die für die Deep-Amazon Inspector-SSM-Plug-In gesammelt wurden:

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - Der `packages.txt` in diesem Verzeichnis speichert die vollständigen Pfade zu Paketen, die bei der eingehenden Überprüfung entdeckt wurden. Wenn Amazon Inspector dasselbe Paket auf Ihrer Instance mehrfach erkannt 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 .

Deinstallieren des Amazon Inspector SSM-Plugins

Wenn die `inspectorssmplugin` Datei versehentlich gelöscht wird, versucht die `InspectorLinuxDistributor-do-not-delete` SSM-Zuordnung, das Plugin im nächsten Scanintervall neu zu installieren.

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

Benutzerdefinierte Pfade für Amazon Inspector Deep Inspector

Sie können benutzerdefinierte Pfade für Amazon Inspector konfigurieren, um zu suchen, wenn es eine gründliche Überprüfung Ihrer Linux-Amazon EC2 durchführt. Wenn Sie einen benutzerdefinierten Pfad hinzufügen, sucht Amazon Inspector nach Paketen in diesem Verzeichnis und allen Unterverzeichnissen darin.

Alle Konten können bis zu 5 benutzerdefinierte Pfade für ihr einzelnes 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 wurden.

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 zugeordneten Netzwerkpfade wie Network File System (NFS)-Mounts oder Amazon 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 Paketlimit von 5 000 pro Instance und ein maximales Zeitlimit für die Erfassung von Paketinventaren von 15 Minuten. Wir empfehlen Ihnen, zu versuchen, benutzerdefinierte Pfade auszuwählen, um diese Grenzwerte zu vermeiden.

Festlegen eines benutzerdefinierten Pfads in der Konsole

Console

Melden Sie sich als delegierter Amazon Inspector-Administrator an und führen Sie die folgenden Schritte aus, um benutzerdefinierte Pfade für Ihre Organisation hinzuzufügen.

1. Öffnen Sie die Amazon 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 Seitennavigationsbereich 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 einzelnes 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 in seine nächste eingehende Überprüfung einbeziehen.

API

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

Unterstützte Programmiersprachen

Bei Linux-Instances kann Amazon Inspector Deep Inspector zusätzlich zu Schwachstellen in Betriebssystempaketen Ergebnisse für Anwendungsprogrammiersprachen liefern. Bei Mac- und Windows-Instances werden nur Betriebssystempakete gescannt.

Informationen zu unterstützten Programmiersprachen finden Sie unter Unterstützte Programmiersprachen für Amazon Inspector Deep Inspector.

Scannen von Windows EC2-Instances mit Amazon Inspector

> **Note**
>
> Am 31. August 2022 erweiterte Amazon Inspector seine Scanabdeckung für Amazon EC2 um EC2-Instances, auf denen ausgeführt wirdWindows.

Amazon Inspector erkennt automatisch alle Windows unterstützten Instances und schließt sie ohne zusätzliche Aktionen in das kontinuierliche Scannen ein. Informationen darüber, welche Instances unterstützt werden, finden Sie unter Unterstützte 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 der Erkennung und dann alle 6 Stunden gescannt. Das standardmäßige 6-stündige Scanintervall ist jedoch einstellbar. Weitere Informationen finden Sie unter Festlegen von benutzerdefinierten Zeitplänen für Windows Instance-Scans. Im Folgenden finden Sie eine Übersicht darüber, wie Amazon Inspector Windows Instances scannt:

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

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

Scananforderungen für Amazon Inspector für Windows Instances

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

- Die Instance ist eine von SSM verwaltete Instance. Anweisungen zum Einrichten Ihrer Instance zum Scannen finden Sie unter Konfigurieren des SSM-Agenten.
- Das Instance-Betriebssystem ist eines der Windows unterstützten Betriebssysteme. Eine vollständige Liste der unterstützten Betriebssysteme finden Sie unter Unterstützte Betriebssysteme für Amazon EC2-Scans.
- Auf der Instance ist das Amazon Inspector SSM-Plugin installiert. Amazon Inspector installiert bei der Erkennung automatisch das Amazon Inspector SSM-Plugin für verwaltete Instances. Weitere Informationen zum Plugin finden Sie im nächsten Thema.

> **Note**
>
> Wenn Ihr Host in einer Amazon VPC ohne ausgehenden Internetzugang ausgeführt wird, erfordert das Windows Scannen, dass Ihr Host auf regionale Amazon S3-Endpunkte zugreifen kann. Informationen zum Konfigurieren eines Amazon 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 speziell den Zugriff auf den von Amazon Inspector verwalteten Bucket in Ihrem zulassen AWS-Region , in dem die OVAL-Definitionen gespeichert sind, die zur Bewertung Ihrer Instance verwendet werden. Dieser Bucket hat das folgende Format: `inspector2-oval-prod-`*`REGION`*.

Informationen zum 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 heißt `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 einer niedrigeren als der normalen Priorität ausgeführt.

Deinstallieren des Amazon Inspector SSM-Plugins

Wenn die `InspectorSsmPlugin.exe` Datei versehentlich gelöscht wird, installiert die `InspectorDistributor-do-not-delete` SSM-Zuordnung das Plugin im nächsten Windows Scanintervall neu. Wenn Sie das Amazon Inspector-SSM-Plugin deinstallieren möchten, können Sie die Deinstallationsaktion 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, bleibt 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 Deaktivieren von Amazon Inspector.

Festlegen von benutzerdefinierten Zeitplänen für Windows Instance-Scans

Sie können die Zeit zwischen Ihren Windows Amazon EC2-Instance-Scans anpassen, indem Sie mithilfe von SSM einen Cron-Ausdruck oder Rate-Ausdruck für die `InvokeInspectorSsmPlugin-do-not-delete` Zuordnung 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 aus den folgenden Windows Codebeispielen aus, um die Scanfrequenz für Instances mithilfe eines Ratenausdrucks oder eines Cron-Ausdrucks von den standardmäßigen 6 Stunden auf 12 Stunden zu ändern.

In den folgenden Beispielen müssen Sie die AssociationId für die Zuordnung mit dem Namen verwenden`InvokeInspectorSsmPlugin-do-not-delete`. Sie können Ihre abrufen, AssociationId indem 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**
>
> Die AssociationId ist regional, daher müssen Sie zuerst eine eindeutige ID für jede abrufen AWS-Region. Anschließend können Sie den Befehl ausführen, um die Scan-Taktfrequenz 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-Images mit Amazon Inspector

Amazon Inspector scannt Container-Images, die in Amazon ECR gespeichert sind, auf Softwareschwachstellen, um Erkenntnisse zur Paketschwachstelle zu generieren. Informationen

zu den Arten von Erkenntnissen, die für diese Probleme erstellt wurden, finden Sie unter Typen 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. Dies ersetzt das standardmäßige einfache Scannen, das von Amazon ECR kostenlos bereitgestellt wird, durch das erweiterte Scannen von , das über Amazon Inspector bereitgestellt und abgerechnet wird.

Das erweiterte Scannen von Amazon Inspector bietet Ihnen den Vorteil des Schwachstellenscans sowohl für Betriebssystem- als auch für Programmiersprachenpakete auf Registrierungsebene. Sie können die mithilfe des erweiterten Scannens auf Image-Ebene für jede Image-Ebene auf der Amazon-ECR-Konsole entdeckten Erkenntnisse überprüfen. Darüber hinaus können Sie diese Erkenntnisse in anderen Services überprüfen und damit arbeiten, die nicht für grundlegende Scanergebnisse verfügbar sind, einschließlich AWS Security Hub und Amazon EventBridge. Sie können die von Scans entdeckten Erkenntnisse in der Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home anzeigen. Informationen zum Arbeiten mit Erkenntnissen finden Sie unter Verwalten von Erkenntnissen in Amazon Inspector.

Anweisungen zum Aktivieren von Amazon-ECR-Scans finden Sie unter Aktivieren eines Scantyps.

Scan-Verhaltensweisen 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 berechtigten Images, 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-Wiederscandauer gepusht oder abgerufen wurden. Weitere Informationen finden Sie unter Konfigurieren der Dauer des erneuten ECR-Scans.

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

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

Wenn Sie Ihr Repository für das Scannen beim Push konfigurieren, werden Images nur gescannt, wenn Sie sie pushen.

Sie können überprüfen, wann ein Container-Image zuletzt auf der Registerkarte Container-Images auf der Seite Kontoverwaltung oder mithilfe der ListCoverage API auf Schwachstellen überprüft wurde. Amazon Inspector aktualisiert das Feld Zuletzt gescannt eines Amazon-ECR-Images als Reaktion auf die folgenden Ereignisse:

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

Unterstützte Betriebssysteme und Medientypen

Informationen zu unterstützten Betriebssystemen finden Sie unter Unterstützte 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-Images und -`DockerV2ListMediaTypeImages` werden nicht unterstützt.

Konfigurieren des erweiterten Scannens für Amazon-ECR-Repositorys

Wenn Sie Amazon Inspector für Amazon-ECR-Container-Images aktivieren, ändern Sie die Scankonfigurationseinstellung für Ihre private Registrierung. Der Scantyp für Ihre Registrierung wird von Einfaches Scannen in Erweitertes Scannen von Amazon Inspector geändert. Weitere Informationen finden Sie unter Scannen von Bildern im Amazon-ECR-Benutzerhandbuch.

Sie können Einstellungen für erweitertes Scannen auf Repository-Ebene in ECR verwalten. Sie können kontinuierliches Scannen oder Push-Scan für Ihre Repositorys wählen. Kontinuierliches Scannen umfasst Push-Scans und automatisierte erneute Scans. Scans bei Push-Scans werden nur gescannt, wenn Sie ein Image zum ersten Mal pushen. Für beide Optionen können Sie den Scanbereich durch Einschlussfilter verfeinern. Wenn Sie das erweiterte Scannen zum ersten Mal aktivieren, werden Ihre Einstellungen standardmäßig auf Kontinuierliches Scannen aller Repositorys festgelegt.

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 zu scannenden Repositorys befinden.
3. Wählen Sie im Navigationsbereich Private Registrierung und dann Scannen aus.
4. Stellen Sie unter Scantyp sicher, dass Erweitertes Scannen ausgewählt ist. Wenn dies nicht der Fall ist, wählen Sie Erweitertes Scannen aus.

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

Weitere Informationen zur Konfiguration erweiterter Scans finden Sie unter Verwenden von erweitertem Scannen im Amazon-ECR-Benutzerhandbuch.

Konfigurieren der Dauer des erneuten ECR-Scans

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

Dauer des Image-Push-Datums

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

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

Dauer des Image-Pull-Datums

Die Dauer des Image-Pull-Datums bestimmt, wie lange Amazon Inspector Images nach dem letzten Pull-Datum kontinuierlich überwacht. Die folgenden Optionen sind als Wiederholungsscan-Dauer verfügbar:

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

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

> **Note**
>
> Wenn Amazon Inspector die Überwachung eines Images beendet, wird der Statuscode des Image-Scans auf `inactive` und der Ursachencode auf gesetzt`expired`. Anschließend werden alle zugehörigen Image-Ergebnisse geschlossen.

Legen Sie die Dauer des erneuten Scannens so fest, dass sie Ihrer Umgebung am besten entspricht. Wenn Sie beispielsweise häufig Images erstellen, wählen Sie eine kürzere Scandauer. Wenn Sie Bilder über einen längeren Zeitraum verwenden, wählen Sie eine längere Scandauer aus.

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

So konfigurieren Sie die Dauer des erneuten ECR-Scans

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

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

Scannen von AWS Lambda Funktionen mit Amazon Inspector

Amazon Inspector bietet AWS Lambda kontinuierliche, automatisierte Schwachstellenbewertungen für Lambda-Funktionen und -Ebenen. Amazon Inspector bietet zwei Arten des Scannens nach Lambda. Diese Scantypen suchen nach verschiedenen Arten von Schwachstellen.

Amazon Inspector Lambda-Standardscan

Dies ist der standardmäßige Lambda-Scantyp. Lambda-Standardscan scannt Anwendungsabhängigkeiten innerhalb einer Lambda-Funktion und ihrer Ebenen auf Paketschwachstellen. Weitere Informationen finden Sie unter Lambda-Standardscan.

Codescan von Amazon Inspector Lambda

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 Codescan von Amazon Inspector Lambda.

Wenn Sie das Scannen von Lambda 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 auf Scans zu überwachen. Weitere Informationen zu serviceverknüpften Kanälen finden Sie unter Anzeigen von serviceverknüpften Kanälen für CloudTrail mithilfe der AWS CLI .

> **Note**
>
> Die von Amazon Inspector erstellten serviceverknüpften Kanäle ermöglichen es Ihnen, CloudTrail Ereignisse in Ihrem Konto so zu sehen, als hätten Sie einen CloudTrail Trail. Wir empfehlen Ihnen jedoch, Ihre eigenen zu erstellen, CloudTrail um Ereignisse für Ihr Konto zu verwalten.

Anweisungen zum Aktivieren von Lambda-Funktionsscans finden Sie unter Aktivieren eines Scantyps.

Scanverhalten für das Scannen von 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 überprüfen, wann eine Lambda-Funktion zuletzt auf der Registerkarte Lambda-Funktionen auf der Seite Kontoverwaltung oder mithilfe der ListCoverage API auf Schwachstellen überprüft wurde. 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 abgeschlossen hat.
- Wenn eine Lambda-Funktion aktualisiert wird.
- Wenn Amazon Inspector eine Lambda-Funktion erneut scannt, weil der Amazon Inspector-Datenbank ein neues CVE-Element hinzugefügt wurde, das sich auf diese Funktion auswirkt.

Unterstützte Laufzeiten und berechtigte Funktionen

Amazon Inspector unterstützt verschiedene Laufzeiten für Lambda-Standardscan und Lambda-Codescan. Eine Liste der unterstützten Laufzeiten für jeden Scantyp finden Sie unter Unterstützte Laufzeiten: Amazon Inspector Lambda-Standardscan und Unterstützte Laufzeiten: Codescan von Amazon Inspector Lambda.

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 mit gekennzeichnet`$LATEST`.
- Die Funktion wird nicht von Scans durch 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.

Amazon Inspector Lambda-Standardscan

Amazon Inspector Lambda-Standardscan identifiziert Softwareschwachstellen in den Anwendungspaketabhängigkeiten, die Sie Ihrem Lambda-Funktionscode und Ihren Ebenen hinzufügen. Wenn Ihre Lambda-Funktion beispielsweise eine Version des `python-jwt` Pakets mit einer bekannten Schwachstelle verwendet, generiert das Lambda-Standardscan ein Ergebnis für diese Funktion.

Wenn Amazon Inspector eine Schwachstelle in den Abhängigkeiten Ihres Lambda-Funktionsanwendungspakets erkennt, erzeugt Amazon Inspector eine detaillierte Erkenntnis zum Typ der Paketschwachstelle.

Anweisungen zum Aktivieren eines Scantyps finden Sie unter Aktivieren eines Scantyps.

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

> **Note**
>
> Durch die Deaktivierung des Amazon-Amazon Inspector-Lambda-Standardscans wird auch Amazon Inspector-Lambda-Codescan deaktiviert.

Ausschließen von Funktionen vom Lambda-Standardscan

Sie können bestimmte Funktionen markieren, um sie von Amazon Inspector-Lambda-Standardscans auszuschließen. Das Ausschließen von Funktionen von Scans kann dazu beitragen, nicht umsetzbare Warnungen zu verhindern.

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

- Schlüssel:`InspectorExclusion`

- Wert:`LambdaStandardScanning`

So schließen Sie eine Funktion vom Lambda-Standardscan aus

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

Codescan von Amazon Inspector Lambda

> **Important**
>
> Codescan erfasst Codeausschnitte von Lambda-Funktionen, um erkannte Schwachstellen hervorzuheben. Diese Ausschnitte können fest codierte Anmeldeinformationen oder andere sensible Materialien im Klartext anzeigen.

Amazon Inspector Lambda-Codescan scannt den benutzerdefinierten Anwendungscode innerhalb einer Lambda-Funktion auf Code-Schwachstellen basierend auf bewährten AWS Sicherheitsmethoden. Lambda-Codescans können Injektionsfehler, Datenlecks, schwache Kryptografie oder fehlende Verschlüsselung in Ihrem Code erkennen. Informationen zu den verfügbaren Regionen finden Sie unter Verfügbarkeit regionsspezifischer Feature.

Lambda-Standardscan ist eine Funktion, die die Anwendungspaketabhängigkeiten auswertet, die in einer Funktion auf häufige Schwachstellen und Risiken (CVE) verwendet werden. Sie können das Scannen von Lambda-Code zusammen mit dem Lambda-Standardscan aktivieren.

Amazon Inspector wertet Ihren Lambda-Funktionsanwendungscode mithilfe von automatisiertem Denken und Machine Learning aus, das Ihren Anwendungscode auf allgemeine Sicherheitskonformität analysiert. Es identifiziert Richtlinienverstöße und Schwachstellen 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 Schwachstelle in Ihrem Lambda-Funktionsanwendungscode erkennt, erzeugt Amazon Inspector eine detaillierte Erkenntnis zum Typ der Codeschwachstelle. Dieser Erkenntnistyp enthält den genauen Speicherort des Problems im Code, einen Codeausschnitt, der das Problem zeigt, und vorgeschlagene Behebung. Die vorgeschlagene Abhilfe umfasst plug-and-play Codeblöcke, mit denen Sie Ihre anfälligen Codezeilen ersetzen können. Diese vorgeschlagenen Codekorrekturen werden zusätzlich zu den allgemeinen Anleitungen zur Codekorrektur für diese Erkenntnis bereitgestellt.

> **Important**
>
> Vorschläge zur Codekorrektur basieren auf automatisierten Argumenten und generativen Services für künstliche Intelligenz und funktionieren daher möglicherweise nicht wie vorgesehen. Sie sind für die Vorschläge zur Codekorrektur verantwortlich, die Sie ergreifen. Überprüfen Sie immer Vorschläge zur Codekorrektur, bevor Sie sie übernehmen. Möglicherweise müssen Sie Änderungen an Vorschlägen zur Codekorrektur vornehmen, um sicherzustellen, dass Ihr Code wie beabsichtigt funktioniert. Bitte lesen Sie die Richtlinie für verantwortliche KI .

Verschlüsseln Ihres Codes in Ergebnissen zu Code-Schwachstellen

Codeausschnitte, die im Zusammenhang mit einer Code-Schwachstellen-Erkenntnis mithilfe des Lambda-Codescans erkannt wurden, werden vom CodeGuru Service gespeichert. Standardmäßig wird ein -AWS eigener Schlüssel, der von kontrolliert CodeGuru wird, verwendet, um Ihren Code zu verschlüsseln. 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 Code in Ihren Ergebnissen

Das Scannen von Lambda-Code kann zusammen mit dem Lambda-Standardscan aktiviert werden. Anweisungen zum Aktivieren eines Scantyps finden Sie unter Aktivieren eines Scantyps.

Ausschließen von Funktionen vom Lambda-Codescan

Sie können bestimmte Funktionen markieren, um sie von Code-Scans von Amazon Inspector Lambda auszuschließen. Das Ausschließen von Funktionen von Scans kann dazu beitragen, nicht umsetzbare Warnungen zu verhindern.

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

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

So schließen Sie eine Funktion vom Scannen von Lambda-Code aus

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 Tabelle Funktionen den Namen einer Funktion aus, die Sie vom Codescan von Amazon Inspector Lambda ausschließen möchten.
4. Wählen Sie Konfiguration und dann Tags aus dem Menü aus.
5. Wählen Sie Tags verwalten und dann Neues Tag hinzufügen aus.
6. Geben Sie im Feld Schlüssel ein und geben Sie `InspectorCodeExclusion`dann im Feld Wert ein`LambdaCodeScanning`.
7. Wählen Sie Speichern aus, um das Tag hinzuzufügen und Ihre Funktion vom Codescan von Amazon Inspector Lambda auszuschließen.

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

Deaktivieren eines Scantyps

Sie können einen neuen Scantyp von Amazon Inspector jederzeit deaktivieren. Wenn Sie einen Scantyp deaktivieren, verlieren Sie den Zugriff auf alle vorhandenen Erkenntnisse, die von diesem Scantyp erstellt wurden. Wenn Sie den Scantyp reaktivieren, werden Ihre berechtigten Ressourcen gescannt und Amazon Inspector generiert 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 in diesem AWS Konto auftreten. Im Folgenden sind die Änderungen aufgeführt, die auftreten, wenn Sie diese Scantypen deaktivieren:

- Amazon EC2-Scan – Wenn Sie Amazon EC2-Scannen von Amazon Inspector für ein Konto deaktivieren, werden die folgenden von Amazon Inspector verwendeten SSM-Zuordnungen 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 über diese Zuordnung installierte Amazon Inspector SSM-Plugin von allen Ihren Windows Hosts entfernt. Weitere Informationen finden Sie unter Scannen von Windows Instances.
- Amazon-ECR-Scan – Wenn Sie das Scannen von Amazon-ECR-Container-Images für ein Konto deaktivieren, ändert sich der Amazon-ECR-Scantyp für dieses Konto von Erweitertes Scannen mit Amazon Inspector zu Einfaches Scannen mit Amazon ECR.
- Lambda-Standardscan – Wenn Sie das Lambda-Standardscannen in einem Konto deaktivieren, wird das Lambda-Codescan deaktiviert, wenn das Codescann ebenfalls aktiv war. Darüber hinaus wird der CloudTrail serviceverknüpfte Kanal, der beim Aktivieren des Scannens erstellt wurde, gelöscht.

Deaktivieren von Scans

Durch die Deaktivierung aller Scantypen für ein Konto wird Amazon Inspector für dieses Konto in dieser deaktiviert AWS-Region. Weitere Informationen finden Sie unter Deaktivieren von Amazon Inspector.

Um dieses Verfahren für eine Umgebung mit mehreren Konten abzuschließen, führen Sie diese Schritte aus, während Sie als delegierter Administrator von Amazon Inspector angemeldet sind.

Console

So deaktivieren Sie Scans

1. Öffnen Sie die Amazon 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 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 dann unter den Optionen Deaktivieren den Scantyp aus, den Sie deaktivieren möchten.
7. (Empfohlen) Wiederholen Sie diese Schritte in jeder , AWS-Region für die Sie diesen Scantyp deaktivieren möchten.

API

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

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

Wenn Sie das Scannen von Amazon Inspector EC2 für ein Konto aktivieren, ermöglichen Sie Amazon Inspector, CIS-Scans durchzuführen oder zu planen. Amazon-Amazon Inspector-CIS-Scans vergleichen die Betriebssysteme Ihrer Amazon EC2-Instances, um festzustellen, ob sie gemäß den vom Center for Internet Security festgelegten Empfehlungen für bewährte Methoden konfiguriert sind. Das Programm CIS Security Benchmarks 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-Ziel-Instances basierend auf den Instance-Tags und dem Scan-Zeitplan durch, die Sie in einer Scan-Konfiguration definieren. Für jede Ziel-Instance führt Amazon Inspector eine Reihe von Prüfungen für die Instance durch. Bei jeder Prüfung wird geprüft, ob Ihre Systemkonfiguration einer bestimmten CIS-Benchmark-Empfehlung entspricht. Jede Prüfung hat eine CIS-Prüfungs-ID und einen Titel, die direkt mit einer CIS-Benchmark-Empfehlung für diese Plattform korreliert. Wenn ein Scan abgeschlossen ist, können Sie die Ergebnisse anzeigen 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, verlangt Amazon Inspector, 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 unter Unterstützte Betriebssysteme: CIS-Scan.
- Die Instance ist eine von Amazon EC2 Systems Manager (SSM) verwaltete Instance. Weitere Informationen finden Sie unter Arbeiten mit SSM Agent.
- 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 zum Verwalten der Instance erteilt, und Amazon Inspector zum Ausführen von CIS-Scans für diese Instance. Um diese Berechtigungen zu erteilen, fügen Sie die Richtlinien AmazonInspector2FullAccess,

AmazonSSMManagedInstanceCore und AmazonInspector2ManagedCispolicy einer IAM-Rolle an und fügen Sie diese Rolle als Instance-Profil an Ihre Instance an. Anweisungen zum Erstellen und Anhängen eines Instance-Profils finden Sie unter Arbeiten mit IAM-Rollen im Amazon EC2-Benutzerhandbuch.

> **Note**
>
> Die Aktivierung von Amazon Inspector Deep Inspector ist keine Voraussetzung mehr, wenn ein CIS-Scan auf einer Instance ausgeführt wird. Wenn Sie Deep Inspector deaktivieren, installiert Amazon Inspector weiterhin den SSM-Agenten, aber das Plugin wird nicht mehr aufgerufen, um Deep Inspect auszuführen. Das bedeutet, dass die folgende Zuordnung in Ihrem Konto vorhanden ist: `InspectorLinuxDistributor-do-not-delete`.

Ausführen von CIS-Scans

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

Wenn Sie eine Scankonfiguration erstellen, geben Sie Tag-Schlüssel-Wert-Paare an, die für Ziel-Instances verwendet werden sollen. Wenn Sie der delegierte Amazon Inspector-Administrator für eine Organisation sind, können Sie mehrere Konten in der Scankonfiguration angeben, und Amazon Inspector sucht nach Instances mit den angegebenen Tags in jedem dieser Konten. Sie wählen die CIS-Benchmark-Ebene für den Scan aus. Für jeden Benchmark unterstützt CIS ein Profil der Stufen 1 und 2, das Grundlagen für verschiedene Sicherheitsebenen bereitstellt, die verschiedene Umgebungen möglicherweise benötigen.

- Stufe 1 – empfiehlt grundlegende grundlegende Sicherheitseinstellungen, die auf jedem System konfiguriert werden können. Die Implementierung dieser Einstellungen sollte zu einer geringen oder gar keiner Serviceunterbrechung führen. Ziel dieser Empfehlungen ist es, die Anzahl der Einstiegspunkte in Ihre Systeme zu reduzieren und Ihre gesamten Cybersicherheitsrisiken zu reduzieren.
- Stufe 2 – empfiehlt erweiterte Sicherheitseinstellungen für Hochsicherheitsumgebungen. Die Implementierung dieser Einstellungen erfordert Planung und Koordination, um das Risiko von Auswirkungen auf das Geschäft zu minimieren. Ziel dieser Empfehlungen ist es, Ihnen zu helfen, die Einhaltung gesetzlicher Vorschriften zu erreichen.

Stufe 2 erweitert Stufe 1. Wenn Sie Stufe 2 wählen, prüft Amazon Inspector auf alle Konfigurationen, die für Stufe 1 und Stufe 2 empfohlen werden.

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

> **Tip**
>
> Wir empfehlen, einen Tag und eine Uhrzeit auszuwählen, die sich am wenigsten auf Ihr System auswirken, während der Scan ausgeführt wird.

So erstellen Sie eine CIS-Scankonfiguration

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit dem AWS-Region Selektor in der oberen rechten Ecke der Seite die aus, AWS-Region in der 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 Scan-Konfigurationsnamen ein.
    b. Geben Sie für Zielressource den Schlüssel und den entsprechenden Wert eines Tags auf den Instances 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 eine CIS-Benchmark-Ebene aus. Sie können Stufe 1 für grundlegende Sicherheitskonfigurationen oder Stufe 2 für erweiterte Sicherheitskonfigurationen auswählen.
5. Geben Sie für Zielkonten an, welche Konten in den Scan aufgenommen werden sollen. Ein eigenständiges Konto oder Mitglied in einer Organisation kann sich selbst auswählen, um eine Scankonfiguration für ihr Konto zu erstellen. Ein delegierter Amazon Inspector-Administrator kann Alle Konten auswählen, um alle Konten innerhalb der Organisation anzuvisieren, oder Konten angeben auswählen und eine Teilmenge der Mitgliedskonten angeben, auf die abgezielt werden soll. Der delegierte Administrator kann `SELF` anstelle einer Konto-ID eingeben, um eine

Scankonfiguration 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 aus. Wählen Sie zwischen Einmaliger Scan, der ausgeführt wird, sobald Sie die Scankonfiguration abgeschlossen haben, oder Wiederkehrende Scans, der zu dem von Ihnen ausgewählten geplanten Zeitpunkt ausgeführt wird, bis er gelöscht wird.
7. Wählen Sie Erstellen, um die Erstellung der Scankonfiguration abzuschließen.

Anzeigen und Bearbeiten von CIS-Scankonfigurationen

Sie können Ihre zuvor geplanten Scans jederzeit anzeigen oder bearbeiten.

So zeigen Sie eine CIS-Scankonfiguration an oder bearbeiten sie

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

Anzeigen von Ergebnissen aus Ihren CIS-Scans

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

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

Nach Prüfungen aggregierte Scanergebnisse

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

Nach Ressource aggregierte Scanergebnisse

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

So zeigen Sie Scanergebnisse an

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit dem AWS-Region Selektor in der oberen rechten Ecke der Seite die aus, AWS-Region in der Sie die Scanergebnisse anzeigen möchten.
3. Wählen Sie im Navigationsbereich unter On-Demand-Scans die Option CIS-Scans aus.
4. Wählen Sie die ID des Scans, für den Sie Ergebnisse anzeigen möchten, aus der Spalte Scan-ID aus.
5. Wählen Sie aus, wie Sie Ihre Scanergebnisse anzeigen möchten:
    - Wählen Sie die Registerkarte Prüfungen aus, um die Scanergebnisse anzuzeigen, die nach Prüfungen aggregiert sind.
        - Wählen Sie für eine aufgeführte Prüfung eine Zahl aus bestanden, übersprungen oder fehlgeschlagen in der Spalte Ressourcenstatus aus, um eine Ansicht der nach diesem Status und dieser Prüfung gefilterten Ressourcen zu öffnen.
    - Wählen Sie die Registerkarte Gescannte Ressourcen aus, um die nach Ressourcen aggregierten Scanergebnisse anzuzeigen.
        - Wählen Sie eine Ressource aus, um ein Detailfenster 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 API herunterladen.

So laden Sie Scanergebnisse herunter

1. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home.
2. Wählen Sie mit dem AWS-Region Selektor in der oberen rechten Ecke der Seite die aus, AWS-Region in der Sie die Scanergebnisse anzeigen möchten.
3. Wählen Sie im Navigationsbereich unter On-Demand-Scans die Option CIS-Scans aus.
4. Wählen Sie die ID des Scans, für den Sie Ergebnisse anzeigen möchten, aus der Spalte Scan-ID aus.
5. Wählen Sie Herunterladen aus. Wenn Sie der delegierte Administrator sind, können Sie die Ergebnisse für bestimmte Mitgliedskonten herunterladen.

Überlegungen zur Verwaltung von Amazon Inspector CIS-Scans in einer AWS Organisation

Wenn Sie CIS-Scans innerhalb einer Organisation ausführen, interagieren Mitgliedskonten und delegierte Administratoren von Amazon Inspector 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, besitzt die Organisation diese Scan-Konfiguration. Unabhängig davon, welches Konto der aktuelle delegierte Administrator ist, kann Scankonfigurationen verwalten, die der Organisation gehören, auch wenn sie von einem anderen Konto erstellt wurden. CIS-Scankonfigurationen, die der Organisation gehören, verfügen über einen ARN, der die Organisations-ID als Eigentümer auflistet, gemäß dem Muster: `arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId`*. Die Konto-ID ist die ID des Organizations-Verwaltungskontos.

> **Important**
>
> Sie können CIS-Scankonfigurationen, die der Organisation gehören, keine Tags hinzufügen.

Wenn ein delegierter Administrator eine Scankonfiguration erstellt und `SELF` als Zielkonto angibt, besitzt sein Konto diese Scankonfiguration. Auch wenn sie ihre Organisation verlassen, können sie diese Scankonfiguration weiterhin verwalten.

> **Note**
>
> Ein delegierter Administrator kann die Ziele einer Scankonfiguration, die auf abzielt, nicht ändern`SELF`.

Scan-Konfigurationen, die von Mitgliedskonten, eigenständigen Konten oder delegierten Administratoren mit `SELF` als Ziel erstellt wurden, gehören dem Konto, das sie erstellt hat. Diese CIS-Scankonfigurationen verfügen über einen ARN, der dieses Konto als Eigentümer nach dem Muster 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 Scankonfigurationen anzeigen, die von Mitgliedern erstellt wurden, sie aber nicht bearbeiten oder löschen. Wenn ein Mitgliedskonto die Organisation verlässt, kann der delegierte Administrator keine Scankonfigurationen mehr sehen, die von diesem Konto erstellt wurden.

Der delegierte Administrator kann die Scanergebnisse jedes Kontos in der Organisation anzeigen, einschließlich der von Mitgliedern geplanten. Ein Mitgliedskonto kann die Ergebnisse aller CIS-Scans nach Ressourcen in seinem Konto anzeigen, einschließlich der vom delegierten Administrator geplanten.

Amazon Inspector-eigene Amazon S3-Buckets, die für Amazon Inspector-CIS-Scans verwendet werden

Amazon Inspector Stages hat die Open Vulnerability and Assessment Language (OVAL)-Definitionsdateien aktualisiert, die für CIS-Scans erforderlich sind. Die folgende Tabelle listet alle Amazon-SAmazon S3-Buckets im Besitz von Amazon Inspector mit OVAL-Definitionen auf, die CIS Scan pro unterstütztem verwendet AWS-Region. Die Buckets sollten bei Bedarf in VPCs auf die Zulassungsliste gesetzt werden.

> **Note**
>
> Die Details für jeden der folgenden Amazon-SAmazon S3-Buckets im Besitz von Amazon Inspector können sich nicht ändern. Die Liste wird jedoch möglicherweise aktualisiert, um die neue Unterstützung für neue widerzuspiegeln AWS-Regionen. Sie können diese

Buckets nicht für andere Amazon S3-Operationen oder in Ihren eigenen Amazon S3-Buckets verwenden.

CIS-Bucket	AWS-Region
`cis-datasets-prod-arn-5908f6f`	Europe (Stockholm)
`cis-datasets-prod-bah-8f88801`	Middle East (Bahrain)
`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-Bucket	AWS-Region
`cis-datasets-prod-osu-5bead6f`	AWS GovCloud (USA-Ost)
`cis-datasets-prod-pdt-adadf9c`	AWS GovCloud (USA-West)
`cis-datasets-prod-pdx-acfb052`	USA West (Oregon)
`cis-datasets-prod-sfo-1515ba8`	USA West (Nordkalifornien)
`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 Bewertung und Interpretation der Abdeckung Ihrer AWS Umgebung durch Amazon Inspector zu helfen, bietet die Seite Kontoverwaltung in der Amazon Inspector-Konsole Statistiken und Details zum Status des Scannens von Amazon Inspector für Ihre Konten und Ressourcen. Auf dieser Seite können Sie aggregierte Statistiken und andere Daten für Ihre Ressourcen überprüfen. Sie können auch eine detaillierte Analyse der Abdeckung von Amazon Inspector für einzelne Ressourcen durchführen und die Ergebnisse für bestimmte Ressourcen detailliert untersuchen. Wenn Sie der delegierte Amazon Inspector-Administrator für eine Organisation sind, enthalten die Daten Statistiken und Details für alle Konten in Ihrer Organisation.

So bewerten Sie die Abdeckung Ihrer AWS Umgebung durch Amazon Inspector

1. Öffnen Sie die Amazon 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 Abdeckungsansichten aus:

   - Konten , für Abdeckung auf Kontoebene.
   - Instances für die Abdeckung von Amazon Elastic Compute Cloud (Amazon EC2)-Instances.
   - Repositorys für die Abdeckung von Amazon Elastic Container Registry (Amazon ECR)-Repositorys.
   - Images , zur Abdeckung von Amazon-ECR-Container-Images.
   - Lambda zur Abdeckung von Lambda-Funktionen.

In den Themen in diesem Abschnitt werden die Informationen beschrieben, die jede Registerkarte bereitstellt, einschließlich des Scanstatus, den eine einzelne Ressource haben kann.

Themen

- Bewertung der Abdeckung von Amazon-ECR-Container-Images
- Bewertung der Abdeckung von AWS Lambda Funktionen

Bewertung der Abdeckung auf Kontoebene

Wenn Ihr Konto nicht Teil einer Organisation ist oder nicht das delegierte Amazon Inspector-Administratorkonto für eine Organisation ist, enthält die 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 für bestimmte Ressourcentypen für Ihr Konto aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Automatisiertes Scannen von Ressourcen mit Amazon Inspector.

Wenn Ihr Konto das delegierte Amazon Inspector-Administratorkonto für eine Organisation ist, 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, falls ja, welche Ressourcenscantypen für das Konto aktiviert sind. Als delegierter Administrator können Sie diese Registerkarte verwenden, um die Einstellungen für die automatische Aktivierung für Ihre Organisation zu ändern. Sie können auch bestimmte Arten von Ressourcenscans für einzelne Mitgliedskonten aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Aktivieren von Amazon Inspector-Scans für Mitgliedskonten.

Bewertung der Abdeckung von Amazon EC2

Auf der Registerkarte Instances werden Amazon EC2-Instances in Ihrer AWS Umgebung angezeigt. Die Listen sind auf den folgenden Registerkarten in Gruppen organisiert:

- All e– Zeigt alle Instances in Ihrer Umgebung an. Die Spalte Status gibt den aktuellen Scanstatus für eine Instance an.
- 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 mehreren Gründen auf der Registerkarte Kein Scannen angezeigt werden. Amazon Inspector verwendet AWS Systems Manager (SSM) und den SSM-Agenten, um

Ihre EC2-Instances automatisch zu überwachen und auf Schwachstellen zu scannen. Wenn auf einer Instance der SSM-Agent nicht ausgeführt wird, keine AWS Identity and Access Management (IAM)-Rolle, die Systems Manager unterstützt, oder kein unterstütztes Betriebssystem oder keine Architektur ausführt, kann Amazon Inspector die Instance nicht überwachen und scannen. Weitere Informationen finden Sie unter Scannen von Amazon EC2.

Auf jeder Registerkarte gibt die Spalte Konto die anAWS-Konto, die eine Instance besitzt.

EC2-Instance-Tags – Diese Spalte zeigt Ihnen die Tags, die der Instance zugeordnet sind, und kann verwendet werden, um festzustellen, ob Ihre Instance von Scans durch Tags ausgeschlossen wurde.

Betriebssystem – In dieser Spalte wird der Betriebssystemtyp angezeigt, der `WINDOWS`, `MACLINUX`, oder sein kann`UNKNOWN`.

Überwacht mit – Diese Spalte zeigt, ob Amazon Inspector die agentenbasierte oder agentenlose Scanmethode auf dieser Instance verwendet.

Letztes Scannen – In dieser Spalte wird angezeigt, wann Amazon Inspector diese Ressource zuletzt auf Schwachstellen überprüft hat. Die Häufigkeit, mit der Amazon Inspector Scans durchführt, hängt von der Scanmethode ab, mit der die Instance gescannt wird.

Um zusätzliche Details zu einer EC2-Instance zu überprüfen, wählen Sie den Link in der Spalte EC2-Instance. Amazon Inspector zeigt dann Details zur Instance und die aktuellen Ergebnisse für die Instance an. Um die Details einer Erkenntnis zu überprüfen, wählen Sie den Link in der Spalte Titel. Informationen zu diesen Details finden Sie unter Details zu den Erkenntnissen in Amazon Inspector .

Scannen von Statuswerten für Amazon EC2

Für eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance sind die möglichen Statuswerte:

- Aktive Überwachung – Amazon Inspector überwacht und scannt die Instance kontinuierlich.
- EC2-Instance angehalten – Amazon Inspector hat das Scannen für die Instance angehalten, da sich die Instance in einem angehaltenen Zustand befindet. Alle vorhandenen Erkenntnisse bleiben bestehen, bis die Instance beendet wird. Wenn die Instance neu gestartet wird, setzt Amazon Inspector das Scannen nach der Instance automatisch fort.
- Interner Fehler – Beim Versuch von Amazon Inspector, die Instance zu scannen, ist ein interner Fehler aufgetreten. Amazon Inspector behebt den Fehler automatisch und setzt das Scannen so schnell wie möglich fort.

- Kein Bestand – Amazon Inspector konnte das Softwareanwendungsinventar nicht finden, um nach der Instance zu suchen. Die Amazon Inspector-Zuordnungen für die Instance wurden möglicherweise gelöscht oder sie konnten möglicherweise nicht ausgeführt werden.

  Um dieses Problem zu beheben, verwenden Sie , AWS Systems Manager um sicherzustellen, dass die `InspectorInventoryCollection-do-not-delete` Zuordnung vorhanden ist und ihr Zuordnungsstatus erfolgreich ist. Verwenden Sie außerdem AWS Systems Manager Fleet Manager, um den Bestand der Softwareanwendung für die Instance zu überprüfen.
- Deaktivieren ausstehend – Amazon Inspector hat das Scannen der Instance eingestellt. Die Instance wird deaktiviert, bis die Bereinigungsaufgaben abgeschlossen sind.
- Ausstehender erster Scan – Amazon Inspector hat die Instance für einen ersten Scan in die Warteschlange gestellt.
- Ressource beendet – Die Instance wurde beendet. Amazon Inspector bereinigt derzeit vorhandene Erkenntnisse und Abdeckungsdaten für die Instance.
- Veraltetes Inventar – Amazon Inspector konnte kein aktualisiertes Softwareanwendungsinventar erfassen, das innerhalb der letzten 7 Tage für die Instance erfasst wurde.

  Um dieses Problem zu beheben, verwenden Sie , AWS Systems Manager um sicherzustellen, dass die erforderlichen Amazon Inspector-Zuordnungen vorhanden sind und für die Instance ausgeführt werden. Verwenden Sie außerdem AWS Systems Manager Fleet Manager, um den Bestand der Softwareanwendung für die Instance zu überprüfen.
- Nicht verwaltete EC2-Instance – Amazon Inspector überwacht oder scannt die Instance nicht. Die Instance wird nicht von verwaltetAWS Systems Manager.

  Um dieses Problem zu beheben, können Sie die von AWS Systems Manager Automation AWSSupport-TroubleshootManagedInstance runbook bereitgestellte verwenden. Nachdem Sie AWS Systems Manager für die Verwaltung der Instance konfiguriert 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 unter Unterstützte Betriebssysteme für Amazon EC2-Scans.
- Aktive Überwachung mit Teilfehlern – Dieser Status bedeutet, dass das EC2-Scannen aktiv ist, aber dass Fehler mit verknüpft sindDetaillierte Überprüfung von Amazon Inspector für Amazon EC2-Linux-Instances. Die möglichen Fehler bei der Untersuchung sind:

- Limit für die Erfassung von Deep Inspect-Paketen überschritten – Die Instance hat das Paketlimit von 5000 für Amazon Inspector Deep Inspector überschritten. Um die eingehende Überprüfung für diese Instance fortzusetzen, können Sie versuchen, die dem Konto zugeordneten benutzerdefinierten Pfade anzupassen.
- Das tägliche SSM-Bestandslimit für die eingehende Überprüfung wurde überschritten – Der SSM-Agent konnte den Bestand nicht an Amazon Inspector senden, da das SSM-Kontingent für Bestandsdaten, die pro Instance und Tag erfasst wurden, für diese Instance bereits erreicht wurde. Weitere Informationen finden Sie unter Endpunkte und Kontingente von Amazon EC2 Systems Manager.
- Zeitlimit für die Erfassung von Deep Inspects überschritten – Amazon Inspector konnte das Paketinventar nicht extrahieren, da die Paketerfassungszeit den maximalen Schwellenwert von 15 Minuten überschreitet.
- Detaillierte Überprüfung hat kein Inventar – Das Amazon Inspector SSM-Plugin konnte noch kein Inventar von Paketen für diese Instance erfassen. Dies ist normalerweise das Ergebnis eines ausstehenden Scans. Wenn dieser Status jedoch nach 6 Stunden bestehen bleibt, verwenden Sie Amazon EC2 Systems Manager, um sicherzustellen, dass die erforderlichen Amazon Inspector-Zuordnungen vorhanden sind und für die Instance ausgeführt werden.

Weitere Informationen zum Konfigurieren der Scaneinstellungen für eine EC2-Instance finden Sie unter Scannen von Amazon EC2.

Bewertung der Abdeckung von Amazon-ECR-Repositorys

Auf der Registerkarte Repositorys werden Amazon-ECR-Repositorys in Ihrer AWS Umgebung angezeigt. Die Listen sind auf den folgenden Registerkarten in Gruppen organisiert:

- All e– Zeigt alle Repositorys in Ihrer Umgebung an. Die Spalte Status gibt den aktuellen Scanstatus für ein Repository an.
- Aktiviert – Zeigt alle Repositorys an, für deren Überwachung und Scan Amazon Inspector in Ihrer Umgebung konfiguriert ist. Die Spalte Status gibt 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 die anAWS-Konto, die ein Repository besitzt.

Um weitere Details zu einem Repository zu überprüfen, wählen Sie den Namen des Repositorys aus. Amazon Inspector zeigt dann eine Liste der Container-Images im Repository und Details für jedes Image an. Zu den Details gehören das Image-Tag, der Image-Digest und der Scanstatus. Sie enthalten auch wichtige Erkenntnisstatistiken, z. B. die Anzahl der kritischen Erkenntnisse für das Bild. Um die unterstützenden Daten für die Suche nach Statistiken aufzuschlüsseln und zu überprüfen, wählen Sie das Image-Tag für das Image aus.

Scannen von Statuswerten für Amazon-ECR-Repositorys

Für ein Amazon Elastic Container Registry (Amazon ECR)-Repository sind die möglichen Statuswerte:

- Aktiviert (Kontinuierlich) – Für ein Repository überwacht Amazon Inspector kontinuierlich Images in diesem Repository. Die Einstellung für das erweiterte Scannen für das Repository ist auf kontinuierliches Scannen festgelegt. Amazon Inspector scannt zunächst neue Images, wenn sie per Push übertragen werden, und scannt Images erneut, wenn ein neues für dieses Image relevantes CVE veröffentlicht wird. Amazon Inspector überwacht weiterhin Images 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 auf Scan bei Push gesetzt.
- Zugriff verweigert – Amazon Inspector darf nicht auf das Repository oder 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 erlauben.
- Deaktiviert (Manuell) – Amazon Inspector überwacht oder scannt keine Container-Images im Repository. Die Amazon-ECR-Scaneinstellung für das Repository ist auf einfaches manuelles Scannen festgelegt.

  Um mit dem Scannen von Images im Repository mit Amazon Inspector zu beginnen, ändern Sie die Scaneinstellung für das Repository auf erweitertes Scannen und wählen Sie dann aus, ob Images kontinuierlich oder nur gescannt werden sollen, wenn ein neues Image übertragen wird.
- Aktiviert (bei Push) – Amazon Inspector scannt automatisch einzelne Container-Images im Repository, wenn ein neues Image übertragen wird. Die Einstellung für das erweiterte Scannen für das Repository ist so eingestellt, dass es bei Push scannt.

- Interner Fehler – Ein interner Fehler ist aufgetreten, als Amazon Inspector versucht hat, das Repository zu scannen. Amazon Inspector behebt den Fehler automatisch und setzt das Scannen so schnell wie möglich fort.

Einzelheiten zur Konfiguration der Scaneinstellungen für Repositorys finden Sie unter Scannen von Amazon-ECR-Container-Images.

Bewertung der Abdeckung 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 organisiert:

- All e– Zeigt alle Container-Images in Ihrer Umgebung an. Die Spalte Status gibt den aktuellen Scanstatus für ein Bild an.
- Scannen – Zeigt alle Container-Images an, die Amazon Inspector in Ihrer Umgebung überwachen und scannen soll. Die Spalte Status gibt den aktuellen Scanstatus für ein Bild an.
- Kein 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 Image nicht überwacht und scannt.

  Ein Container-Image kann aus mehreren Gründen auf der Registerkarte Nicht aktiviert angezeigt werden. Das Image kann in einem Repository gespeichert werden, für das Amazon Inspector-Scans nicht aktiviert sind, oder Amazon-ECR-Filterregeln verhindern, dass dieses Repository gescannt wird. Oder das Image wurde nicht innerhalb der Anzahl der Tage übertragen oder abgerufen, die Sie für die Dauer des erneuten ECR-Scans konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren der Dauer des erneuten ECR-Scans.

Auf jeder Registerkarte gibt die Spalte Repository-Name den Namen des Repositorys an, das ein Container-Image speichert. Die Spalte Konto gibt das anAWS-Konto, dem das Repository gehört. In der Spalte Zuletzt gescannt wird angezeigt, wann Amazon Inspector diese Ressource zuletzt auf Schwachstellen überprüft hat. Dies kann Prüfungen umfassen, wenn eine Aktualisierung der Suche nach Metadaten erfolgt, wenn eine Aktualisierung des Anwendungsbestands der Ressource erfolgt oder wenn als Reaktion auf ein neues CVE ein erneuter Scan durchgeführt wird. Weitere Informationen finden Sie unter Scan-Verhaltensweisen für Amazon-ECR-Scans.

Um zusätzliche 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 die aktuellen Ergebnisse

für das Bild an. Um die Details einer Erkenntnis zu überprüfen, wählen Sie den Link in der Spalte Titel. Weitere Informationen zu diesen Details finden Sie unter Details zu den Erkenntnissen in Amazon Inspector .

Scannen von Statuswerten für Amazon-ECR-Container-Images

Für ein Container-Image von Amazon Elastic Container Registry sind die möglichen Statuswerte:

- Aktive Überwachung (Continuous) – Amazon Inspector überwacht kontinuierlich und das Image und neue Scans werden darauf durchgeführt, wenn ein neues relevantes CVE veröffentlicht wird. Die Dauer des erneuten Scannens von Amazon ECR für das Image wird aktualisiert, wenn das Image gepusht oder abgerufen wird. Das erweiterte Scannen ist für das Repository aktiviert, in dem das Image gespeichert wird, und die Einstellung für das erweiterte Scannen für das Repository ist auf kontinuierliches Scannen festgelegt.
- Aktiviert (bei Push) – Amazon Inspector scannt das Image jedes Mal automatisch, wenn ein neues Image gepusht wird. Das erweiterte Scannen ist für das Repository aktiviert, in dem das Image gespeichert ist, und die Einstellung für das erweiterte Scannen für das Repository ist so eingestellt, dass es bei Push-Vorgang gescannt wird.
- Interner Fehler – Ein interner Fehler ist aufgetreten, als Amazon Inspector versucht hat, das Container-Image zu scannen. Amazon Inspector behebt den Fehler automatisch und setzt das Scannen so schnell wie möglich fort.
- Ausstehender erster Scan – Amazon Inspector hat das Image für einen ersten Scan in die Warteschlange gestellt.
- Scanberechtigung abgelaufen (kontinuierlich) – Amazon Inspector hat das Scannen für das Bild ausgesetzt. Das Image wurde nicht innerhalb der Dauer aktualisiert, die Sie für automatische erneute Scans von Images im Repository angegeben haben. Sie können das Image pushen oder abrufen, um das Scannen fortzusetzen.
- Scanberechtigung abgelaufen (bei Push) – Amazon Inspector hat das Scannen für das Image ausgesetzt. Das Image wurde nicht innerhalb der Dauer aktualisiert, die Sie für automatische erneute Scans von Images im Repository angegeben haben. Sie können das Image pushen, um das Scannen fortzusetzen.
- Manuelle Scanfrequenz (manuell) – Amazon Inspector scannt das Amazon-ECR-Container-Image nicht. Die Amazon-ECR-Scaneinstellung für das Repository, in dem das Image gespeichert ist, ist auf einfaches, manuelles Scannen festgelegt. Um mit dem automatischen Scannen des Images mit Amazon Inspector zu beginnen, ändern Sie die Repository-Einstellung auf erweitertes Scannen

und wählen Sie dann aus, ob Images kontinuierlich oder nur gescannt werden sollen, wenn ein neues Image übertragen wird.

- Nicht unterstütztes Betriebssystem – Amazon Inspector überwacht oder scannt das Image nicht. Das Image 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 unter Unterstützte Betriebssysteme für Amazon-ECR-Scans. Eine Liste der von Amazon Inspector unterstützten Medientypen finden Sie unter Unterstützte Medientypen.

Weitere Informationen zum Konfigurieren der Scaneinstellungen für Repositorys und Images finden Sie unter Scannen von Amazon-ECR-Container-Images.

Bewertung der Abdeckung von AWS Lambda Funktionen

Auf der Registerkarte Lambda werden Lambda-Funktionen in Ihrer AWS Umgebung angezeigt. Diese Seite enthält zwei Tabellen, eine mit Details zur Funktionsabdeckung für Lambda-Standardscan und eine weitere für Lambda-Codescan. Sie können Funktionen basierend auf den folgenden Registerkarten gruppieren:

- All e– Zeigt alle Lambda-Funktionen in Ihrer Umgebung an. Die Spalte Status gibt den aktuellen Scanstatus für eine Lambda-Funktion an.
- Scannen – Zeigt die Lambda-Funktionen an, für deren Scannen Amazon Inspector konfiguriert ist. Die Spalte Status gibt den aktuellen Scanstatus für jede Lambda-Funktion an.
- Kein 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 mehreren Gründen auf der Registerkarte Kein Scannen angezeigt werden. Die Lambda-Funktion kann zu einem Konto gehören, das Amazon Inspector nicht hinzugefügt wurde, oder Filterregeln verhindern, dass diese Funktion gescannt wird. Weitere Informationen finden Sie unter Scannen von AWS Lambda Funktionen.

Auf jeder Registerkarte gibt die Spalte Funktionsname den Namen der Lambda-Funktion an. Die Spalte Konto gibt das anAWS-Konto, dem die Funktion gehört. Die Laufzeit gibt die Laufzeit der Funktion an. Die Spalte Status gibt den aktuellen Scanstatus für jede Lambda-Funktion an.

Ressourcen-Tags zeigen die Tags an, die auf die Funktion angewendet wurden. In der Spalte Zuletzt gescannt wird angezeigt, wann Amazon Inspector diese Ressource zuletzt auf Schwachstellen überprüft hat. Dies kann Prüfungen umfassen, wenn eine Aktualisierung der Suche nach Metadaten erfolgt, wenn eine Aktualisierung des Anwendungsbestands der Ressource erfolgt oder wenn als Reaktion auf ein neues CVE ein erneuter Scan durchgeführt wird. Weitere Informationen finden Sie unter Scanverhalten für das Scannen von Lambda-Funktionen.

Scannen von Statuswerten für AWS Lambda Funktionen

Für eine Lambda-Funktion sind die möglichen Statuswerte:

- Aktive Überwachung – Amazon Inspector überwacht und scannt kontinuierlich Lambda-Funktionen. Kontinuierliches Scannen beinhaltet einen ersten Scan neuer Funktionen, wenn sie in das Repository übertragen werden, und automatisierte erneute Scans von Funktionen, wenn sie aktualisiert werden oder wenn neue Common Vulnerabilities and Exposures (CVEs) veröffentlicht werden.
- Ausgeschlossen nach Tag – Amazon Inspector scannt diese Funktion nicht, da sie von Scans nach Tags ausgeschlossen wurde.
- Scanberechtigung abgelaufen – Amazon Inspector überwacht diese Funktion nicht, da es seit dem letzten Aufruf oder der letzten Aktualisierung 90 Tage oder länger ist.
- Interner Fehler – Beim Versuch von Amazon Inspector, die Funktion zu scannen, ist ein interner Fehler aufgetreten. Amazon Inspector behebt den Fehler automatisch und setzt das Scannen so schnell wie möglich fort.
- Ausstehender erster Scan – Amazon Inspector hat die Funktion für einen ersten Scan in die Warteschlange gestellt.
- Nicht unterstützt – Die Lambda-Funktion hat eine nicht unterstützte Laufzeit.

Verwalten mehrerer Konten in Amazon Inspector mit Organizations

Sie können Amazon Inspector verwenden, um mehrere Konten zu verwalten, die über AWS Organizations zugeordnet sind. Um mehrere Amazon Inspector-Konten zu verwalten, bestimmt das Organizations-Verwaltungskonto ein Konto innerhalb der Organisation als delegiertes Administratorkonto für Amazon Inspector . Der delegierte Administrator verwaltet Amazon Inspector für die Organisation und erhält spezielle Berechtigungen zum Ausführen von Aufgaben im Namen Ihrer Organisation. Zu diesen Aufgaben gehören das Aktivieren oder Deaktivieren von Scans für Mitgliedskonten, das Anzeigen aggregierter Erkenntnisdaten aus der gesamten Organisation und das Erstellen und Verwalten von Unterdrückungsregeln.

> **Note**
>
> Um Amazon Inspector für mehrere Konten in mehreren programmgesteuert zu aktivierenAWS-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 - GitHub Website.

Themen

Verstehen der Beziehung zwischen Administrator- und Mitgliedskonten in Amazon Inspector

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 und Ergebnisse von Sicherheitserkenntnissen für Mitgliedskonten. Das Administratorkonto kann auch Regeln zur Unterdrückung von Erkenntnissen erstellen, die auf Mitgliedskonten angewendet werden. Weitere Informationen finden Sie unter Unterdrücken von Amazon Inspector-Ergebnissen 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 zugehörige Mitglied anzeigen und abrufen. Ein delegiertes Administratorkonto von Amazon Inspector kann die folgenden Aktionen ausführen:

- Zeigen Sie den Status von Amazon Inspector für zugehörige Konten an und verwalten Sie ihn, einschließlich der Aktivierung und Deaktivierung von Amazon Inspector .
- Aktivieren oder deaktivieren Sie Scantypen für alle Mitgliedskonten in der Organisation.
- Zeigen Sie aggregierte Erkenntnisdaten in der gesamten Organisation und Erkenntnisdetails für alle Mitgliedskonten innerhalb der Organisation an.
- Erstellen und verwalten Sie Unterdrückungsregeln, die für Ergebnisse für alle 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 automatisierte erneute Scans von ECR-Container-Images für alle Mitgliedskonten in der Organisation. Die Einstellung für die Scandauer des delegierten Administrators überschreibt alle Einstellungen, die das Mitgliedskonto zuvor festgelegt hat. Alle Konten in der Organisation teilen sich die Dauer des automatischen erneuten Scannens von Amazon ECR der delegierten Administratoren. Sie können für einzelne Konten keine unterschiedlichen Wiederholungsscan-Dauern festlegen.
- Geben Sie fünf benutzerdefinierte Pfade für Amazon Inspector Deep Inspector 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 einzelnes Konto festlegen kann. Weitere Informationen zum Konfigurieren benutzerdefinierter Deep-Inspection-Pfade finden Sie unter Benutzerdefinierte Pfade für Amazon Inspector Deep Inspector.
- Aktivieren und deaktivieren Sie Amazon Inspector Deep Inspector für Mitgliedskonten.
- Exportieren Sie SBOMs für alle Mitgliedskonten in der Organisation.
- Legen Sie den Amazon EC2-Scanmodus für alle Mitgliedskonten in der Organisation fest. Weitere Informationen finden Sie unter Verwalten des Scanmodus.
- 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 CIS-Scanergebnisse für alle Konten in der Organisation an.

Aktionen für Mitgliedskonten

Ein Mitgliedskonto kann Informationen über sein Konto in Amazon Inspector anzeigen 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.
- Zeigen Sie die Ressourcenabdeckung für ihr eigenes Konto an.
- Zeigen Sie die Ergebnisdetails für ihr eigenes Konto an.
- Sehen Sie sich die Einstellung für die Dauer des automatischen erneuten Scannens des ECR-Container-Images für ihr eigenes Konto an.
- Geben Sie fünf benutzerdefinierte Pfade für Amazon Inspector Deep Inspector für EC2 an, die für ihr einzelnes Konto verwendet werden. Diese Pfade werden zusätzlich zu allen benutzerdefinierten Pfaden gescannt, die der delegierte Administrator für die Organisation angegeben hat. Weitere Informationen zum Konfigurieren von Deep-Inspection-Pfaden finden Sie unter Benutzerdefinierte Pfade für Amazon Inspector Deep Inspector.
- Zeigen Sie die benutzerdefinierten Pfade an, die von Ihrem delegierten Administrator für die Amazon Inspector-Deep-Inspection festgelegt wurden.
- Exportieren Sie SBOMs für alle Ressourcen, die ihrem Konto zugeordnet sind.
- Zeigen Sie den Scanmodus für ihr Konto an.
- Erstellen und verwalten Sie CIS-Scankonfigurationen für ihr Konto.
- Zeigen Sie die Ergebnisse aller CIS-Scans für Ressourcen in ihrem Konto an, einschließlich der vom delegierten Administrator geplanten.

> **Note**
>
> Nach der Aktivierung kann Amazon Inspector nur von einem delegierten Administratorkonto deaktiviert werden.

Festlegen 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 Amazon Inspector-Administrator hat ein Kontingent von 5 000 Mitgliedskonten. Ihre Organisation könnte jedoch mehr als 5 000 Konten umfassen. Wenn Sie 5 000 Mitgliedskonten überschreiten, 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 Gegensatz zu ist AWS Organizations Amazon Inspector ein regionaler Service. Das bedeutet, dass Sie den delegierten Administrator benennen, Mitgliedskonten hinzufügen und Scantypen in jedem aktivieren müssen, in dem AWS-Region Sie Amazon Inspector verwenden möchten.

Eine Organisation kann nur einen delegierten Administrator haben.

Sie können nur einen delegierten Administrator für Amazon Inspector für eine Organisation haben. Wenn Sie ein Konto in einer Region als delegierten Administrator festgelegt haben, muss dieses Konto in allen anderen Regionen Ihr delegierter Administrator sein.

Das Ändern eines delegierten Administrators deaktiviert Amazon Inspector nicht für Mitgliedskonten.

Wenn Sie den delegierten Administrator entfernen, wird Amazon Inspector in diesen Konten nicht deaktiviert und die Scaneinstellungen sind davon nicht betroffen.

In Ihrer AWS Organisation müssen alle Funktionen aktiviert sein.

Dies ist die Standardeinstellung für AWS Organizations. Wenn es nicht aktiviert ist, finden Sie weitere Informationen unter Aktivieren aller Funktionen in Ihrer Organisation.

Erforderliche Berechtigungen zum designieren eines delegierten Administrators

Sie müssen über die Berechtigung verfügen, Amazon Inspector zu aktivieren und einen delegierten Amazon Inspector-Administrator zu benennen.

Fügen Sie die folgende Anweisung am Ende einer IAM-Richtlinie hinzu, um diese Berechtigungen zu erteilen.

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Festlegen eines delegierten Administrators für Ihre AWS Organisation

Das folgende Verfahren zeigt Ihnen, wie Sie einen delegierten Administrator für Ihre AWS Organisation festlegen. Wenn diese Bezeichnung abgeschlossen ist, wird Amazon Inspector sowohl für das Verwaltungskonto von Organizations als auch für das ausgewählte delegierte Administratorkonto aktiviert.

> **Note**
>
> Nur das Verwaltungskonto von 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 unter Verwenden von serviceverknüpften Rollen für Amazon Inspector. Informationen zu serviceverknüpften Rollen im Allgemeinen finden Sie unter Verwenden von serviceverknüpften Rollen im IAM-Benutzerhandbuch.

So weisen Sie einen delegierten Administrator für Amazon Inspector an

Console

Festlegen eines delegierten Administrators in der Konsole

1. Melden Sie sich mit dem AWS Organizations-Verwaltungskonto in der AWS Management Console an.
2. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und verwenden Sie dann die AWS-Region Auswahl oben rechts, um die Region anzugeben, in der Sie einen Administrator festlegen möchten.
3. Geben Sie im Bereich Delegierter Administrator die zwölfstellige Konto-ID des einAWS-Konto, das Sie als delegierten Amazon Inspector-Administrator für Ihre Organisation festlegen möchten. Wählen Sie dann Verwaltung delegieren aus.
4. (Empfohlen) Wiederholen Sie die vorherigen Schritte für jede AWS-Region.

API

Benennen eines delegierten Administrators mithilfe der API

- Führen Sie den EnableDelegatedAdminAccount API-Vorgang mit den Anmeldeinformationen des des AWS-Konto Verwaltungskontos von Organizations aus. Sie können auch die verwendenAWS 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 als delegierter Amazon Inspector-Administrator einrichten 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.

Aktivieren von Amazon Inspector-Scans für Mitgliedskonten

Als delegierter Administrator für Ihre Organisation können Sie Amazon EC2-Scannen, das Amazon-ECR-Scannen oder beides für jedes Mitglied aktivieren, das dem AWS Organizations Verwaltungskonto zugeordnet 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 unter Automatisiertes Scannen von Ressourcen mit Amazon Inspector.

Amazon Inspector bietet mehrere Optionen zum Verwalten und Aktivieren von Scans für Mitgliedskonten, darunter Mitgliedskonten, Amazon Inspector zu aktivieren. Verwenden Sie eine der folgenden Optionen, um Scans für Ihre Mitgliedskonten zu starten.

So aktivieren Sie das Scannen für alle Mitgliedskonten automatisch

1. Melden Sie sich beim delegierten Administratorkonto an.
2. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home. Verwenden Sie dann die AWS-Region Auswahl oben rechts, um die Region anzugeben, in der Sie das Scannen für alle Mitgliedskonten aktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus. In der Tabelle Konten 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 Ihre bevorzugte Scantypoption aus dem Menü aus.

> **Note**
>
> Es werden nur die Konten ausgewählt, die derzeit auf der Seite sichtbar sind. Wenn Sie mehrere Seiten von Konten haben, müssen Sie diesen Vorgang auf jeder Seite wiederholen. Um die Anzahl der auf der Seite angezeigten Konten zu ändern, wählen Sie das Zahnradsymbol aus.

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 Ihrer Organisation hinzugefügt werden.
6. (Empfohlen) Wiederholen Sie diese Schritte in jeder Region, in der Sie Mitgliedskonten scannen möchten.

Mit der Einstellung Inspector automatisch für neue Mitgliedskonten aktivieren wird Amazon Inspector für alle zukünftigen Mitglieder Ihrer Organisation aktiviert. 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 abnimmt, wird die Einstellung automatisch erneut aktiviert.

So aktivieren Sie Mitgliedskonten selektiv

1. Melden Sie sich beim delegierten Administratorkonto an.
2. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und verwenden Sie dann die AWS-Region Auswahl oben rechts, um die Region anzugeben, in der Sie das Scannen für bestimmte Mitgliedskonten aktivieren möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus. In der Tabelle Konten 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 das Scannen 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 Scan-Optionen wählen:
   - Alle Scans – um alle Scantypen zu aktivieren.
   - EC2-Scan – um Scans von Amazon EC2 zu aktivieren.
   - ECR-Container-Scan – um Scans von ECR-Container-Images zu aktivieren.
   - AWS Lambda Standardscan – 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 Scandetails für Ihr eigenes Konto anzeigen.

So aktivieren Sie das Scannen als Mitgliedskonto

1. Melden Sie sich bei Ihrem -Konto an.
2. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und verwenden Sie dann die AWS-Region Auswahl oben rechts, um die Region anzugeben, 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 Scan-Optionen wählen:
   - Alle Scans – um alle Scantypen zu aktivieren.
   - EC2-Scan – um Scans von Amazon EC2 zu aktivieren.
   - ECR-Container-Scan – um Scans von ECR-Container-Images zu aktivieren.
   - AWS Lambda Standardscan – um Scans von Lambda-Funktionen zu aktivieren.
6. (Empfohlen) Wiederholen Sie diese Schritte in jeder Region, in der Sie Scans aktivieren möchten.

Aufheben der Zuordnung von Mitgliedskonten in Amazon Inspector

Das folgende Verfahren zeigt, wie Sie Mitgliedskonten trennen. Nicht zugeordnete Mitgliedskonten verbleiben in Ihrer AWS Organizations Organisation als eigenständige Amazon Inspector-Konten. Der delegierte Amazon Inspector-Administrator hat keine Berechtigung mehr, Amazon Inspector für diese Konten zu aktivieren und zu verwalten. Sie können getrennte Konten später wieder als Mitglieder hinzufügen.

> **Note**
>
> Durch das Aufheben der Zuordnung eines Kontos werden Amazon Inspector-Scans für dieses Konto nicht deaktiviert.

Console

So heben Sie die Zuordnung von Mitgliedskonten mithilfe der Konsole auf

1. Melden Sie sich beim delegierten Administratorkonto an.
2. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und verwenden Sie dann die AWS-Region Auswahl oben rechts, um die Region anzugeben, in der Sie die Zuordnung eines oder mehrerer 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 Zuordnung 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 die Zuordnung von Konten aufheben möchten.

API

So heben Sie die Zuordnung von Mitgliedskonten mithilfe der API auf

Führen Sie den DisassociateMember -API-Vorgang aus. Geben Sie in der Anforderung die Konto-IDs an, die Sie trennen.

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 der Organisation nicht deaktiviert. Konten innerhalb Ihrer Organisation werden in eigenständige Konten konvertiert und behalten die Scaneinstellungen bei, die sie hatten, bevor sie von einem delegierten Administrator verwaltet werden.

So entfernen Sie den delegierten Administrator

1. Melden Sie sich AWS Management Console mit dem AWS Organizations Verwaltungskonto bei der an.

2. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und verwenden Sie dann die AWS-Region Auswahl oben rechts, um die Region anzugeben, in der Sie den delegierten Administrator entfernen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus.
4. Wählen Sie im Abschnitt 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. Führen Sie die folgenden Schritte aus, um Organisationsmitglieder dem neuen Administratorkonto zuzuordnen.

So verknüpfen Sie Mitglieder mit einem neuen delegierten Administrator

1. Melden Sie sich AWS Management Console mit dem delegierten Administratorkonto bei der an.
2. Öffnen Sie die Amazon Inspector-Konsole unter https://console.aws.amazon.com/inspector/v2/home und verwenden Sie dann die AWS-Region Auswahl oben rechts, um die Region anzugeben, in der Sie Mitglieder dem neuen delegierten Administrator zuordnen möchten.
3. Wählen Sie im Navigationsbereich unter Einstellungen die Option Kontoverwaltung aus.
4. Aktivieren Sie alle aufgelisteten Konten in Ihrer Organisation, indem Sie das oberste 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.

Überwachen von Nutzung und Kosten in Amazon Inspector

Sie können die Amazon Inspector-Konsole und API-Operationen verwenden, um die monatlichen Kosten für die Verwendung von Amazon Inspector in Ihrer Umgebung zu projizieren. Wenn Sie der Amazon Inspector-Administrator für eine Umgebung mit mehreren Konten sind, können Sie die Gesamtkosten für Ihre gesamte Umgebung und die Kostenmetriken für jedes Ihrer Mitgliedskonten anzeigen.

Verwenden der -Nutzungskonsole

Sie können die Nutzung und die voraussichtlichen Kosten für Amazon Inspector über die Konsole bewerten.

So greifen Sie auf Nutzungsstatistiken zu

1. Öffnen Sie die Amazon 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 sehen Sie die prognostizierten Gesamtkosten basierend auf dem 30-Tage-Zeitraum, der unter Kontonutzung aufgeführt ist. Wählen Sie in der Tabelle in der Spalte Projizierte 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 innerhalb Ihrer Organisation eine Zeile angezeigt. Wenn ein Konto in Ihrer Organisation getrennt ist, zeigt die Konsole die voraussichtlichen Kosten als - an.

Auf der Registerkarte Nach Scantyp können Sie eine Aufschlüsselung der tatsächlichen Nutzung im aktuellen Zeitraum von 30 Tagen nach Scantyp sehen. Dies sind die Informationen, die zur Berechnung der prognostizierten Kosten auf der Registerkarte Nach Konto verwendet werden.

Wenn Sie der delegierte Administrator für eine Organisation sind, können Sie die Nutzung für jedes Konto in Ihrer Organisation sehen.

Auf dieser Registerkarte können Sie einen der folgenden Bereiche für Nutzungsstatistiken erweitern:

Amazon EC2-Scan

Die Amazon Inspector-Nutzungskonsole verfolgt die folgenden Metriken für das agentenbasierte Scannen und das agentenlose Scannen:

- Instances (Durchschnitt) – Amazon Inspector berechnet anhand der Abdeckungsstunden die durchschnittliche Anzahl von Ressourcen für das Scannen von EC2-Instances. Der Durchschnitt ist die Gesamtzahl der Abdeckungsstunden geteilt durch 720 Stunden (die Anzahl der Stunden in einem Zeitraum von 30 Tagen).
- Abdeckungsstunden – für das Scannen von Amazon EC2 ist dies die Gesamtzahl der Stunden innerhalb der letzten 30 Tage, für die Amazon Inspector für jede EC2-Instance in einem Konto eine aktive Abdeckung bereitgestellt hat. Bei EC2-Instances sind Abdeckungsstunden die Stunden ab dem Zeitpunkt, an dem Amazon Inspector die Instance entdeckt hat, bis sie beendet, gestoppt oder von Scans durch Tags ausgeschlossen wurde. (Wenn Sie eine angehaltene Instance neu starten oder ein Ausschluss-Tag entfernen, nimmt Amazon Inspector die Abdeckungs- und Abdeckungsstunden für diese Instance wieder auf).

CIS-Instance-Scans – Die Gesamtzahl der CIS-Scans, die für Instances im Konto durchgeführt wurden.

Amazon-ECR-Scan

Erste Scans – Die Summe der ersten Scans von Bildern im Konto innerhalb der letzten 30 Tage.

Erneute Scans – Die Summe der erneuten Scans für Bilder im Konto innerhalb der letzten 30 Tage. Ein erneuter Scan ist jeder Scan, der an einem ECR-Image durchgeführt wurde, das Amazon Inspector zuvor gescannt hat. Wenn Sie Ihr ECR-Repository für kontinuierliches Scannen konfiguriert haben, werden erneute Scans automatisch durchgeführt, wenn Amazon Inspector der Datenbank ein neues Common Vulnerabilities and Exposures (CVE) hinzufügt.

Lambda-Scan

Die Amazon Inspector-Nutzungskonsole verfolgt die folgenden Metriken für das Scannen von Lambda-Standard- und Lambda-Code:

- Anzahl der Lambda-Funktionen (Avg) – Amazon Inspector berechnet anhand der Abdeckungsstunden die durchschnittliche Anzahl von Funktionen für das Scannen von Lambda-Funktionen. Durchschnitt ist die Gesamtzahl der Abdeckungsstunden geteilt durch 720 Stunden (die Anzahl der Stunden in einem Zeitraum von 30 Tagen).

- Abdeckungsstunden – Für das Scannen von Lambda-Funktionen ist dies die Gesamtzahl der Stunden innerhalb der letzten 30 Tage, für die Amazon Inspector für jede Lambda-Funktion in einem Konto eine aktive Abdeckung bereitgestellt hat. Für AWS Lambda Funktionen werden die Abdeckungsstunden berechnet, wenn Amazon Inspector eine Funktion entdeckt, bis sie gelöscht oder aus Scans ausgeschlossen wird. Wenn eine ausgeschlossene Funktion erneut enthalten ist, fallen für diese Funktion weiterhin Abdeckungsstunden an.

Verstehen, wie Amazon Inspector die Nutzungskosten berechnet

Bei den von Amazon Inspector bereitgestellten Kosten handelt es sich um Schätzungen, nicht um tatsächliche Kosten, sodass sie sich von denen in Ihrer AWS BillingKonsole unterscheiden können.

Beachten Sie Folgendes darüber, wie Amazon Inspector die Kosten auf der Seite Nutzung berechnet:

- Die Nutzungskosten spiegeln nur die aktuelle Region wider. Die Preise pro Scantyp variieren je nach AWS Region. Informationen zur Überprüfung der 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 prognostizierten Kosten enthalten.
- Die prognostizierten Kosten stellen die Gesamtkosten für den 30-tägigen Nutzungszeitraum pro Scantyp dar. Wenn es weniger als 30 Tage für ein Konto gegeben hat, prognostiziert Amazon Inspector die Kosten nach 30 Tagen, als ob derzeit abgedeckte Ressourcen für den Rest des 30-Tage-Zeitraums abgedeckt bleiben würden.
- Die Kosten pro Scantyp werden auf der Grundlage der folgenden Faktoren berechnet:
  - EC2-Scan: Die Kosten spiegeln die durchschnittliche Anzahl von EC2-Instances wider, die von Amazon Inspector in den letzten 30 Tagen abgedeckt wurden.
  - ECR-Container-Scan: Die Kosten spiegeln die Summe der Anzahl der ersten Image-Scans + Image-Neuscans in den letzten 30 Tagen wider.
  - Lambda-Standardscan: Die Kosten spiegeln die durchschnittliche Anzahl von Lambda-Funktionen wider, die von Amazon Inspector in den letzten 30 Tagen abgedeckt wurden.
  - Scannen von Lambda-Code: Die Kosten spiegeln die durchschnittliche Anzahl von Lambda-Funktionen wider, die von Amazon Inspector in den letzten 30 Tagen abgedeckt wurden.

Informationen zur kostenlosen Testversion von Amazon Inspector

Wenn Sie einen Scantyp von Amazon Inspector aktivieren, werden Sie automatisch bei einer 15-tägigen kostenlosen Testversion für diesen Scantyp registriert. Jeder Scantyp verfügt über einen unabhängigen kostenlosen Trail, der Folgendes umfasst: EC2-Scan, ECR-Scan, Lambda-Standard-Scan und Lambda-Code-Scan.

> **Note**
>
> Die kostenlose Testversion gilt nicht für CIS-Scans.

Wenn Sie einen Scantyp während der kostenlosen Testversion deaktivieren, wird die kostenlose Testversion für diesen Scantyp angehalten. Wenn Sie diesen Service reaktivieren, wird die kostenlose Testversion fortgesetzt und Sie erhalten die verbleibenden Tage dieser kostenlosen Testversion.

Sicherheit in Amazon Inspector

Cloud-Sicherheit hat AWS bei höchste Priorität. Als - AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die entwickelt wurden, um die Anforderungen der sicherheitssensibelsten Organisationen zu erfüllen.

Sicherheit ist eine geteilte Verantwortung zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS Services in der ausführt AWS Cloud. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Externe Prüfer testen und überprüfen im Rahmen der AWS Compliance-Programme . Informationen zu den Compliance-Programmen, die für Amazon Inspector gelten, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -ServicesIm.
- Sicherheit in der Cloud – Ihre Verantwortung wird durch den - AWS Service bestimmt, den Sie verwenden. 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 geteilten Verantwortung bei der Verwendung von Amazon Inspector einsetzen können. Die folgenden Themen zeigen Ihnen, wie Sie Amazon Inspector konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere - AWS Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer Amazon Inspector-Ressourcen unterstützen.

Themen

Datenschutz in Amazon Inspector

Das AWS Modell der geteilten VerantwortungModell gilt für den Datenschutz in Amazon Inspector . Wie in diesem Modell beschrieben, AWS ist für den Schutz der globalen Infrastruktur verantwortlich, die alle ausführt 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 Ihnen, -Anmeldeinformationen zu schützen AWS-Konto und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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 für die Kommunikation mit - AWS Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API- und Benutzeraktivitätsprotokollierung mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in 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 auf 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, API AWS CLI 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 standardmäßig sicher mithilfe von AWS Verschlüsselungslösungen. Amazon Inspector verschlüsselt Daten, z. B. den mit AWS Systems Manager erfassten Ressourcenbestand, den aus Amazon-ECR-Images analysierten Ressourcenbestand und generierte Sicherheitsergebnisse, mit AWS eigenen Verschlüsselungsschlüsseln vom AWS Key Management Service (AWS KMS). Sie können keine - AWS eigenen Schlüssel anzeigen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen oder Programme ändern, um die Schlüssel zu schützen, die Ihre Daten verschlüsseln. Weitere Informationen finden Sie unter AWS -eigene Schlüssel.

Wenn Sie Amazon Inspector deaktivieren, werden alle Ressourcen, die es für Sie speichert oder verwaltet, wie z. B. erfasste Inventar- und Sicherheitsergebnisse, dauerhaft gelöscht.

Verschlüsselung im Ruhezustand für Code in Ihren Ergebnissen

Für das Scannen von Amazon Inspector Lambda-Code arbeitet Amazon Inspector mit zusammen, CodeGuru um Ihren Code auf Schwachstellen zu scannen. Wenn eine Schwachstelle erkannt wird, CodeGuru extrahiert einen Ausschnitt Ihres Codes, der die Schwachstelle enthält, und speichert diesen Code, bis Amazon Inspector Zugriff anfordert. Standardmäßig CodeGuru verwendet einen - AWS eigenen Schlüssel, um den extrahierten Code zu verschlüsseln. Sie können Amazon Inspector jedoch so konfigurieren, dass Ihr eigener kundenverwalteter AWS KMS Schlüssel für die Verschlüsselung verwendet wird.

Der folgende Workflow erklärt, wie Amazon Inspector den -Schlüssel verwendet, den Sie für die Verschlüsselung Ihres Codes konfigurieren:

1. Sie stellen Amazon Inspector mithilfe der Amazon Inspector UpdateEncryptionKey API einen AWS KMS Schlüssel zur Verfügung.
2. Amazon Inspector leitet die Informationen über Ihren AWS KMS Schlüssel an weiter CodeGuru. CodeGuru speichert die Informationen für die zukünftige Verwendung.

3. CodeGuru fordert eine Erteilung von AWS KMS für den Schlüssel an, den Sie in Amazon Inspector konfiguriert haben.
4. CodeGuru erstellt einen verschlüsselten Datenschlüssel aus Ihrem AWS KMS Schlüssel und speichert ihn. Dieser Datenschlüssel wird verwendet, um Ihre von gespeicherten Codedaten zu verschlüsseln CodeGuru.
5. Immer wenn Amazon Inspector Daten aus Code-Scans anfordert, CodeGuru verwendet die Erteilung zum Entschlüsseln des verschlüsselten Datenschlüssels, verwendet diesen Schlüssel zum Entschlüsseln der Daten, damit er abgerufen werden kann.

Wenn Sie das Lambda-Codescannen deaktivieren, wird die Erteilung CodeGuru aufgehoben und der zugehörige Datenschlüssel gelöscht.

Berechtigungen für die Codeverschlüsselung mit einem vom Kunden verwalteten Schlüssel

Um die Verschlüsselung zu verwenden, benötigen Sie eine Richtlinie, die den Zugriff auf - AWS KMS Aktionen erlaubt, sowie eine Anweisung, die Amazon Inspector und CodeGuru Berechtigungen zur Verwendung dieser Aktionen über Bedingungsschlüssel gewährt.

Wenn Sie den Verschlüsselungsschlüssel für Ihr Konto festlegen, aktualisieren oder zurücksetzen, müssen Sie eine Amazon Inspector-Administratorrichtlinie verwenden, z. B. AWS Von verwaltete Richtlinie: AmazonInspector2FullAccess. Sie müssen auch die folgenden Berechtigungen für schreibgeschützte Benutzer erteilen, die Codeausschnitte aus Erkenntnissen oder Daten über den für die Verschlüsselung ausgewählten Schlüssel abrufen müssen.

Für KMS muss Ihnen die Richtlinie die Durchführung der folgenden Aktionen erlauben:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

Sobald Sie sich vergewissert haben, dass Sie über die richtigen AWS KMS Berechtigungen in Ihrer Richtlinie verfügen, müssen Sie eine Anweisung anfügen, die es Amazon Inspector und

ermöglicht, Ihren Schlüssel für die Verschlüsselung CodeGuru zu verwenden. Fügen Sie die folgende Richtlinienanweisung an:

> **Note**
>
> Ersetzen Sie Region durch die AWS Region, in der Sie Amazon Inspector Lambda-Codescan 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 ein Komma nach der schließenden Klammer für die vorherige Anweisung hinzu. Wenn Sie sie als erste Anweisung oder zwischen zwei vorhandenen Anweisungen hinzufügen, fügen Sie ein Komma nach der schließenden Klammer für die Anweisung hinzu.

Konfigurieren 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 multiregionalen Schlüssel . Sie können einen vorhandenen symmetrischen Schlüssel in Ihrem Konto verwenden oder einen symmetrischen, vom Kunden verwalteten Schlüssel mithilfe der - AWS Managementkonsole oder der AWS KMS APIs erstellen. Weitere Informationen finden Sie unter Erstellen von symmetrischen AWS KMS Verschlüsselungsschlüsseln im AWS KMS - Benutzerhandbuch.

Verwenden der Amazon Inspector API zum Konfigurieren der Verschlüsselung

So legen Sie einen Schlüssel für die Verschlüsselung fest, UpdateEncryptionKey wenn Sie als Amazon InspectorAmazon Inspector-Administrator angemeldet sind. Verwenden Sie in der

API-Anforderung das `kmsKeyId` Feld , um den ARN des AWS KMS Schlüssels anzugeben, den Sie verwenden möchten. Geben `scanType` Sie für `CODE` und für `resourceType` ein`AWS_LAMBDA_FUNCTION`.

Sie können UpdateEncryptionKey die API verwenden, um zu überprüfen, welchen AWS KMS Schlüssel Amazon Inspector für die Verschlüsselung verwendet.

> **Note**
>
> Wenn Sie versuchen, zu verwenden, `GetEncryptionKey` wenn Sie keinen vom Kunden verwalteten Schlüssel festgelegt haben, gibt die Operation einen `ResourceNotFoundException` Fehler zurück, was bedeutet, dass ein - AWS eigener Schlüssel für die Verschlüsselung verwendet wird.

Wenn Sie oder den -Schlüssel löschen oder dessen Richtlinie ändern, um den Zugriff auf Amazon Inspector zu verweigern, können CodeGuru Sie nicht auf Ihre Ergebnisse zur Code-Schwachstelle zugreifen und das Scannen von Lambda-Code schlägt für Ihr Konto fehl.

Sie können verwenden`ResetEncryptionKey`, um die Verwendung eines AWS -eigenen Schlüssels zur Verschlüsselung von Code fortzusetzen, der als Teil Ihrer Amazon Inspector-Ergebnisse extrahiert wurde.

Verschlüsselung während der Übertragung

AWS verschlüsselt alle Daten während der Übertragung zwischen AWS internen Systemen und anderen - AWS Services.

Für die Bestandserfassung sammelt Systems Manager Telemetriedaten von kundeneigenen EC2-Instances, die es zur Bewertung AWS über einen Transport Layer Security (TLS)-geschützten Kanal an zurücksendet. Unter Datenschutz in Systems Manager erfahren Sie, wie SSM Daten während der Übertragung verschlüsselt.

Ebenso werden die Scanergebnisse der Amazon-ECR- und AWS Lambda-Funktionen, die an Security Hub gesendet werden, mit einem TLS-geschützten Kanal verschlüsselt.

Identity and Access Management für Amazon Inspector

AWS Identity and Access Management (IAM) ist ein AWS-Service , mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) ist, Amazon Inspector-Ressourcen zu nutzen. IAM ist ein AWS-Service , den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Amazon Inspector.

Service-Benutzer – Wenn Sie den Amazon Inspector-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Amazon Inspector-Funktionen ausführen, 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 nicht auf ein Feature in Amazon Inspector zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung für Identität und Zugriff auf Amazon Inspector .

Service-Administrator – Wenn Sie in Ihrem Unternehmen für Amazon Inspector-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Amazon Inspector. Ihre Aufgabe besteht darin, zu bestimmen, auf welche Amazon Inspector-Funktionen und -Ressourcen Ihre Service-Benutzer 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 dazu, wie Ihr Unternehmen IAM mit Amazon Inspector verwenden kann, finden Sie unter Funktionsweise von Amazon Inspector mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Amazon Inspector verfassen können. Beispiele für identitätsbasierte Amazon Inspector-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon Inspector.

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten bei anmelden. Sie müssen als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle authentifiziert (bei angemeldet AWS) sein.

Sie können sich bei AWS als Verbundidentität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt werden. AWS IAM Identity Center (IAM Identity Center)-Benutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie AWS über einen Verbund auf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, um welchen Benutzertyp es sich handelt, können Sie sich bei der AWS Management Console oder im - AWS Zugriffsportal anmelden. Weitere Informationen zur Anmeldung bei AWS finden Sie unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung - Benutzerhandbuch.

Wenn Sie AWS programmgesteuert auf zugreifen, AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (Command Line Interface, CLI) bereit, um Ihre Anforderungen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenständigen Signieren von Anforderungen finden Sie unter Signieren von AWS API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. empfiehlt beispielsweise, AWS 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 ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet und Sie melden sich mit der E-Mail-Adresse und dem Passwort an, mit dem 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

Fordern Sie als bewährte Methode menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, auf, den Verbund mit einem Identitätsanbieter zu verwenden, um AWS-Services mithilfe temporärer Anmeldeinformationen auf zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, die AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit AWS-Services Anmeldeinformationen auf zugreift, die über eine Identitätsquelle bereitgestellt werden. Wenn Verbundidentitäten auf 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 eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie für alle Ihre AWS-Konten und 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 in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. 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 in Ihrem AWS-Konto mit bestimmten Berechtigungen. 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 AWS-Services Sie jedoch eine Richtlinie direkt an

eine Ressource anfügen (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 in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anfragen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service 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.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. 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 - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, 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 steuern den Zugriff in , AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anfügen. Eine Richtlinie ist ein Objekt in , AWS das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in 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 AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was 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 aus der AWS Management Console, der AWS CLI 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 anfügen können AWS-Konto. Verwaltete Richtlinien umfassen - 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen 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 AWS WAF, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter Zugriffssteuerungsliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete 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-Kontrollrichtlinien (SCPs)– SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer 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. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder 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. Wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, erfahren Sie unter Logik zur Richtlinienbewertung im IAM-Benutzerhandbuch.

Funktionsweise von Amazon Inspector mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon Inspector zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit Amazon Inspector verwenden können.

IAM-Funktionen, die Sie mit Amazon Inspector verwenden können

IAM-Feature	Amazon Inspector-Unterstützung
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 Überblick über das AWS-Services Zusammenwirken von Amazon Inspector und anderen mit den meisten IAM-Funktionen finden Sie unter , AWS-Services die mit IAM funktionieren 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 Amazon Inspector-Richtlinien 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen 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 in unterschiedlichen befinden AWS-Konten, muss ein IAM-Administrator im vertrauenswürdigen Konto der Prinzipal-Entität (Benutzer oder Rolle) auch die Berechtigung für den 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.

Richtlinienaktionen für Amazon Inspector

Unterstützt Richtlinienaktionen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was 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 in der Regel denselben Namen wie die zugehörige AWS API-Operation. 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-Autorisierungs-Referenz.

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 Amazon Inspector-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon Inspector.

Richtlinienressourcen für Amazon Inspector

Unterstützt Richtlinienressourcen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was 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-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Amazon Inspector definierte Aktionen.

Beispiele für identitätsbasierte Amazon Inspector-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon Inspector.

Richtlinienbedingungsschlüssel für Amazon Inspector

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um festzulegen, wer Zugriff auf was 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 servicespezifische Bedingungsschlüssel. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel von Amazon Inspector finden Sie unter Bedingungsschlüssel für Amazon Inspector in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Inspector definierte Aktionen.

Beispiele für identitätsbasierte Amazon Inspector-Richtlinien 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 werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und viele AWS Ressourcen anfügen. 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.

Verwenden temporärer Anmeldeinformationen mit Amazon Inspector

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich der , die mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich AWS Management Console mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn

Sie beispielsweise AWS über den SSO-Link (Single Sign-On) Ihres Unternehmens auf zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. 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.

Sie können temporäre Anmeldeinformationen manuell mit der AWS CLI oder der AWS API erstellen. Sie können diese temporären Anmeldeinformationen dann verwenden, um auf zuzugreifen AWS. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipal-Berechtigungen für Amazon Inspector

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. 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 könnte die Funktionalität von Amazon Inspector beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon Inspector dazu Anleitungen gibt.

Serviceverknüpfte Rollen für Amazon Inspector

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören dem Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Weitere Informationen zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services , die mit IAM funktionieren. 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

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Amazon Inspector-Ressourcen. 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 Aktionen und Ressourcentypen, die von Amazon Inspector definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Inspector in der Service-Autorisierungs-Referenz.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon Inspector-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS -verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die -AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle 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 für Ihre Anwendungsfälle spezifisch 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 Service-Aktionen zu gewähren, wenn sie über eine

bestimmte verwendet werden AWS-Service, z. B. AWS CloudFormation. 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 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-Konsole

Um auf die Amazon Inspector-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon 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.

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen für die Konsole erteilen. 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 weiterhin die Amazon Inspector-Konsole verwenden können, fügen Sie den Entitäten auch die von Amazon Inspector `ConsoleAccess` oder `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 enthält Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder AWS API.

```
{
    "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": "*"
        }
    ]
}
```

Lesezugriff auf alle Amazon Inspector-Ressourcen zulassen

Dieses Beispiel zeigt eine Richtlinie, die schreibgeschützten Zugriff auf alle Amazon Inspector-Ressourcen erlaubt.

```
{
    "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": "*"
        }
    ]
}
```

Vollständigen Zugriff auf alle Amazon Inspector-Ressourcen zulassen

Dieses Beispiel zeigt eine Richtlinie, die vollen Zugriff auf alle Amazon 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 Von verwaltete Richtlinien für Amazon Inspector

Eine AWS von verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. Von AWS verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele häufige Anwendungsfälle bereitstellen, sodass Sie mit der Zuweisung von Berechtigungen für Benutzer, Gruppen und Rollen beginnen können.

Beachten Sie, dass von AWS verwaltete Richtlinien möglicherweise keine Berechtigungen mit den geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle 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 verwalteten AWS Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS von verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert, wirkt sich die Aktualisierung auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, an die die Richtlinie angefügt ist. aktualisiert am AWS wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer gestartet AWS-Service wird oder neue API-Operationen für vorhandene Services verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Von 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 Funktionalität von Amazon Inspector.
- `iam` – Ermöglicht Amazon Inspector das Erstellen der serviceverknüpften Rolle, `AmazonInspector2AgentlessServiceRole`. Dies ist erforderlich, damit Amazon Inspector Vorgänge wie das Abrufen von Informationen über Ihre Amazon EC2-Instances und Amazon-ECR-Repositorys und Container-Images, das Analysieren Ihres VPC-Netzwerks und das Beschreiben von Konten durchführen kann, die Ihrer Organisation zugeordnet 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. Nachdem der vertrauenswürdige Zugriff für Amazon Inspector in aktiviert wurde AWS Organizations, können Mitglieder des delegierten Administratorkontos

Einstellungen verwalten und Ergebnisse in ihrer gesamten Organisation anzeigen. Amazon Inspector

- `codeguru-security` – Ermöglicht Administratoren die Verwendung von Amazon Inspector, um Informationscodeausschnitte abzurufen und Verschlüsselungseinstellungen für Code zu ändern, der von CodeGuru Security gespeichert wird. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand für 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 Von verwaltete Richtlinie: AmazonInspector2ReadOnlyAccess

Sie können die `AmazonInspector2ReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Berechtigungen, die schreibgeschützten Zugriff auf Amazon Inspector ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `inspector2` – Ermöglicht schreibgeschützten Zugriff auf die Funktionalität von Amazon Inspector.
- `organizations` – Ermöglicht AWS Organizations die Anzeige von Details zur Abdeckung von Amazon Inspector für eine Organisation in .
- `codeguru-security` – Ermöglicht das Abrufen von Codeausschnitten aus der - CodeGuru Sicherheit. Ermöglicht auch die Anzeige von 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 Von verwaltete Richtlinie: AmazonInspector2ManagedCisPolicy

Sie können die `AmazonInspector2ManagedCisPolicy`-Richtlinie auch Ihren IAM-Entitäten anfügen. Diese Richtlinie sollte an eine Rolle angehängt werden, die Ihren Amazon EC2-Instances Berechtigungen zum Ausführen von CIS-Scans der Instance gewährt. Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das der Instance zugeordnet 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 zum Ausführen von CIS-Scans verwendet werden.

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

```
            "Action": [
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
            ],
            "Resource": "*",
        }
    ]
}
```

AWS Von verwaltete Richtlinie: AmazonInspector2ServiceRolePolicy

Sie können die `AmazonInspector2ServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es Amazon Inspector ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Inspector.

AWS Von verwaltete Richtlinie: AmazonInspector2AgentlessServiceRolePolicy

Sie können die `AmazonInspector2AgentlessServiceRolePolicy`-Richtlinie Ihren IAM-Entitäten nicht anfügen. Diese Richtlinie ist an eine serviceverknüpfte Rolle angehängt, 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 von AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für - AWS verwaltete Richtlinien für Amazon Inspector, seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite Dokumentverlauf von Amazon Inspector.

Änderung	Beschreibung	Datum
AmazonInspector2ManagedCisPolicy – Neue Richtlinie	Amazon Inspector hat eine neue verwaltete Richtlinie hinzugefügt, die Sie als	23. Januar 2024

Änderung	Beschreibung	Datum
	Teil eines Instance-Profils verwenden können, um CIS-Scans auf einer Instance zuzulassen.	
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, CIS-Scans auf Ziel-Instances zu starten.	23. Januar 2024
AmazonInspector2AgentlessServiceRolePolicy – Neue Richtlinie	Amazon Inspector hat eine neue serviceverknüpfte Rollenrichtlinie hinzugefügt, um das agentenlose Scannen von EC2-Instances zu ermöglichen.	8. November 2023
AmazonInspector2ReadOnlyAccess – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es schreibgeschützten Benutzern ermöglichen, Details zu Schwachstelleninformationen für Erkenntnisse zu Paketen von Schwachstellen abzurufen.	22. September 2023
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, Netzwerkkonfigurationen von Amazon EC2-Instances zu scannen, die Teil von Elastic Load Balancing-Zielgruppen sind.	31. August 2023

Änderung	Beschreibung	Datum
AmazonInspector2ReadOnlyAccess – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es schreibgeschützten Benutzern ermöglichen, Software Bill of Material (SBOM) für ihre Ressourcen zu exportieren.	29. Juni 2023
AmazonInspector2ReadOnlyAccess – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es schreibgeschützten Benutzern ermöglichen, Details zu Verschlüsselungseinstellungen für Ergebnisse des Lambda-Codescans für ihr Konto abzurufen.	13. Juni 2023
AmazonInspector2FullAccess – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, mit denen Benutzer einen vom Kunden verwalteten KMS-Schlüssel konfigurieren können, um Code in Ergebnissen des Lambda-Codescans zu verschlüsseln.	13. Juni 2023
AmazonInspector2ReadOnlyAccess – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es schreibgeschützten Benutzern ermöglichen, Details zum Lambda-Codescanstatus und zu den Ergebnissen für ihr Konto abzurufen.	02. Mai 2023

Änderung	Beschreibung	Datum
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, AWS CloudTrail serviceverknüpfte Kanäle in Ihrem Konto zu erstellen, wenn Sie das Lambda-Scannen aktivieren. Auf diese Weise kann Amazon Inspector CloudTrail Ereignisse in Ihrem Konto überwachen.	30. April 2023
AmazonInspector2FullAccess – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Benutzern ermöglichen, Details zu Ergebnissen von Code-Schwachstellen aus dem Lambda-Codescan abzurufen.	21. April 2023
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, Informationen über die benutzerdefinierten Pfade, die ein Kunde für Amazon EC2 Deep Inspect definiert hat, an Amazon EC2 Systems Manager zu senden.	17. April 2023

Änderung	Beschreibung	Datum
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, AWS CloudTrail serviceverknüpfte Kanäle in Ihrem Konto zu erstellen, wenn Sie das Lambda-Scannen aktivieren. Auf diese Weise kann Amazon Inspector CloudTrail Ereignisse in Ihrem Konto überwachen.	30. April 2023
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen 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 scannen.	28. Februar 2023

Änderung	Beschreibung	Datum
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen 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
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat eine neue Anweisung hinzugefügt, die es Amazon Inspector ermöglicht, Informationen über AWS Lambda Funktionen abzurufen, einschließlich jeder Ebenenversion, die jeder Funktion zugeordnet ist. Amazon Inspector verwendet diese Informationen, um Lambda-Funktionen auf Sicherheitsschwachstellen zu scannen.	28. November 2022

Änderung	Beschreibung	Datum
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat eine neue Aktion hinzugefügt, damit Amazon Inspector SSM-Zuordnungsausführungen beschreiben kann. Darüber hinaus hat Amazon Inspector zusätzliche Ressource nbereiche hinzugefügt, damit Amazon Inspector SSM-Zuordnungen mit `AmazonInspector2` -eigenen SSM-Dokumenten erstellen, aktualisieren, löschen und starten kann.	31. August 2022
AmazonInspector2ServiceRolePolicy Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat den Ressourcenbereich der Richtlinie aktualisiert, damit Amazon Inspector Softwarei nventar in anderen AWS Partitionen erfassen kann.	12. August 2022
AmazonInspector2ServiceRolePolicy – Aktualisierungen einer vorhandenen Richtlinie	Amazon Inspector hat den Ressourcenbereich der Aktionen neu strukturiert, sodass Amazon Inspector SSM-Zuordnungen erstellen , löschen und aktualisieren kann.	10. August 2022
AmazonInspector2ReadOnlyAccess – Neue Richtlinie	Amazon Inspector hat eine neue Richtlinie hinzugefügt, die schreibgeschützten Zugriff auf die Amazon Inspector-Funktionalität ermöglicht.	21. Januar 2022

Änderung	Beschreibung	Datum
AmazonInspector2FullAccess – Neue Richtlinie	Amazon Inspector hat eine neue Richtlinie hinzugefügt, die vollen Zugriff auf die Amazon Inspector-Funktionalität ermöglicht.	29. November 2021
AmazonInspector2ServiceRolePolicy – Neue Richtlinie	Amazon Inspector hat eine neue Richtlinie hinzugefügt, die es Amazon Inspector ermöglicht, Aktionen in anderen -Services in Ihrem Namen durchzuführen.	29. November 2021
Amazon Inspector hat mit der Verfolgung von Änderungen begonnen	Amazon Inspector hat mit der Verfolgung von Änderungen für seine von AWS verwalteten Richtlinien begonnen.	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`. Diese serviceverknüpfte Rolle ist eine IAM-Rolle, die direkt mit Amazon Inspector verknüpft ist. Sie wird von Amazon Inspector vordefiniert und enthält alle Berechtigungen, die Amazon Inspector zum Aufrufen anderer AWS-Services in Ihrem Namen benötigt.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Amazon Inspector, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon Inspector definiert die Berechtigungen seiner serviceverknüpften Rolle. Sofern keine andere Konfiguration festgelegt wurde, 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 serviceverknüpfte Rolle erst löschen, nachdem Sie die zugehörigen Ressourcen gelöscht haben. Dies schützt Ihre Amazon Inspector-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen 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 Dokumentation der serviceverknüpften Rolle für diesen Service zu überprüfen.

Serviceverknüpfte Rollenberechtigungen für Amazon Inspector

Amazon Inspector verwendet die serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonInspector2`. Diese serviceverknüpfte Rolle vertraut dem `inspector2.amazonaws.com` Service, die Rolle zu übernehmen.

Die Berechtigungsrichtlinie für die Rolle mit dem Namen ermöglicht Amazon Inspector `AmazonInspector2ServiceRolePolicy`die Durchführung von Aufgaben wie:

- Verwenden Sie Amazon Elastic Compute Cloud (Amazon EC2)-Aktionen, um Informationen über Ihre Instances und Netzwerkpfade abzurufen.
- Verwenden Sie - AWS Systems Manager Aktionen, um den Bestand von Ihren Amazon 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 zu Ihren Container-Images abzurufen.
- Verwenden Sie - AWS Lambda Aktionen, um Informationen zu Ihren Lambda-Funktionen abzurufen.
- Verwenden Sie - AWS Organizations Aktionen, um zugeordnete Konten zu beschreiben.
- Verwenden Sie CloudWatch Aktionen, um Informationen über den letzten Aufruf Ihrer Lambda-Funktionen abzurufen.
- Verwenden Sie ausgewählte IAM-Aktionen, um Informationen zu Ihren IAM-Richtlinien abzurufen, die zu Sicherheitslücken in Ihrem Lambda-Code führen könnten.

- Verwenden Sie CodeGuru Sicherheitsaktionen, um Scans des Codes in Ihren Lambda-Funktionen durchzuführen. Amazon Inspector verwendet die folgenden CodeGuru Sicherheitsaktionen:
  - codeguru-security: CreateScan – Gewährt die Berechtigung zum Erstellen eines CodeGuru Sicherheitsscans.
  - codeguru-security: GetScan – Erteilt die Berechtigung zum Abrufen von CodeGuru Sicherheitsscan-Metadaten.
  - codeguru-security: ListFindings – Erteilt die Berechtigung zum Abrufen der von CodeGuru Security generierten Ergebnisse.
  - codeguru-security: DeleteScansByCategory – Erteilt die Berechtigung für CodeGuru Sicherheit zum Löschen von Scans, die von Amazon Inspector initiiert wurden.
  - codeguru-security: BatchGetFindings – Gewährt die Berechtigung zum Abrufen eines Batches bestimmter Erkenntnisse, die von CodeGuru Security generiert wurden.
- Verwenden Sie ausgewählte Elastic Load Balancing-Aktionen, um Netzwerkscans von EC2-Instances, die Teil von Elastic Load Balancing-Zielgruppen sind, vorab zu formulieren.

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"
    }
   }
  }
 ]
}
```

Erstellen einer serviceverknüpften Rolle für Amazon Inspector

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Amazon Inspector in der AWS CLI, AWS Management Console der oder der API aktivieren AWS , erstellt Amazon Inspector die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon Inspector

Amazon Inspector erlaubt es 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 benötigen, empfehlen wir Ihnen, die `AWSServiceRoleForAmazonInspector2` serviceverknüpfte Rolle zu löschen. Bevor Sie die Rolle löschen können, müssen Sie Amazon Inspector in jeder deaktivieren AWS-Region , in der es aktiviert ist. Wenn Sie Amazon Inspector deaktivieren, wird die Rolle nicht für Sie gelöscht. Wenn Sie Amazon Inspector erneut aktivieren, kann es daher die vorhandene Rolle verwenden. Auf diese Weise können Sie vermeiden, dass eine nicht verwendete Entität 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 versuchen Sie es erneut.

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.

Berechtigungen von serviceverknüpften Rollen für Amazon Inspector Agentless-Scans

Das agentenlose Scannen von Amazon Inspector verwendet die serviceverknüpfte Rolle namens `AWSServiceRoleForAmazonInspector2Agentless`. Diese SLR ermöglicht es Amazon Inspector, einen Amazon-EBS-Volume-Snapshot in Ihrem Konto zu erstellen und dann von

diesem Snapshot aus auf die Daten zuzugreifen. Diese serviceverknüpfte Rolle vertraut dem `agentless.inspector2.amazonaws.com` Service, die Rolle zu übernehmen.

> **Important**
>
> Die Anweisungen in dieser serviceverknüpften Rolle verhindern, dass Amazon Inspector agentenlose Scans für jede EC2-Instance durchführt, die Sie mithilfe des `-InspectorEc2Exclusion`Tags von Scans ausgeschlossen haben. Darüber hinaus verhindern die Anweisungen, dass Amazon Inspector auf verschlüsselte Daten von einem Volume zugreift, wenn der KMS-Schlüssel, der zur Verschlüsselung verwendet wird, das `-InspectorEc2Exclusion`Tag hat. Weitere Informationen finden Sie unter Ausschließen von Instances von Amazon Inspector-Scans.

Die Berechtigungsrichtlinie für die Rolle mit dem Namen ermöglicht Amazon Inspector `AmazonInspector2AgentlessServiceRolePolicy`die Durchführung von Aufgaben wie:

- 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 Snapshots für Scans mit dem `InspectorScan` Tag-Schlüssel zu markieren.
  - Verwenden Sie Amazon EC2-Snapshot-Aktionen, um Snapshots zu erstellen, sie mit dem `InspectorScan` Tag-Schlüssel zu markieren und dann Snapshots von Amazon-EBS-Volumes zu löschen, die mit dem `InspectorScan` Tag-Schlüssel markiert wurden.
- 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 AWS KMS Kunden verwalteten Schlüsseln verschlüsselt sind. Amazon Inspector entschlüsselt Snapshots nicht, 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/*"
   }
  ]
}
```

Erstellen einer serviceverknüpften Rolle für das Scannen ohne Kundendienstmitarbeiter

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie Amazon Inspector in der AWS CLI, AWS Management Console der oder der API aktivieren AWS , erstellt Amazon Inspector die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für das Scannen ohne Kundendienstmitarbeiter

Amazon Inspector erlaubt es 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 Kundendienstmitarbeiter

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“ setzen. Weitere Informationen finden Sie unter [Link zur TBD-Einstellung des Scanmodus].

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 für Identität und Zugriff auf Amazon Inspector

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Inspector und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Amazon Inspector auszuführen
- Ich bin nicht autorisiert, iam durchzuführen:PassRole
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Amazon Inspector-Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in Amazon Inspector auszuführen

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 autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Amazon Inspector übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder serviceverknüpfte 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 meines AWS-Konto Zugriff auf meine Amazon Inspector-Ressourcen gewähren

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 Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (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 dazu, ob Amazon Inspector diese Funktionen unterstützt, finden Sie unter Funktionsweise von Amazon Inspector mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre AWS-Konten -Ressourcen in Ihrem Besitz finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten im IAM-Benutzerhandbuch.
- 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.

Überwachen von Amazon Inspector

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Inspector und Ihren anderen - AWS Lösungen aufrechtzuerhalten. AWS bietet Überwachungstools, mit denen Sie Amazon Inspector beobachten, Missstände melden und ggf. automatische Maßnahmen ergreifen können:

- Amazon EventBridge ist ein Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen einfach mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, S-Service-(SaaS)oftware-as-a-Anwendungen und - AWS Services bereit und leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können Sie Ereignisse überwachen, die in -Services auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im Amazon- EventBridge Benutzerhandbuch.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihrer AWS-Konto. CloudTrail stellt die Protokolldateien dann in einem von Ihnen angegebenen Amazon S3-Bucket bereit. Sie können feststellen, welche Benutzer und Konten aufgerufen haben AWS, von welcher Quell-IP-Adresse die Aufrufe stammen und wann die Aufrufe erfolgt sind. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Protokollieren von Amazon Inspector-API-Aufrufen mit AWS CloudTrail

Amazon Inspector ist in integriert, einem Service AWS CloudTrail, der die Aktionen eines IAM-Benutzers oder einer IAM-Rolle oder eines AWS-Service in Amazon Inspector aufzeichnet. CloudTrail erfasst alle API-Aufrufe für Amazon Inspector als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon Inspector-Konsole und Aufrufe der Amazon Inspector-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Amazon Inspector . Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie Folgendes ermitteln:

- Die Anforderung, die an Amazon Inspector gestellt wurde.
- Die IP-Adresse, von der die Anforderung erfolgt ist.
- Wer die Anfrage gestellt hat.
- Wann die Anforderung gestellt wurde.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

Amazon Inspector-Informationen in CloudTrail

CloudTrail wird beim Erstellen des Kontos AWS-Konto auf Ihrem aktiviert. Wenn eine Aktivität in Amazon Inspector auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen AWS-Service Ereignissen im Ereignisverlauf aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Amazon Inspector , einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon 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 erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter den folgenden Themen:

- Übersicht zum Erstellen eines Trails

- CloudTrail Von unterstützte Services 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-Aktionen werden von protokolliert CloudTrail. Alle Aktionen, die Amazon Inspector ausführen kann, sind in der Amazon Inspector API-Referenz dokumentiert. Zum Beispiel werden durch Aufrufe der `CreateFindingsReport`-, `ListCoverage`- und `UpdateOrganizationConfiguration`-Aktionen Einträge in den CloudTrail -Protokolldateien generiert.

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 CloudTrail -Element userIdentity.

Grundlegendes zu Amazon Inspector-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon 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 geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Amazon Inspector Scan-Informationen in CloudTrail

Amazon Inspector Scan ist in integriert CloudTrail. Alle API-Operationen von Amazon Inspector Scan werden als Verwaltungsereignisse protokolliert. Eine Liste der Amazon Inspector Scan-API-

Operationen, die Amazon Inspector in 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"
}
```


Compliance-Validierung für Amazon Inspector

Informationen darüber, ob ein in den Geltungsbereich bestimmter Compliance-Programme AWS-Service fällt, finden Sie AWS-Services unter im Geltungsbereich nach Compliance-Programm und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten unter AWS Artifact .

Ihre Compliance-Verantwortung bei der Verwendung von 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 Unterstützung der Compliance bereit:

- Schnellstartanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte für die Bereitstellung von Basisumgebungen in bereitgestellt AWS , die sich auf Sicherheit und Compliance konzentrieren.
- Architekturerstellung für HIPAA-Sicherheit und -Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe AWS von HIPAA-berechtigte Anwendungen erstellen können.

> **Note**
>
> Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen – Diese Sammlung von Arbeitsmappen und Leitfäden könnte für Ihre Branche und Ihren Standort gelten.
- AWS Kunden-Compliance-Leitfäden – Verstehen Sie das Modell der geteilten Verantwortung aus der Perspektive der Compliance. Die Leitfäden fassen die bewährten Methoden zur Sicherung zusammen AWS-Services und ordnen die Leitlinien den Sicherheitskontrollen in mehreren Frameworks zu (einschließlich National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Officer (PCI) und International Organization for Standardization (ISO)).
- Bewertung von Ressourcen mit 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 Sicherheitsstatus innerhalb von 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 den Umgang mit Risiken und die Einhaltung von Branchenstandards zu vereinfachen.

Ausfallsicherheit in Amazon Inspector

Die AWS globale -Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem

Netzwerk mit niedriger Latenz, hohem Durchsatz und hoher Redundanz 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 die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS Sicherheitsservices und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung mit den bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz in Security Pillar AWS Well-Architected Framework.

Sie verwenden durch 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 höchste Priorität AWS. Im Rahmen des AWS Cloud-Modells der übergreifenden Verantwortlichkeit AWS verwaltet ein Rechenzentrum, ein Netzwerk und eine Softwarearchitektur, die die Anforderungen der sicherheitssensibelsten Organisationen erfüllt. AWS ist für jede Reaktion auf Vorfälle in Bezug auf den AWS Config Service selbst verantwortlich. Als - AWS Kunde haben Sie auch eine gemeinsame Verantwortung für die Aufrechterhaltung der Sicherheit in der Cloud. Das bedeutet, dass Sie die Sicherheit kontrollieren, die Sie anhand der AWS Tools und Funktionen implementieren möchten, auf die Sie Zugriff haben, und für die Reaktion auf Vorfälle auf Ihre Seite des Modells der geteilten Verantwortung verantwortlich sind.

Indem Sie eine Sicherheitsgrundlinie einrichten, die die Ziele für Ihre Anwendungen erfüllt, die in der Cloud ausgeführt werden, 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 die Auswirkungen, die die Reaktion auf Vorfälle (IR) und Ihre Entscheidungen auf Ihre Unternehmensziele haben, besser verstehen können: AWS Leitfaden zur Reaktion auf Sicherheitsvorfälle , Whitepaper AWS Bewährte Methoden für die Sicherheit und das Whitepaper Sicherheitsaussicht des AWS Cloud Adoption Framework (CAF).

Amazon Inspector

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. Lesen Sie die folgenden Integraspecspecspecspecspecspecspecspecspecspecspecspecspecspecspecspecspecspecspecspecspecs

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 ermöglicht. Amazon ECR-Registrierungen hosten Ihre Container-Images in einer hochverfügbaren und skalierbaren Architektur. Sie können Amazon Inspector verwenden, um Container-Images in Ihren Amazon ECR-Repositorys nach anfälligen Betriebssystempaketen und Programmiersprachenpaketen zu durchsuchen.

Weitere Informationen zur Verwendung von Amazon ECR mit Amazon Integration von Amazon Inspector mit Amazon Elastic Container Registry (Amazon ECR)

Amazon Inspector Inspector-Integration mit AWS Security Hub

AWS Security Hubsammelt Sicherheitsdaten aus 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 Ihre Sicherheitslage, sondern bietet auch einen zentralen Ort für die Ergebnisse all Ihrer integrierten AWS Dienste und AWS Partner Network-Produkte. Durch die Aktivierung von Security Hub mit Amazon Inspector kann Security Hub automatisch die Ergebnisdaten von Amazon Inspector aufnehmen.

Weitere Informationen zur Verwendung von Security Hub mit Amazon Inspector Integration von Amazon Inspector 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 Inklusionsfilter 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 Deaktivieren von Amazon Inspector.

Integration von Amazon Inspector mit AWS Security Hub

Security Hub liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu überprüfen. Security Hub sammelt Sicherheitsdaten aus Ihren gesamten AWS Konten, -Services und weiteren unterstützten Produkten. Sie können die bereitgestellten Informationen verwenden, um Sicherheitstrends zu analysieren und Sicherheitstrends mit höchster Priorität zu identifizieren.

Amazon Inspector-Integration mit Security Hub ermöglicht es Ihnen, Ergebnisse von Amazon Inspector an Security Hub zu senden. Security Hub kann diese Erkenntnisse dann in die Analyse Ihres Sicherheitsnivels einbeziehen.

In AWS Security Hub werden Sicherheitsprobleme als Ergebnisse nachverfolgt. Einige Ergebnisse stammen von Problemen, die von anderen erkannt werden AWS -Dienstleistungen 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 anzeigen und Ergebnislisten anzeigen. Weitere Informationen zu den Ergebnissen in Security Hub finden Sie unter Ergebnisse anzeigen im AWS Security HubBenutzerhandbuch. Sie können auch den Status einer Untersuchung zu einem Ergebnis nachverfolgen. Siehe Ergreifen von Maßnahmen zu Ergebnissen im AWS Security Hub-Leitfaden.

Alle Funde in Security Hub verwenden ein Standard-JSON-Format, das so genannte AWS-Security Finding Format (ASFF). Das ASFF enthält Details über die Ursache des Problems, die betroffenen Ressourcen und den aktuellen Ergebnisstatus. 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.

Die Ergebnisse von Amazon Inspector anzeigen in AWS Security Hub

Die Ergebnisse von Amazon Inspector Classic und dem neuen Amazon Inspector sind im selben Panel im 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 einen Befund 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"
}
```

Aktivieren und Konfigurieren der Integration

Um die Integration von Amazon Inspector mit Amazon Inspector verwenden zu könnenAWS Security Hub, müssen Sie Security Hub aktivieren. Informationen zur Aktivierung von Security Hub finden Sie unter Einrichten von Security Hub im AWS Security Hub-Leitfaden.

Wenn Sie sowohl Amazon Inspector als auch Security Hub aktivieren, wird die Integration automatisch aktiviert und Amazon Inspector beginnt, die Ergebnisse an den Security Hub zu senden. Amazon Inspector sendet alle Ergebnisse unter Verwendung des Security Finding Format (ASFF) an AWS Security Hub.

Einstellung der Veröffentlichung von Ergebnissen an AWS Security Hub

So beenden Sie das Senden von Ergebnissen

Um keine Ergebnisse mehr an Security Hub zu senden, können Sie entweder die Security Hub-Konsole oder die API verwenden.

Siehe Deaktivieren und Aktivieren des Flows von Ergebnissen aus einer Integration (Konsole) oder Deaktivieren des Flows von Ergebnissen aus einer Integration (Security Hub Hub-API,AWS CLI) im -Leitfaden AWS Security Hub.

Von Amazon Inspector unterstützte Betriebssysteme und Programmiersprachen

Amazon Inspector kann Softwareanwendungen scannen, die auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances, Container-Images, die in Amazon Elastic Container Registry (Amazon ECR)-Repositorys gespeichert sind, und AWS Lambda Funktionen installiert sind. Bei ECR-Container-Images kann Amazon Inspector sowohl nach Schwachstellen im Betriebssystem als auch im Programmiersprachenpaket suchen. Für 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 Forschung und lizenzierte Datenfeeds.

Damit Amazon Inspector eine Ressource scannen kann, muss die Ressource ein unterstütztes Betriebssystem ausführen oder eine unterstützte Programmiersprache verwenden. In den Themen in diesem Abschnitt werden 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 seitdem von Anbietern eingestellt wurden. Amazon Inspector kann nur begrenzten Support für ein Betriebssystem bieten, nachdem ein Anbieter den Support für das Betriebssystem eingestellt hat.

Themen

Unterstützte Betriebssysteme: Amazon EC2-Scan

In der folgenden Tabelle sind die Betriebssysteme aufgeführt, die Amazon Inspector derzeit für Scans von Amazon EC2 unterstützt. Außerdem wird die Quelle der Anbietersicherheitsempfehlungen für jedes einzelne aufgeführt und ob dieses Betriebssystem mit der agentenbasierten oder agentenlosen Scanmethode gescannt werden kann. Weitere Informationen zu Scanmethoden finden Sie unter Agentbasiertes Scannen und Agentless-Scan.

> **Note**
>
> Linux-Betriebssystemerkennungen werden nur für das Standard-Paketmanager-Repository unterstützt und umfassen keine Anwendungen von Drittanbietern, erweiterte Support-Repositorys (z. B. BYOS RHEL, PG RHEL und RHEL für SAP) und optionale Repositorys wie Red Hat Application Streams.

Betriebssystem	Version	Sicherheitshinweise für Anbieter	Unterstützung für Agentless-Scans	Unterstützung für Agent-basierte Scans
AlmaLinux	8	ALSA	Ja	Ja
AlmaLinux	9	ALSA	Ja	Ja
Amazon Linux (AL2)	AL2	ALAS	Ja	Ja
Amazon Linux 2023 (AL2023)	AL2023	ALAS	Ja	Ja
Bottlerocket	1.7.0 und höher	GHSA, CVE	Nein	Ja
CentOS Linux (CentOS)	7	CESA	Ja	Ja
Debian Server (Buster)	10	DSA	Ja	Ja

Betriebssystem	Version	Sicherheitshinweise für Anbieter	Unterstützung für Agentless-Scans	Unterstützung für Agent-basierte Scans
Debian Server (Bullseye)	11	DSA	Ja	Ja
Debian Server (Buchwurm)	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	Sicherheitshinweise für Anbieter	Unterstützung für Agentless-Scans	Unterstützung für Agent-basierte Scans
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE	Ja	Ja
SUSE Linux Enterprise Server (SLES)	12,5	SUSE CVE	Ja	Ja
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE	Ja	Ja
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE	Ja	Ja
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE	Ja	Ja
Ubuntu (vertrauenswürdig)	14.04 (ESM)	USN, Ubuntu Pro	Ja	Ja
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro	Ja	Ja
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro	Ja	Ja
Ubuntu (Focal)	20.04 (LTS)	USN	Ja	Ja
Ubuntu (Jammy)	22.04 (LTS)	USN	Ja	Ja

Betriebssystem	Version	Sicherheitshinweise für Anbieter	Unterstützung für Agentless-Scans	Unterstützung für Agent-basierte Scans
Ubuntu (mantische Minotaur)	23.10	USN	Ja	Ja
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 (Katalina)	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 Inspect

Amazon Inspector unterstützt derzeit die folgenden Programmiersprachen beim Scannen von Amazon EC2 Linux-Instances auf Schwachstellen in Softwarepaketen von Drittanbietern:

- Java
- JavaScript
- Python

Amazon Inspector verwendet Systems Manager Distributor, um das Plugin bereitzustellen, das für die Deep-Inspection in Ihrer Amazon EC2-Instance verwendet wird. Systems Manager Distributor

unterstützt die Betriebssysteme, die als Unterstützte Paketplattformen und Architekturen im Systems Manager-Handbuch aufgeführt sind. Das Betriebssystem Ihrer Amazon EC2-Instance muss vom Systems Manager Distributor und Amazon Inspector unterstützt werden, damit Amazon Inspector Deep-Inspection-Scans durchführen kann.

> **Note**
>
> Eine gründliche Überprüfung wird für Bottlerocket-Betriebssysteme nicht unterstützt.

Unterstützte Betriebssysteme: CIS-Scan

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 zum Durchführen von Scans dieses Betriebssystems verwendet wird.

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-Scan mit Amazon Inspector

Amazon Inspector unterstützt derzeit das Scannen der folgenden Betriebssysteme beim Scannen von Container-Images in Amazon-ECR-Repositorys: Die Tabelle listet auch die Quelle der Anbietersicherheitshinweise für jedes Betriebssystem auf.

Betriebssystem	Version	Sicherheitshinweise für Anbieter
Alpine Linux (Alpine)	3.16	Alpine SecDB
Alpine Linux (Alpine)	3.17	Alpine SecDB
Alpine Linux (Alpine)	3.18	Alpine SecDB
Alpine Linux (Alpine)	3.19	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
CentOS Linux (CentOS)	7	CESA
Debian Server (Buster)	10	DSA
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA
Fedora	38	CVE
Fedora	39	CVE
OpenSUSE	15.5	CVE
Oracle Linux (Oracle)	7	ELSA
Oracle Linux (Oracle)	8	ELSA
Oracle Linux (Oracle)	9	ELSA
Photon OS	3	PHSA
Photon OS	4	PHSA

Betriebssystem	Version	Sicherheitshinweise für Anbieter
Photon OS	5	PHSA
Red Hat Enterprise Linux (RHEL)	7	RHSA
Red Hat Enterprise Linux (RHEL)	8	RHSA
Red Hat Enterprise Linux (RHEL)	9	RHSA
Rocky Linux	8	RLSA
Rocky Linux	9	RLSA
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12.5	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE
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

Betriebssystem	Version	Sicherheitshinweise für Anbieter
Ubuntu (Jammy)	22.04 (LTS)	USN
Ubuntu (Mantic Minotaur)	23.10	USN

Unterstützte Programmiersprachen: Amazon-ECR-Scan

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-Standardscan

Amazon Inspector Lambda-Standardscan unterstützt derzeit die folgenden Programmiersprachen beim Scannen von Lambda-Funktionen auf Schwachstellen 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: Codescan von Amazon Inspector Lambda

Amazon Inspector Lambda-Codescan unterstützt derzeit die folgenden Programmiersprachen, wenn Lambda-Funktionen auf Schwachstellen im Code gescannt werden:

- 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

Trennung von Betriebssystemen

Die Standardunterstützung des Anbieters für die in den folgenden Tabellen aufgeführten Betriebssysteme wurde vom Anbieter eingestellt. In den Tabellen wird in der Spalte Dis microSD angegeben, wann der Anbieter den Standard-Support für ein Betriebssystem eingestellt hat.

Amazon Inspector hat zuvor vollen Support für diese Betriebssysteme bereitgestellt und scannt weiterhin Amazon EC2-Instances und Amazon-ECR-Container-Images, auf denen sie ausgeführt werden. In Übereinstimmung mit den Anbieterrichtlinien werden die Betriebssysteme jedoch nicht mehr mit Patches aktualisiert und in vielen Fällen werden keine neuen Sicherheitshinweise mehr für sie veröffentlicht. Darüber hinaus entfernen einige Anbieter vorhandene Sicherheitshinweise und Erkennungen aus ihren Feeds, wenn ein betroffenes Betriebssystem das Ende des Standard-Supports erreicht. Folglich generiert Amazon Inspector möglicherweise keine Ergebnisse mehr für bekannte CVEs. Alle Erkenntnisse, die Amazon Inspector für ein eingestelltes Betriebssystem generiert, sollten nur zu Informationszwecken verwendet werden.

Als bewährte Sicherheitsmethode und für eine kontinuierliche Abdeckung von Amazon Inspector empfehlen wir Ihnen, auf eine aktuelle, unterstützte Version eines Betriebssystems umzusteigen.

Deaktivieren von Betriebssystemen: Amazon EC2-Scan

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 (Impisch)	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

Betriebssysteme außer Betrieb nehmen: Amazon-ECR-Scan

Betriebssystem	Version	Nicht mehr angeboten
Alpine Linux (alpin)	3.12	01.Mai 2022
Alpine 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 (Impisch)	21.10	31. Juli 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024

Deaktivieren von Amazon Inspector

Sie können Amazon Inspector in jeder deaktivieren, AWS-Region indem Sie die Amazon 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 ein deaktivierenAWS-Konto, wird Amazon Inspector für dieses Konto automatisch deaktiviert. Informationen zum Deaktivieren 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 Scaneinstellungen, Unterdrückungsregeln und Filter und Ergebnisse von Amazon Inspector für das Konto in dieser Region gelöscht.

Die Verwendung von Amazon Inspector wird Ihnen nicht in Rechnung gestellt, solange es für Ihr Konto in dieser Region deaktiviert ist. Nachdem Sie Amazon Inspector deaktiviert haben, können Sie es zu einem späteren Zeitpunkt wieder 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 Amazon EC2-Scannen von Amazon Inspector deaktivieren, werden die folgenden von Amazon Inspector verwendeten SSM-Zuordnungen gelöscht:

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`. Darüber hinaus wird das über diese Zuordnung installierte Amazon Inspector SSM-Plugin von allen Ihren Windows Hosts entfernt. Weitere Informationen finden Sie unter Scannen von Windows Instances.

Voraussetzungen

Abhängig von Ihrem Kontotyp müssen Sie möglicherweise zusätzliche Schritte unternehmen, bevor Sie Amazon Inspector wie folgt deaktivieren:

- Wenn Sie über ein eigenständiges Amazon Inspector-Konto verfügen, können Sie es jederzeit deaktivieren.
- Wenn Sie ein Mitgliedskonto in einer Amazon 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 Aufheben der Zuordnung von Mitgliedskonten in Amazon Inspector.

> **Note**
>
> Durch das Aufheben der Zuordnung eines Kontos wird Amazon Inspector für dieses Konto nicht deaktiviert, sondern ein getrenntes Mitgliedskonto wird zu einem eigenständigen Konto.

> **Note**
>
> Wenn Sie Amazon Inspector als delegierten Administrator deaktivieren, wird die Funktion zur automatischen Aktivierung für Ihre Organisation deaktiviert.

Amazon Inspector deaktivieren

Console

So deaktivieren Sie Amazon Inspector

1. Öffnen Sie die Amazon 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 aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie Deaktivieren in das Textfeld ein und wählen Sie dann Inspector deaktivieren aus.

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 Anforderung die Konto-IDs an, die Sie deaktivieren, und `EC2, ECR, LAMBDA` für , `resourceTypes` um alle Scans zu deaktivieren, wodurch das Konto deaktiviert wird.

Kontingente für Amazon Inspector

Ihr AWS Konto verfügt über die folgenden Kontingente für Amazon Inspector pro Region.

Ressource	Standard	Kommentare
Unterdrückungsregeln	500	Die maximale Anzahl gespeicherter Unterdrückungsregeln pro AWS Konto und Region. Sie können keine Kontingenterhöhung beantragen.
Amazon EC2-Netzwerkergebnisse	10.000	Die maximale Anzahl von Amazon EC2-Netzwerkergebnissen pro AWS Konto. Sie können keine Kontingenterhöhung beantragen.
Mitgliedskonten	10000	Die maximale Anzahl von Mitgliedskonten, die einem delegierten Amazon Inspector-Administratorkonto zugeordnet sind. Dieses Limit basiert auf AWS Organizations, siehe Kontingente für AWS Organizations.

Ressource	Standard	Kommentare
CIS-Scankonfigurationen	500	Die maximale Anzahl von CIS-Scank onfigurationen. Sie können keine Kontingenterhöhung beantragen.

Eine Liste der mit Amazon Inspector Classic verknüpften Kontingente finden Sie unter Amazon Inspector Service Quotas im Allgemeine AWS-Referenz.

Eine Liste der Kontingente, die Organizations zugeordnet sind, finden Sie unter Organizations-Servicekontingente im 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 AWSServicebedingungen („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
South America (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 beschriebenAWS-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
Asia Pacific (Tokyo)	ap-northeast-1
Europa (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (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.

Dokumentverlauf für das Amazon 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 den Aufbewahrungszeitraum für geschlossene Erkenntnisse von 30 Tagen auf 7 Tage. Weitere Informationen finden Sie unter Erkenntnisse in Amazon Inspector verstehen.	12. Februar 2024
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicy Richtlinie eine neue Anweisung 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, AmazonInspector2ManagedCisPolicy Richtlinie , hinzugefügt, die Sie als Teil von in einem Instance-Profil verwenden können, um CIS-Scans auf einer Instance zuzulassen.	23. Januar 2024
Neue Funktion	Amazon Inspector aktualisiert jetzt die Dauer des erneuten	23. Januar 2024

	ECR-Scans von Container-Images, wenn Sie sie abrufen. Informationen zum Ändern Ihrer Dauer des erneuten Scannens basierend auf Push- oder Pull-Daten finden Sie unter Konfigurieren der Dauer des erneuten ECR-Scans.	
Neue Funktion	Amazon Inspector kann jetzt Center for Internet Security (CIS)-Scans auf EC2-Instances ausführen. Weitere Informationen finden Sie unter CIS-Scans von Amazon Inspector.	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 zur Richtlinie finden Sie unter Agentless-Scan.	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 Agentless-Scan.	8. November 2023
Neue unterstützte Ressourcen	Amazon Inspector unterstützt jetzt das Scannen von MacOS-Amazon EC2Instances. Weitere Informationen finden Sie unter Unterstützte Betriebssysteme: Amazon EC2-Scan 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-Instances zu scannen, die Teil von Elastic Load Balancing-Zielgruppen sind.	31. August 2023

Neues Feature	Amazon Inspector stellt jetzt Details zu Schwachstelleninformationen für Erkenntnisse zu Paketen bereit.	31. Juli 2023
Aktualisierte Funktionalität	Amazon Inspector hat neue Berechtigungen hinzugefügt, die es schreibgeschützten Benutzern ermöglichen, Software Bill of Material (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 zum Scannen von Lambda-Code identifiziert wurde. Darüber hinaus bietet das Scannen von Lambda-Code jetzt Vorschläge für das Umschreiben Ihres Codes.	13. Juni 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ReadOnlyAccess Richtlinie eine neue Anweisung hinzugefügt. Die neuen Anweisungen ermöglichen es schreibgeschützten Benutzern, Details zum Lambda-Codescanstatus und zu den Ergebnissen für ihr Konto abzurufen.	2. Mai 2023
Neues Feature	Amazon Inspector hat eine Schwachstellendatenbanksuche hinzugefügt, mit der Sie überprüfen können, ob Amazon Inspector ein bestimmtes CVE abdeckt.	1. Mai 2023
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicy Richtlinie neue Berechtigungen hinzugefügt, die es Amazon Inspector ermöglichen, AWS CloudTrail serviceverknüpfte Kanäle in Ihrem Konto zu erstellen, wenn Sie das Lambda-Scannen aktivieren. Auf diese Weise kann Amazon Inspector CloudTrail Ereignisse in Ihrem Konto überwachen.	30. April 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2FullAccess Richtlinie eine neue Anweisung hinzugefügt. Die neue Anweisung ermöglicht es Benutzern, Details zu den Ergebnissen von Code-Schwachstellen aus dem Lambda-Codescan abzurufen.	17. April 2023
Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicy Richtlinie eine neue Anweisung hinzugefügt. Die neue Anweisung ermöglicht es Amazon Inspector, Informationen über die benutzerdefinierten Pfade, die Sie für Amazon EC2-EC2-Deep-Inspection definiert haben, an Amazon EC2 Systems Manager zu senden.	17. April 2023
Neues Feature	Amazon Inspector fügt zusätzliche Unterstützung für Linux-EC2-Instances in Form von Amazon Inspector Deep Inspector hinzu, die Ihre Instances auf Paketschwachstellen in Sprachpaketen für die Anwendungsprogrammierung scannt.	17. April 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicy Richtlinie eine neue Anweisung 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 scannen.	28. Februar 2023
Neues Feature	Amazon Inspector fügt zusätzliche Unterstützung für Lambda-Funktionen in Form von Lambda-Codescan hinzu, die den Entwicklercode Ihrer Lambda-Funktionen auf Sicherheitsschwachstellen scannen.	28. Februar 2023

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicy Richtlinie eine neue Anweisung hinzugefügt. Die neue Anweisung ermöglicht es Amazon Inspector, Informationen CloudWatch darüber abzurufen, wann eine -AWS LambdaFunktion 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 AmazonInspector2ServiceRolePolicy Richtlinie eine neue Anweisung hinzugefügt. Die neue Anweisung ermöglicht es Amazon Inspector, Informationen über Ihre AWS Lambda Funktionen abzurufen. Amazon Inspector verwendet diese Informationen, um Ihre Lambda-Funktionen auf Sicherheitsschwachstellen zu scannen.	28. November 2022
Neues Feature	Amazon Inspector bietet Unterstützung für Scanfunktionen AWS Lambda.	28. November 2022

Aktualisierter Inhalt	Verfahren, Richtlinienbeispiele und Tipps zum Exportieren 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-Abdeckung Ihrer AWS Umgebung mithilfe der Amazon Inspector-Konsole hinzugefügt. Die Informationen enthalten Beschreibungen der Statuswerte für einzelne Ressourcen in Ihrer Umgebung.	7. Oktober 2022
Neues Feature	Amazon Inspector bietet jetzt zusätzliche Details zur Behebung von Paketschwachstellen. Den Erkenntnisdetails wurden neue Felder hinzugefügt. Die neuen Felder enthalten Kontext darüber, ob ein Fix über ein Paket-Update verfügbar ist. Wenn eine Korrektur verfügbar ist, zeigt der Abschnitt Vorgeschlagene Korrektur eines Ergebnisses die Befehle an, die Sie ausführen können, um die Korrektur vorzunehmen.	02. September 2022

Aktualisierte Funktionalität	Amazon Inspector hat der AmazonInspector2ServiceRolePolicy Richtlinie eine neue Aktion hinzugefügt. Die neue Aktion ermöglicht es Amazon Inspector, SSM-Zuordnungsausführungen zu beschreiben. Amazon Inspector hat auch zusätzlichen Ressourcenumfang hinzugefügt, damit Amazon Inspector SSM-Zuordnungen 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 Windows unterstützte Betriebssysteme ausgeführt werden. Scans von Windows Hosts werden vom Amazon Inspector-SSM-Plugin durchgeführt, das über neue SSM-Zuordnungen installiert und aufgerufen wird, die automatisch von Amazon Inspector erstellt werden.	31. August 2022

Aktualisierte Funktionalität	Amazon Inspector hat den Ressourcenbereich der AmazonInspector2ServiceRolePolicy Richtlinie aktualisiert, damit Amazon Inspector Softwareinventar in anderen AWS Partitionen erfassen kann.	12. August 2022
Aktualisierte Funktionalität	In der AmazonInspector2ServiceRolePolicy Richtlinie hat Amazon Inspector den Ressourcenbereich der Aktionen neu strukturiert, sodass Amazon Inspector SSM-Zuordnungen erstellen, löschen und aktualisieren kann.	10. August 2022

Neues Feature	Amazon Inspector unterstützt jetzt das Ändern Ihrer Einstellung für die Dauer des automatischen erneuten ECR-Scans. Die Einstellung für die Dauer des automatischen erneuten Scannens von Amazon ECR bestimmt, wie lange Amazon Inspector kontinuierlich Images überwacht, die in Repositorys übertragen werden. Wenn ein Image älter als die Scandauer ist, scannt Amazon Inspector das Image nicht mehr und schließt alle vorhandenen Ergebnisse dafür. Für alle neuen Konten ist die Dauer des automatischen erneuten ECR-Scans automatisch auf Lebensdauer festgelegt. Zuvor erstellte Konten hatten eine automatisierte ECR-Wiederholungsdauer von 30 Tagen, aber Sie können jetzt zwischen 30 Tagen, 180 Tagen oder Lebensdauer für Scans wählen.	25. Juni 2022

Neue Funktionalität	Amazon Inspector hat eine neue AWS verwaltete Richtlinie, die AmazonInspector2ReadOnlyAccess Richtlinie , hinzugefügt, um schreibgeschützten Zugriff auf die Funktionalität von Amazon Inspector zu ermöglichen.	21. Januar 2022
Allgemeine Verfügbarkeit	Dies ist die erste öffentliche Version des Amazon 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.