aws

Benutzerhandbuch

Amazon Inspector Classic

Version Latest

Amazon Inspector Classic: Benutzerhandbuch

Table of Contents

Hinweis zum Ende des Supports: Am 20. Mai 2026 AWS wird der Support für Amazon Inspector Classic eingestellt. Nach dem 20. Mai 2026 können Sie nicht mehr auf die Amazon Inspector Classic-Konsole oder die Amazon Inspector Classic-Ressourcen zugreifen. Amazon Inspector Classic ist nicht mehr für neue Konten und Konten verfügbar, die in den letzten 6 Monaten keine Bewertung abgeschlossen haben. Für alle anderen Konten bleibt der Zugriff bis zum 20. Mai 2026 gültig. Danach können Sie nicht mehr auf die Amazon Inspector Classic-Konsole oder die Amazon Inspector Classic-Ressourcen zugreifen. Weitere Informationen finden Sie unter Ende des Supports für Amazon Inspector Classic.

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.

Was ist Amazon Inspector-Scan

> **Note**
>
> Der neue Amazon Inspector, eine komplett überarbeitete und neu gestaltete Version von Amazon Inspector Classic, ist jetzt überall verfügbar. AWS-Regionen Der neue Amazon Inspector wurde erweitert und unterstützt nun zusätzlich zu Instances auch Container-Images, die sich in Amazon Elastic Container Registry (Amazon ECR) befinden. EC2 Der neue Amazon Inspector bietet Unterstützung für mehrere Konten durch Integration und kontinuierliche Scans nach Softwareschwachstellen und Netzwerkerreichbarkeit auf der Grundlage gängiger Sicherheitslücken und Sicherheitslücken (). AWS Organizations CVEs Wir empfehlen Ihnen, diese und andere neue und verbesserte Funktionen zu testen und zu nutzen und von dem deutlich verbesserten Sicherheitswert zu profitieren. Weitere Informationen zu Funktionen und Preisen für den neuen Amazon Inspector finden Sie unter Amazon Inspector. Informationen zum Umstieg auf den neuen Amazon Inspector finden Sie unterEnde der Unterstützung für Amazon Inspector Classic.

Amazon Inspector-Scan testen Sie die Netzwerkzugänglichkeit Ihrer EC2 Amazon-Instances und den Sicherheitsstatus Ihrer Anwendungen, die auf diesen Instances ausgeführt werden. Amazon Inspector-Scan bewertet Schwachstellen in Anwendungen sowie Abweichungen von bewährten Methoden. Im Anschluss an eine Bewertung erstellt Amazon Inspector-Scan eine detaillierte Liste der Sicherheitsergebnisse, die nach Schweregrad geordnet ist.

Mit Amazon Inspector Classic können Sie die Bewertung von Sicherheitslücken in Ihren Entwicklungs- und Bereitstellungspipelines oder für statische Produktionssysteme automatisieren. Sie können dadurch Sicherheitstests regelmäßig im Rahmen der Entwicklungs- und IT-Vorgänge ausführen.

Amazon Inspector Classic bietet auch eine vordefinierte Software namens Agent, die Sie optional im Betriebssystem der EC2 Instances installieren können, die Sie bewerten möchten. Der Agent überwacht das Verhalten der EC2 Instances, einschließlich Netzwerk-, Dateisystem- und Prozessaktivität. Außerdem sammelt er eine Vielzahl von Verhaltens- und Konfigurationsdaten (Telemetrie).

> **Important**
>
> AWS garantiert nicht, dass durch Befolgung der bereitgestellten Empfehlungen alle potenziellen Sicherheitsprobleme behoben werden. Die von Amazon Inspector Classic generierten Ergebnisse hängen von Ihrer Wahl der Regelpakete ab, die in jeder Bewertungsvorlage enthalten sind, vom Vorhandensein von AWS Nichtkomponenten in Ihrem System und anderen Faktoren. Sie sind für die Sicherheit von Anwendungen, Prozessen und Tools verantwortlich, die auf AWS Services ausgeführt werden. Weitere Informationen finden Sie im Modell der AWS übergreifende Verantwortlichkeit für Sicherheit.

> **Note**
>
> AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der die in der AWS Cloud angebotenen Dienste ausgeführt werden. Diese Infrastruktur besteht aus der Hardware, Software, dem Netzwerk und den Einrichtungen, auf und in denen AWS Services ausgeführt werden. AWS bietet mehrere Berichte von externen Prüfern, die bestätigt haben, dass wir eine Vielzahl von Computersicherheitsstandards und -vorschriften einhalten. Weitere Informationen erhalten Sie unter AWS Cloud-Compliance.

Informationen zur Amazon Inspector Classic-Terminologie finden Sie unterTerminologie und Konzepte von Amazon Inspector Classic.

Vorteile von Amazon Inspector-Scan

Hier sind einige Hauptvorteile von Amazon Inspector-Scan:

- Integrieren Sie automatisierte Sicherheitsüberprüfungen in Ihre regulären Bereitstellungs- und Produktionsprozesse — Beurteilen Sie die Sicherheit Ihrer AWS Ressourcen für forensische Untersuchungen, Problembehebungen oder aktive Prüfungen. Führen Sie die Bewertungen während des Entwicklungsprozesses oder in einer stabilen Produktionsumgebung aus.
- Finden Sie Sicherheitsprobleme bei Anwendungen — Automatisieren Sie die Sicherheitsbeurteilung Ihrer Anwendungen und identifizieren Sie proaktiv Sicherheitslücken. Dies ermöglicht Ihnen, neue Anwendungen schnell zu entwickeln und zu durchlaufen und die Compliance mit bewährten Methoden und Richtlinien zu bewerten.

- Gewinnen Sie ein tieferes Verständnis Ihrer AWS Ressourcen — Bleiben Sie über die Aktivitäts- und Konfigurationsdaten Ihrer AWS Ressourcen auf dem Laufenden, indem Sie die Ergebnisse von Amazon Inspector Classic überprüfen.

Funktionen von Amazon Inspector-Scan

Hier sind einige Hauptfunktionen von Amazon Inspector-Scan:

- Engine zum Scannen von Konfigurationen und zur Aktivitätsüberwachung — Amazon Inspector Classic bietet einen Agenten, der die System- und Ressourcenkonfiguration analysiert. Außerdem werden die Aktivitäten überwacht, um festzustellen, wie ein Bewertungsziel aussieht, wie es sich verhält und welche Komponenten von ihm abhängig sind. Die Kombination dieser Telemetrie bietet ein vollständiges Bild des Ziels und seiner potenziellen Sicherheits- oder Compliance-Probleme.
- Integrierte Inhaltsbibliothek — Amazon Inspector Classic enthält eine integrierte Bibliothek mit Regeln und Berichten. Diese beinhalten Überprüfungen auf bewährte Methoden, allgemeinen Compliance-Standards und Schwachstellen. Die Überprüfungen umfassen detaillierte empfohlene Schritte zur Behebung möglicher Sicherheitsprobleme.
- Automatisierung über eine API — Amazon Inspector Classic kann über eine API vollständig automatisiert werden. Dies ermöglicht Ihnen, Sicherheitstests in den Entwicklungs- und Designprozess einzubeziehen, einschließlich der Auswahl, Durchführung und Berichterstattung über die Ergebnisse dieser Tests.

Zugriff auf Amazon Inspector-Scan

Sie können auf eine der folgenden Arten mit dem Amazon Inspector-Scan arbeiten:

Amazon Inspector-Scan

Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.

Die Konsole ist eine browserbasierte Schnittstelle, mit der Sie auf den Amazon Inspector-Scan zugreifen und ihn verwenden können.

AWS SDKs

AWS stellt Software Development Kits (SDKs) zur Verfügung, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen. Dazu gehören

Java, Python, Ruby, .NET, iOS, Android und vieles mehr. Sie sind SDKs gut zur Einrichtung des programmgesteuerten Zugriffs auf den Amazon Inspector-Scan geeignet. Weitere Informationen zu AWS SDKs, inklusive einer Anleitung zum Herunterladen und Installieren, finden Sie unter Tools für Amazon Web Services.

Amazon Inspector-Süß-API

Sie können auf Amazon Inspector-Scan und AWS programmgesteuert über die HTTPS-API von Amazon Inspector Classic, mit der Sie HTTPS-Anfragen direkt an den Service ausgeben können. Weitere Informationen finden Sie in der Amazon Inspector-Class-Referenz.

AWS -Befehlszeilen-Tools

Sie können die AWS Befehlszeilen-Tools von verwenden, um Befehle in der Befehlszeile Ihres Systems auszuführen, mit denen Amazon Inspector-Classic durchgeführt werden. Die Befehlszeilen-Tools können auch beim Erstellen von Skripts für AWS -Aufgaben hilfreich sein. Weitere Informationen finden Sie in der Amazon AWS Inspector-Scan.

Terminologie und Konzepte von Amazon Inspector Classic

Wenn Sie mit Amazon Inspector Classic beginnen, können Sie davon profitieren, mehr über die wichtigsten Konzepte zu erfahren.

Amazon Inspector Classic-Agent

Ein Software-Agent, den Sie auf den EC2 Instances installieren können, die im Bewertungsziel enthalten sind. Außerdem erfasst der Agent umfassende Konfigurationsdaten (Telemetrie). Weitere Informationen finden Sie unter Amazon Inspector Classic-Agenten.

Bewertungslauf

Der Prozess der Erkennung potenzieller Sicherheitsprobleme durch die Analyse der Konfiguration des Bewertungsziels anhand von bestimmten Regelpaketen. Während eines Bewertungslaufs überwacht, erfasst und analysiert Amazon Inspector Konfigurationsdaten (Telemetrie) von Ressourcen im angegebenen Ziel. Anschließend analysiert Amazon Inspector die Daten und vergleicht sie mit einem Satz von Sicherheitsregelpaketen, die in der während des Bewertungslaufs verwendeten Bewertungsvorlage angegeben sind. Ein abgeschlossener Bewertungslauf führt zu einer Liste von Ergebnissen mit potenziellen Sicherheitsproblemen verschiedener Schweregrade. Weitere Informationen finden Sie unter Amazon Inspector Classic Bewertungsvorlagen und Bewertungsläufe.

Bewertungsziel

Im Kontext von Amazon Inspector Classic eine Sammlung von AWS-Ressourcen, die als Einheit zusammenarbeiten, um Sie beim Erreichen Ihrer Geschäftsziele zu unterstützen. Amazon Inspector Classic bewertet den Sicherheitsstatus der Ressourcen, die das Bewertungsziel bilden.

> **Important**
>
> Derzeit können Ihre Amazon Inspector Classic-Bewertungsziele nur aus EC2 Instances bestehen. Weitere Informationen finden Sie unter Amazon Inspector Classic-Servicebeschränkungen

Um ein Amazon Inspector Classic-Bewertungsziel zu erstellen, müssen Sie Ihre EC2 Instances zunächst mit Schlüssel-Wert-Paaren Ihrer Wahl kennzeichnen. Als Nächstes können Sie eine Ansicht dieser mit Tags versehenen EC2 Instances mit gemeinsamen Schlüsseln oder gemeinsamen Werten erstellen. Weitere Informationen finden Sie unter Bewertungsziele von Amazon Inspector Classic.

Bewertungsvorlage

Eine Konfiguration, die während des Bewertungslaufs verwendet wird. Die Vorlage umfasst Folgendes:

- Regelpakete, die Amazon Inspector Classic zur Bewertung Ihres Bewertungsziels verwendet
- Amazon SNS SNS-Themen, an die Amazon Inspector Classic Benachrichtigungen über den Status und die Ergebnisse der Testläufe senden soll
- Tags (Schlüssel-Wert-Paare), die Sie Ergebnissen zuweisen können, die vom Bewertungslauf generiert werden
- Die Dauer des Bewertungslaufs

Erkenntnis

Ein potenzielles Sicherheitsproblem, das Amazon Inspector Classic während eines Bewertungslaufs des angegebenen Ziels entdeckt. Die Ergebnisse werden in der Amazon Inspector Classic-Konsole angezeigt oder über die API abgerufen. Sie enthalten sowohl eine detaillierte Beschreibung des Sicherheitsproblems als auch eine Empfehlung, wie es behoben werden kann. Weitere Informationen finden Sie unter Ergebnisse von Amazon Inspector Classic.

Regel

Im Rahmen von Amazon Inspector Classic wird eine Sicherheitsüberprüfung während eines Bewertungslaufs durchgeführt. Wenn eine Regel ein potenzielles Sicherheitsproblem erkennt, generiert Amazon Inspector Classic ein Ergebnis, das das Problem beschreibt.

Regelpaket

Im Kontext von Amazon Inspector Classic eine Sammlung von Regeln. Ein Regelpaket entspricht einem Sicherheitsziel, das Sie möglicherweise haben. Sie können Ihr Sicherheitsziel angeben, indem Sie bei der Erstellung einer Amazon Inspector Classic-Bewertungsvorlage das entsprechende Regelpaket auswählen. Weitere Informationen finden Sie unter Amazon Inspector Classic: Regelpakete und Regeln.

Telemetrie

Informationen zum installierten Paket und Softwarekonfiguration für eine EC2 Instance. Amazon Inspector Classic sammelt die Daten während eines Bewertungslaufs.

Amazon Inspector Classic-Servicebeschränkungen

Die folgende Tabelle zeigt die Amazon Inspector Classic-Limits für ein AWS-Konto.

> **Important**
>
> Derzeit können Ihre Bewertungsziele nur aus EC2 Instances bestehen.

Im Folgenden sind die Amazon Inspector Classic-Limits pro AWS-Konto und Region aufgeführt:

Ressource	Standardlimit	Kommentare
Instances in laufenden Bewertungen	500	Die maximale Anzahl von EC2 Instances, die in alle laufenden Bewertungen pro Konto und Region einbezogen werden können.

Ressource	Standardlimit	Kommentare
Bewertungsläufe	50000	Die maximale Anzahl der Bewertungsläufe, die Sie pro Konto und pro Region erstellen können. Sie können mehrere Bewertung släufe gleichzei tig durchführen, solange die für diese Läufe verwendet en Bewertung sziele keine sich überschneidenden EC2 Instanzen enthalten.
-Bewertungsvorlagen	500	Die maximale Anzahl von Bewertung svorlagen, über die Sie zu einem bestimmten Zeitpunkt pro Konto und pro Region verfügen können.
-Bewertungsziele	50	Die maximale Anzahl von Bewertung szielen, über die Sie zu einem bestimmte n Zeitpunkt pro Konto und pro Region verfügen können.

Sofern nicht anders angegeben, können diese Grenzwerte auf Anfrage erhöht werden, indem Sie sich an das AWS -Support Center wenden.

Amazon Inspector-Scan

Die Preise von Amazon Inspector Classic basieren auf der Anzahl der in jeder Bewertung enthaltenen EC2 Instances und den in diesen Bewertungen verwendeten Regelpaketen.

Die Preisgestaltung für das Regelpaket zur Netzwerkerreichbarkeit

Amazon Inspector Classic-Bewertungen mit den Regelpaketen zur Netzwerkerreichbarkeit werden pro Instanz pro Bewertung (Instance-Bewertung) pro Monat berechnet. Wenn Sie beispielsweise 1 Assessment für 1 Instance durchführen, ist das 1 Instance-Assessment. Wenn Sie 1 Assessment für 10 Instances ausführen, sind das 10 Instance-Assessments. Die Preise beginnen bei 0,15 USD pro Instance-Assessment und Monat, wobei Mengenrabatte bis zu 0,04 USD pro Instance-Assessment und Monat betragen können.

Einzelheiten zur kostenlosen Testversion

Die ersten 90 Tage mit Amazon Inspector Classic	Preis pro Testinstanz
Die ersten 250 Instance-Bewertungen	0,00$

Preisdetails

In einem bestimmten Monat	Preis pro Testinstanz
Die ersten 250 Instance-Bewertungen	0,15$
Die nächsten 750 Instanzbewertungen	0,13$
Die nächsten 4.000 Instanzbewertungen	$0.10
Die nächsten 45.000 Instanzbewertungen	0,07$
Alle anderen Instanzbewertungen	0,04$

Preise für Regelpakete zur Host-Assessment

Für jede Kombination aus Common Vulnerabilities and Exposures (CVE), Benchmarks des Center for Internet Security (CIS), bewährten Sicherheitsmethoden und Runtime Behavior Analysis, die in den Bewertungen enthalten sind

Die Regelpakete für die Hostbewertung von Amazon Inspector Classic verwenden einen Agenten, der auf den EC2 Amazon-Instances bereitgestellt wird, auf denen die Anwendungen ausgeführt werden, die Sie bewerten möchten. Bewertungen mit den Host-Regelpaketen werden pro Agent und Bewertung (Agentenbeurteilung) pro Monat berechnet. Wenn Sie beispielsweise eine Bewertung für einen Agenten durchführen, ist das eine Bewertung durch einen Agenten. Wenn Sie 1 Bewertung für 10 Agenten durchführen, sind das 10 Agentenbewertungen. Die Preise beginnen bei 0,30$ pro Agentenbewertung und Monat, wobei Mengenrabatte bis zu 0,05$ pro Agentenbewertung pro Monat betragen können.

Einzelheiten zur kostenlosen Testversion

Die ersten 90 Tage mit Amazon Inspector Classic	Preis pro Assessment durch einen Agenten
Die ersten 250 Assessments durch Agenten	0,00$

Preisdetails

In einem bestimmten Monat	Preis pro Sachverständigenbewertung
Die ersten 250 Assessments durch Agenten	0,30$
Die nächsten 750 Agentenbeurteilungen	0,25$
Die nächsten 4.000 Agentenbewertungen	0,15$
Die nächsten 45.000 Agentenbeurteilungen	$0.10
Alle anderen Agentenbeurteilungen	$0.05

Von Amazon Inspector Classic unterstützte Betriebssysteme und Regionen

Dieses Kapitel enthält Informationen zu den Betriebssystemen und AWS-Regionen, die Amazon Inspector Classic unterstützt.

> **Important**
>
> Derzeit können Amazon Inspector Classic-Bewertungsziele nur aus EC2 Instances bestehen. Sie können eine agentenlose Bewertung mit dem Regelpaket für Network Reachability auf allen EC2 Instances unabhängig vom Betriebssystem durchführen.

Informationen zu den Amazon Inspector Classic-Regelpaketen, die für alle unterstützten Betriebssysteme verfügbar sind, finden Sie unterAmazon Inspector Classic-Regelpakete für unterstützte Betriebssysteme.

Themen

Unterstützte Linux-basierte Betriebssysteme für den Amazon Inspector Classic-Agenten

Sie können den Amazon Inspector Classic-Agent auf 64-Bit-x86- und EC2 Arm-Instances verwenden. Der Agent ist mit den folgenden Versionen von Linux-basierten Betriebssystemen kompatibel:

- 64-Bit-x86-Instanzen
  - Amazon Linux 2
  - Amazon Linux (2018.03, 2017.09, 2017.03, 2016.09, 2016.03, 2015.09, 2015.03, 2014.09, 2014.03, 2013.09, 2013.03, 2012.09, 2012.03)
  - Ubuntu (20.04 LTS, 18.04 LTS, 16.04 LTS, 14,04 LTS)
  - Debian (10.x, 9,0—9,5, 8,0—8,7)

  - RedHat Enterprise Linux (8.x, 7.2, 6.2 — 6.9)
  - CentOS (7,2-7.x, 6,2-6,9)
- ARM-Instanzen
  - Amazon Linux 2
  - RedHat Enterprise Linux (7.6 — 7.x)
  - Ubuntu (18,04 LTS, 16,04 LTS)

Unterstützte Windows-basierte Betriebssysteme für den Amazon Inspector Classic-Agenten

Sie können den Amazon Inspector Classic-Agent nur auf EC2 Instances verwenden, auf denen die 64-Bit-Version der folgenden Windows-basierten Betriebssysteme ausgeführt wird:

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

Unterstützte AWS Regionen

Amazon Inspector Classic wird in den folgenden AWS-Regionen unterstützt:

- USA Ost (Ohio) – us-east-2
- USA Ost (Nord-Virginia) us-east-1
- USA West (Nordkalifornien) us-west-1
- USA West (Oregon) us-west-2
- Asien-Pazifik (Mumbai) – ap-south-1
- Asien-Pazifik (Seoul) – ap-northeast-2
- Asien-Pazifik (Sydney) ap-southeast-2
- Asien-Pazifik (Tokio) ap-northeast-1
- Europa (Frankfurt) eu-central-1

- Europa (Irland) (eu-west-1)
- Europa (London) eu-west-2
- Europa (Stockholm) eu-north-1
- AWS GovCloud (US-Ost) -1 gov-us-east
- AWS GovCloud (US-West) -1 gov-us-west

> **Note**
>
> Das Regelpaket zur Netzwerkerreichbarkeit ist in den Regionen AWS GovCloud (USA) nicht verfügbar.

Ende der Unterstützung für Amazon Inspector Classic

Nach reiflicher Überlegung haben wir beschlossen, den Support für Amazon Inspector Classic mit Wirkung zum 20. Mai 2026 einzustellen. Amazon Inspector Classic akzeptiert ab dem 20. Mai 2025 keine Neukunden mehr. Als Bestandskunde mit einem Konto, das vor dem 20. Mai 2025 für den Service registriert wurde, können Sie die Funktionen von Amazon Inspector Classic weiterhin nutzen. Nach dem 20. Mai 2026 können Sie Amazon Inspector Classic nicht mehr verwenden.

Der neue Amazon Inspector ist jetzt weltweit verfügbar in AWS-Regionen. Der neue Amazon Inspector ist eine komplett überarbeitete und neu gestaltete Version des bestehenden Amazon Inspector, der jetzt Amazon Inspector Classic heißt. Die folgenden Funktionen sind die wichtigsten Verbesserungen von Amazon Inspector:

- Maßgeschneidert — Der neue Amazon Inspector ist für Skalierung und dynamische Cloud-Umgebungen konzipiert. Es gibt keine Beschränkungen in Bezug auf die Anzahl der -Instances oder -Bilder, die in einem Konto gescannt werden können.
- Support für Container-Images — Der neue Amazon Inspector scannt auch Container-Images, die sich in Amazon Elastic Container Registry (Amazon ECR) befinden, auf Software-Schwachstellen.
- Support für die Verwaltung mehrerer Konten — Der neue Amazon Inspector ist in Organizations integriert. Auf diese Weise können Sie ein Administratorkonto für Amazon Inspector von Ihrer Organisation delegieren. Das delegierte Administratorkonto ist ein zentralisiertes Konto, das alle Ergebnisse konsolidiert und alle Mitgliedskonten konfigurieren kann.
- Verwendet AWS Systems Manager Agent (SSM Agent) — Mit dem neuen Amazon Inspector müssen Sie nicht mehr auf all Ihren EC2 Instances einen eigenständigen Amazon Inspector-Agenten installieren und verwalten. Der neue Amazon Inspector nutzt den weit verbreiteten SSM-Agenten.
- Automatisiertes und kontinuierliches Scannen — Mit Amazon Inspector Classic richten Sie manuell Bewertungsziele und Bewertungsvorlagen ein und konfigurieren die Häufigkeit der Bewertungen. Die neue Version von Amazon Inspector erkennt jedoch automatisch alle neu gestarteten EC2 Instances und infrage kommenden Container-Images, die an Amazon ECR übertragen wurden, und untersucht diese sofort auf Software-Schwachstellen und unbeabsichtigte Netzwerkoffenlegung. Die Ressourcen werden auf der Grundlage mehrerer Auslöser automatisch erneut gescannt, z. B. wenn eine neue EC2 Instance gestartet wird, ein Container-Image an Amazon ECR gesendet wird, ein neues Paket in einer EC2 Instance installiert, ein Patch installiert oder ein neues Common Vulnerabilities and Exposure (CVE) veröffentlicht wird, das sich auf die Ressource auswirkt.

- Amazon Inspector-Risikobewertung — Der neue Amazon Inspector berechnet eine Amazon Inspector-Risikobewertung, um Ihnen bei der Priorisierung Ihrer Ergebnisse zu helfen. Die Risikobewertung wird berechnet, indem up-to-date CVE-Informationen mit zeitlichen und umweltbedingten Faktoren wie Netzwerkzugänglichkeit und Ausnutzbarkeit korreliert werden.
- Mehr Integrationen — Alle Ergebnisse werden in einer neu gestalteten Amazon Inspector Inspector-Konsole zusammengefasst und an AWS Security Hub Amazon übertragen, EventBridge um Workflows wie das Ticketing zu automatisieren. Ergebnisse im Zusammenhang mit Container-Images werden ebenfalls an Amazon ECR übertragen.

Informationen zu allen Funktionen und Preisen des neuen Amazon Inspector finden Sie im Amazon Inspector Inspector-Benutzerhandbuch.

Wir werden Amazon Inspector Classic zwar noch einige Zeit unterstützen und Kunden können sowohl den neuen Amazon Inspector als auch Amazon Inspector Classic in demselben Konto verwenden, wir empfehlen Ihnen jedoch dringend, auf den neuen Amazon Inspector umzusteigen. Die folgenden Abschnitte führen Sie durch den Umstieg von Amazon Inspector Classic auf den neuen Amazon Inspector.

Themen

Schritt 1: (Optional) Exportieren Sie Bewertungsberichte und Ergebnisse

Um die Bewertungsberichte und Ergebnisse in Amazon Inspector Classic zu speichern, generieren Sie einen Bewertungsbericht.

Erstellen Sie einen Bewertungsbericht wie folgt:

1. Suchen Sie auf der Seite Assessment runs (Bewertungsläufe) den Bewertungslauf, für den Sie für einen Bericht erstellen möchten. Stellen Sie sicher, dass der Status laute Analyse abgeschlossen.
2. Wählen Sie in der Spalte Berichte dieses Bewertungslaufs das Berichtsymbol aus.

> **Important**
>
> Das Berichtsymbol wird in der Spalte Reports (Berichte) nur für Bewertungsläufe angezeigt, die nach dem 25. April 2017 erstellt wurden. Zu diesem Zeitpunkt wurden Bewertungsberichte in Amazon Inspector Classic verfügbar.

3. Wählen Sie im Dialogfeld Bewertungsbericht den Berichtstyp aus, den Sie anzeigen möchten (entweder einen Ergebnisbericht oder einen vollständigen Bericht) und das Berichtsformat (HTML oder PDF). Wählen Sie dann Bericht erstellen.

Schritt 2: Löschen Sie alle geplanten Bewertungsläufe in Amazon Inspector Classic

Um Amazon Inspector Classic zu deaktivieren, löschen Sie alle Bewertungsvorlagen in Ihrem Konto, sofern sie aktiv sind AWS-Regionen. Durch das Löschen von Bewertungsvorlagen werden all Ihre geplanten future Bewertungsläufe gestoppt.

So löschen Sie eine Bewertungsvorlage

- Wählen Sie auf der Seite Assessment Templates (Bewertungsvorlagen) die zu löschende Vorlage aus und wählen Sie dann Delete (Löschen). Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja aus.

> **Important**
>
> Wenn Sie eine Bewertungsvorlage löschen, werden alle Bewertungsläufe, Ergebnisse und Versionen der dieser Vorlage zugeordneten Berichte ebenfalls gelöscht.

Schritt 3: Aktivieren des neuen Amazon Inspector

Sie können den neuen Amazon Inspector mit dem AWS Management Console oder dem neuen Amazon Inspector aktivieren APIs. Informationen zu den ersten Schritten mit dem neuen Amazon Inspector finden Sie unter Erste Schritte im Amazon Inspector Inspector-Benutzerhandbuch.

Erste Schritte mit Amazon Inspector Classic

Dieses Tutorial zeigt Ihnen, wie Sie Amazon Inspector Classic einrichten und mit der Erstellung und Ausführung Ihres ersten Assessments beginnen.

One-Click-Setup

Das folgende Verfahren zeigt Ihnen, wie Sie eine automatische Bewertung mithilfe einer vorgefertigten Vorlage und vordefinierter Planungsparameter (einmal pro Woche oder nur einmal) für alle verfügbaren Amazon Elastic Compute Cloud (Amazon EC2) -Instances in der aktuellen AWS-Konto Version und ausführen. AWS-Region

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.
2. Wählen Sie auf der Seite Willkommen den Bewertungstyp aus, den Sie ausführen möchten. Netzwerkbewertungen analysieren die Netzwerkkonfigurationen Ihrer AWS Umgebung auf Schwachstellen und erfordern keinen Amazon Inspector Classic-Agent. Host Assessments analysieren die On-Host-Software und die Konfigurationen Ihrer EC2 Instances auf Sicherheitslücken und setzen voraus, dass auf den EC2 Instances ein Agent installiert ist.

   Wählen Sie entweder Run weekly (recommended) (Wöchentlich ausführen (empfohlen)) oder Run once (Einmal ausführen) aus. Sobald Sie Ihre Auswahl getroffen haben, erstellt der Service automatisch die Bewertung. In diesem Beispiel führt der Service folgende Schritte aus:

   a. Erstellt eine serviceverknüpfte Rolle.

      > **Note**
      >
      > Um die EC2 Instances zu identifizieren, die in den Bewertungszielen angegeben sind, muss Amazon Inspector Classic Ihre EC2 Instances und Tags auflisten. Amazon Inspector Classic erhält Zugriff auf diese Ressourcen in Ihrem AWS-Konto über eine serviceverknüpfte Rolle namens`AWSServiceRoleForAmazonInspector`. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Inspector Classic und Verwenden von serviceverknüpften Rollen.

b. Falls zutreffend, installiert einen Amazon Inspector Classic-Agenten auf allen verfügbaren EC2 Instances in Ihrer Region AWS-Konto und in Ihrer Region.

> **Note**
>
> Der Service installiert einen Amazon Inspector Classic-Agenten nur auf den EC2 Instances, die AWS Systems Manager Run Command zulassen. Um diese Option zu verwenden, stellen Sie sicher, dass alle Ihre EC2 Instances in der aktuellen Version AWS-Region sind AWS-Konto und dass der SSM-Agent installiert ist und dass sie über eine IAM-Rolle verfügen, die Run Command ermöglicht. Weitere Informationen finden Sie unter Installation des Agenten auf mehreren EC2 Instanzen mithilfe des Systems Manager Manager-Befehls Run.

c. Fügt diese Instances zu einem Bewertungsziel hinzu.

d. Fügt dieses Ziel mit einem standardisierten Satz Regelpaketen in eine Bewertungsvorlage ein.

e. Führt die Bewertung wöchentlich oder einmalig aus, je nachdem, ob Sie Run weekly (recommended) oder Run once ausgewählt haben.

3. Wählen Sie im Bestätigungsdialogfeld OK aus. Amazon Inspector Classic führt Ihre Bewertung automatisch durch.

Erweiterte Einstellungen

Das folgende Verfahren zeigt Ihnen, wie Sie bestimmte EC2 Amazon-Instances, Regelpakete und Planungsparameter auswählen, die in ein Bewertungsziel und eine Vorlage aufgenommen werden sollen.

1. Wählen Sie auf der Seite Welcome Advanced setup aus.
2. Geben Sie auf der Seite Define an assessment target (Definieren eines Bewertungsziels) den Namen Ihres Bewertungsziels ein.
3. Für Alle Instances können Sie das Kontrollkästchen aktiviert lassen, um alle EC2 Instances in Ihrer Region AWS-Konto und Ihrer Region in das Bewertungsziel einzubeziehen. Wenn Sie auswählen möchten, welche EC2 Instances eingeschlossen werden sollen, deaktivieren Sie das Kontrollkästchen Alle Instances und geben Sie die Key - und Value-Tags ein, die den EC2 Ziel-Instances zugeordnet sind. Weitere Informationen zum Taggen Ihrer EC2 Instances finden Sie unter Tagging Your Amazon EC2 Resources.

4. Für Install Agents können Sie das Kontrollkästchen standardmäßig aktiviert lassen, wenn Ihre Instances System Manager Run Command zulassen. Der Service installiert einen Amazon Inspector Classic-Agenten auf allen EC2 Instances im Bewertungsziel, die dies zulassen AWS Systems Manager. Um diese Option zu verwenden, stellen Sie sicher, dass alle Ihre EC2 Instances in der aktuellen Version AWS-Region sind AWS-Konto und dass der SSM-Agent installiert ist und dass sie über eine IAM-Rolle verfügen, die Run Command ermöglicht. Weitere Informationen finden Sie unter Installation des Agenten auf mehreren EC2 Instanzen mithilfe des Systems Manager Manager-Befehls Run. Wenn Sie den Agenten manuell installieren möchten, finden Sie weitere Informationen unter Installieren von Amazon Inspector-Agents.
5. Wählen Sie Weiter.
6. Geben Sie auf der Seite Define an assessment template (Definieren einer Bewertungsvorlage) den Namen Ihrer Bewertungsvorlage ein.
7. Wählen Sie für Rules packages die Regelpakete aus, das in die Bewertungsvorlage aufgenommen werden sollen. Weitere Informationen über Regelpakete finden Sie unter Amazon Inspector-Regelpakete und -Regeln.
8. Wählen Sie für Duration die Dauer des Bewertungslaufs aus.
9. (Optional) Legen Sie für den Bewertungszeitplan einen Zeitplan für wiederkehrende Bewertungsläufe fest.
10. Wählen Sie Weiter.
11. Überprüfen Sie auf der Seite Review Ihre Auswahl für das Bewertungsziel und die Bewertungsvorlage. Wenn Sie mit der Konfiguration zufrieden sind, wählen Sie Create aus. Wenn Sie für Ihre Bewertungsvorlage einen Bewertungsplan erstellen, wird die Bewertung nach der Wahl von Create (Erstellen) automatisch ausgeführt.

> **Note**
>
> Um die EC2 Instances zu identifizieren, die in den Bewertungszielen angegeben sind, muss Amazon Inspector Classic Ihre EC2 Instances und Tags auflisten. Amazon Inspector Classic erhält Zugriff auf diese Ressourcen in Ihrem AWS-Konto über eine serviceverknüpfte Rolle namens`AWSServiceRoleForAmazonInspector`. Weitere Informationen zur Verwendung von serviceverknüpften Rollen in Amazon Inspector Classic finden Sie unterVerwenden von serviceverknüpften Rollen für Amazon Inspector Classic. Ausführliche Informationen zur Verwendung von serviceverknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen im AWS Identity and Access Management Benutzerhandbuch.

12. Wenn Sie keinen Bewertungsplan eingerichtet haben, navigieren Sie über die Konsole zu Ihrer Bewertungsvorlage und wählen Sie Run (Ausführen) aus.
13. Um den Fortschritt des Bewertungslaufs zu überwachen, wählen Sie im Navigationsbereich der Konsole Assessment runs aus und klicken Sie auf Findings. Weitere Informationen zu Ergebnissen finden Sie unter Ergebnisse von Amazon Inspector Classic.

Anleitungen für Amazon Inspector Classic

Die folgenden Tutorials zeigen Ihnen, wie Sie Amazon Inspector Classic Assessment-Läufe auf den Betriebssystemen Red Hat Enterprise Linux und Ubuntu durchführen.

Tutorials

- Tutorial: Amazon Inspector Classic mit Red Hat Enterprise Linux verwenden
- Tutorial: Amazon Inspector Classic mit Ubuntu Server verwenden

Anleitung zu Amazon Inspector Classic — Red Hat Enterprise Linux

Bevor Sie die Anweisungen in diesem Tutorial folgen, empfehlen wir, sich mit Terminologie und Konzepte von Amazon Inspector Classicvertraut zu machen.

Dieses Tutorial zeigt, wie Sie Amazon Inspector Classic verwenden, um das Verhalten einer EC2 Instance zu analysieren, auf der das Betriebssystem Red Hat Enterprise Linux 7.5 ausgeführt wird. Es enthält step-by-step Anweisungen zur Navigation im Amazon Inspector Classic-Workflow. Der Arbeitsablauf umfasst die Vorbereitung von EC2 Amazon-Instances, die Ausführung einer Bewertungsvorlage und die Durchführung der empfohlenen Sicherheitskorrekturen, die in den Ergebnissen der Bewertung generiert wurden. Wenn Sie zum ersten Mal ein Amazon Inspector Classic-Assessment einrichten und ausführen möchten, finden Sie weitere Informationen unter Basic Assessment erstellen.

Themen

- Schritt 1: Richten Sie eine EC2 Amazon-Instance für die Verwendung mit Amazon Inspector Classic ein
- Schritt 2: Ändern Sie Ihre EC2 Amazon-Instance
- Schritt 3: Erstellen Sie ein Bewertungsziel und installieren Sie einen Agenten auf der EC2 Instance
- Schritt 4: Erstellen und Ausführen der Bewertungsvorlage
- Schritt 5: Suchen und Analysieren der Ergebnisse
- Schritt 6: Anwenden der empfohlenen Lösung auf das Bewertungsziel

Schritt 1: Richten Sie eine EC2 Amazon-Instance für die Verwendung mit Amazon Inspector Classic ein

Erstellen Sie für dieses Tutorial eine EC2 Instance, auf der Red Hat Enterprise Linux 7.5 ausgeführt wird, und kennzeichnen Sie sie mit dem Name-Schlüssel und dem Wert von**`InspectorEC2InstanceLinux`**.

> **Note**
>
> Weitere Informationen über das Taggen von EC2 Instanzen finden Sie unter Ressourcen und Tags.

Schritt 2: Ändern Sie Ihre EC2 Amazon-Instance

In diesem Tutorial ändern Sie Ihre EC2 Ziel-Instance, um sie dem potenziellen Sicherheitsproblem CVE-2018-1111 auszusetzen. Weitere Informationen finden Sie unter https://cve.mitre. org/cgi-bin/cvename.cgi? name=CVE-2018-1111 und. Häufige Schwachstellen und Expositionen

Stellen Sie eine Verbindung zu Ihrer Instance **`InspectorEC2InstanceLinux`** her und führen Sie den folgenden Befehl aus:

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

Anweisungen zum Herstellen einer Verbindung mit einer EC2 Instance finden Sie unter Connect to Your Instance im EC2 Amazon-Benutzerhandbuch.

Schritt 3: Erstellen Sie ein Bewertungsziel und installieren Sie einen Agenten auf der EC2 Instance

Amazon Inspector Classic verwendet Bewertungsziele, um die AWS-Ressourcen zu bestimmen, die Sie bewerten möchten.

Um ein Bewertungsziel zu erstellen und einen Agenten auf einer EC2 Instance zu installieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.
2. Wählen Sie im Navigationsbereich Assessment targets (Bewertungsziele) und danach Create (Erstellen) aus.

Gehen Sie wie folgt vor:

a. Geben Sie unter Name den Namen für Ihr Bewertungsziel ein.

   Geben Sie für dieses Tutorial **`MyTargetLinux`** ein.

b. Wählen Sie unter Use Tags die EC2 Instances aus, die Sie in dieses Bewertungsziel einbeziehen möchten, indem Sie Werte in die Felder Schlüssel und Wert eingeben.

   Wählen Sie für dieses Tutorial die EC2 Instanz aus, die Sie im vorherigen Schritt erstellt haben, indem Sie sie **`Name`** in die Felder Schlüssel und **`InspectorEC2InstanceLinux`** Wert eingeben.

   Um alle EC2 Instances in Ihrem AWS-Konto und Ihrer Region in das Bewertungsziel aufzunehmen, aktivieren Sie das Kontrollkästchen Alle Instances.

c. Wählen Sie Save (Speichern) aus.

d. Installieren Sie einen Amazon Inspector Classic-Agenten auf Ihrer markierten EC2 Instance. Um einen Agenten auf allen EC2 Instances zu installieren, die in einem Bewertungsziel enthalten sind, aktivieren Sie das Kontrollkästchen Agenten installieren.

   > **Note**
   >
   > Sie können den Amazon Inspector Classic-Agent auch mit dem AWS Systems Manager Run Command installieren. Um den Agenten auf allen Instances im Bewertungsziel zu installieren, können Sie dieselben Tags angeben, die für die Erstellung des Bewertungsziels verwendet wurden. Oder Sie können den Amazon Inspector Classic-Agent manuell auf Ihrer EC2 Instance installieren. Weitere Informationen finden Sie unter Amazon Inspector Classic-Agenten installieren.

e. Wählen Sie Save (Speichern) aus.

> **Note**
>
> Zu diesem Zeitpunkt erstellt Amazon Inspector Classic eine serviceverknüpfte Rolle mit dem Namen`AWSServiceRoleForAmazonInspector`. Die Rolle gewährt Amazon Inspector Classic den erforderlichen Zugriff auf Ihre Ressourcen. Weitere Informationen finden Sie unter Eine serviceverknüpfte Rolle für Amazon Inspector Classic erstellen.

Schritt 4: Erstellen und Ausführen der Bewertungsvorlage

So erstellen Sie Ihre Vorlage und führen Sie aus

1. Wählen Sie im Navigationsbereich die Option Assessment Templates (Bewertungsvorlagen) und danach Create (Erstellen).
2. Geben Sie unter Name den Namen für Ihre Bewertungsvorlage ein. Geben Sie für dieses Tutorial **`MyFirstTemplateLinux`** ein.
3. Wählen Sie für Target name das Bewertungsziel aus, das Sie oben erstellt haben: **`MyTargetLinux`**.
4. Wählen Sie für Rules packages die Regelpakete aus, die in dieser Bewertungsvorlage verwendet werden sollen.

   Wählen Sie für dieses Tutorial Common Vulnerabilities and Exposures-1.1 aus.
5. Geben Sie unter Duration die Dauer für Ihre Bewertungsvorlage an.

   Wählen Sie für dieses Tutorial 15 Minuten aus.
6. Wählen Sie Create and run aus.

Schritt 5: Suchen und Analysieren der Ergebnisse

Ein abgeschlossener Bewertungslauf führt zu einer Reihe von Ergebnissen oder potenziellen Sicherheitsproblemen, die Amazon Inspector Classic in Ihrem Bewertungsziel entdeckt. Sie können die Ergebnisse überprüfen und die empfohlenen Schritte zur Behebung der potenziellen Sicherheitsprobleme befolgen.

Wenn Sie die vorherigen Schritte durchgeführt haben, erzeugt Ihr Bewertungslauf in diesem Tutorial ein Ergebnis für die gängige Schwachstelle CVE-2018-1111.

So suchen und analysieren Sie Ihre Ergebnisse

1. Wählen Sie im Navigationsbereich Bewertungsläufe aus. Vergewissern Sie sich, dass der Status des Laufs für die aufgerufene Bewertungsvorlage auf Daten sammeln gesetzt MyFirstTemplateLinuxist. Dies zeigt an, dass der Bewertungslauf derzeit läuft und die Telemetriedaten für Ihr Ziel gesammelt und gegen die ausgewählten Regelpakete analysiert werden.

2. Sie können die vom Bewertungslauf generierten Ergebnisse nicht anzeigen, während er noch läuft. Lassen Sie den Bewertungslauf vollständig ausführen. Für dieses Tutorial können Sie die Ausführung jedoch nach einigen Minuten stoppen.

   Der Status von MyFirstTemplateLinuxändert sich zunächst in Stopp, dann in ein paar Minuten in Analysieren und schließlich in Analyse abgeschlossen. Um diese Statusänderung zu sehen, können Sie das Symbol Refresh auswählen.

3. Wählen Sie im Navigationsbereich Findings aus.

   Sie können ein neues Ergebnis mit hohem Schweregrad namens Instance Inspector EC2 InstanceLinux ist anfällig für CVE-2018-1111 sehen.

   > **Note**
   >
   > Falls keine neuen Ergebnisse zu sehen sind, wählen Sie das Symbol Refresh aus.

   Um die Ansicht zu erweitern und die Details dieses Fundes zu sehen, wählen Sie den Pfeil links vom Fund aus. Die Details des Fundes schließen folgendes mit ein:

   - ARN des Ergebnisses
   - Name des Bewertungslaufs, der dieses Ergebnis generiert hat
   - Name des Bewertungsziels, das dieses Ergebnis generiert hat
   - Name der Bewertungsvorlage, die dieses Ergebnis generiert hat
   - Startzeit des Bewertungslaufs
   - Endzeitpunkt des Bewertungslaufs
   - Status des Bewertungslaufs
   - Name des Regelpakets, das die Regel enthält, die dieses Ergebnis ausgelöst hat
   - Amazon Inspector Classic-Agenten-ID
   - Name des Ergebnisses
   - Schweregrad des Ergebnisses
   - Beschreibung des Ergebnisses
   - Empfohlene Korrekturmaßnahmen, die Sie ergreifen können, um das potenzielle Sicherheitsproblem zu beheben, das durch das Ergebnis beschrieben wird

Schritt 6: Anwenden der empfohlenen Lösung auf das Bewertungsziel

Sie haben für dieses Tutorial Ihr Bewertungsziel geändert, um es dem potenziellen Sicherheitsproblem CVE-2018-1111 auszusetzen. Mit diesem Verfahren wenden Sie die empfohlene Lösung für das Problem an.

So wenden Sie die Lösung auf Ihr Ziel an

1. Stellen Sie eine Verbindung mit Ihrer Instance **`InspectorEC2InstanceLinux`** her, die Sie im vorherigen Abschnitt erstellt haben, und führen Sie den folgenden Befehl aus:

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

2. Wählen Sie auf der Seite Bewertungsvorlagen die Option und anschließend Ausführen aus MyFirstTemplateLinux, um einen neuen Bewertungslauf mit dieser Vorlage zu starten.
3. Folgen Sie den Anweisungen unterSchritt 5: Suchen und Analysieren der Ergebnisse, um die Ergebnisse zu sehen, die sich aus dieser nachfolgenden Ausführung der MyFirstTemplateLinuxVorlage ergeben.

   Da Sie das Sicherheitsproblem CVE-2018-1111 behoben haben, sollten Sie keine Ergebnisse mehr dafür finden.

Anleitung zu Amazon Inspector Classic — Ubuntu Server

Bevor Sie die Anweisungen in diesem Tutorial folgen, empfehlen wir, sich mit Terminologie und Konzepte von Amazon Inspector Classicvertraut zu machen.

Dieses Tutorial zeigt, wie Sie Amazon Inspector Classic verwenden, um das Verhalten einer EC2 Instance zu analysieren, auf der das Betriebssystem Ubuntu Server 16.04 LTS ausgeführt wird. Es enthält step-by-step Anweisungen zur Navigation im Amazon Inspector Classic-Workflow.

Wenn Sie zum ersten Mal ein Amazon Inspector Classic-Assessment einrichten und ausführen möchten, finden Sie weitere Informationen unter Basic Assessment erstellen.

Themen

- Schritt 1: Richten Sie eine EC2 Amazon-Instance für die Verwendung mit Amazon Inspector Classic ein
- Schritt 2: Erstellen Sie ein Bewertungsziel und installieren Sie einen Agenten auf der Instanz EC2

- Schritt 3: Erstellen Sie Ihre Bewertungsvorlage und führen Sie sie aus
- Schritt 4: Finden und analysieren Sie die generierten Ergebnisse
- Schritt 5: Wenden Sie die empfohlene Lösung auf Ihr Bewertungsziel an

Schritt 1: Richten Sie eine EC2 Amazon-Instance für die Verwendung mit Amazon Inspector Classic ein

Um eine EC2 Instance einzurichten

- Erstellen Sie für dieses Tutorial eine EC2 Instanz, auf der Ubuntu Server 16.04 LTS ausgeführt wird, und taggen Sie sie mit dem Name-Schlüssel und dem Wert. **`InspectorEC2InstanceUbuntu`**

> **Note**
>
> Weitere Informationen zum Markieren von EC2 Instanzen finden Sie unter Ressourcen und Tags.

Schritt 2: Erstellen Sie ein Bewertungsziel und installieren Sie einen Agenten auf der Instanz EC2

Amazon Inspector Classic verwendet Bewertungsziele, um die zu bewertenden AWS-Ressourcen festzulegen.

Um ein Bewertungsziel zu erstellen und einen Agenten auf der EC2 Instance zu installieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.
2. Wählen Sie im Navigationsbereich Assessment targets (Bewertungsziele) und danach Create (Erstellen) aus.
3. Geben Sie unter Name den Namen für Ihr Bewertungsziel ein.

   Geben Sie in diesem Tutorial **`MyTargetUbuntu`** ein.
4. Wählen Sie unter Use Tags die EC2 Instances aus, die Sie in dieses Bewertungsziel einbeziehen möchten, indem Sie Werte in die Felder Schlüssel und Wert eingeben.

Wählen Sie für dieses Tutorial die EC2 Instanz aus, die Sie im vorherigen Schritt erstellt haben, indem Sie sie **`Name`** in die Felder Schlüssel und **`InspectorEC2InstanceUbuntu`** Wert eingeben.

Um alle EC2 Instances in Ihrem AWS-Konto und Ihrer Region in das Bewertungsziel aufzunehmen, wählen Sie das Feld Alle Instances aus.

5. Installieren Sie einen Amazon Inspector Classic Agent auf Ihrer markierten EC2 Instance. Um einen Agenten auf allen EC2 Instances zu installieren, die in einem Bewertungsziel enthalten sind, wählen Sie das Feld Agenten installieren aus.

> **Note**
>
> Sie können den Amazon Inspector-Agent auch mit dem Systems Manager Run Command installieren. Um den Agenten auf allen Instances im Bewertungsziel zu installieren, können Sie dieselben Tags angeben, die für die Erstellung des Bewertungsziels verwendet wurden. Oder Sie können den Amazon Inspector Agent manuell auf Ihrer EC2 Instance installieren. Weitere Informationen finden Sie unter Amazon Inspector Classic-Agenten installieren.

6. Wählen Sie Save (Speichern) aus.

> **Note**
>
> Zu diesem Zeitpunkt `AWSServiceRoleForAmazonInspector` wird eine servicebezogene Rolle namens erstellt, um Amazon Inspector Classic Zugriff auf Ihre Ressourcen zu gewähren. Weitere Informationen finden Sie unter Eine serviceverknüpfte Rolle für Amazon Inspector Classic erstellen.

Schritt 3: Erstellen Sie Ihre Bewertungsvorlage und führen Sie sie aus

So erstellen Sie Ihre Vorlage und führen Sie aus

1. Wenn Sie Advanced setup (Erweiterte Einstellungen) verwenden, werden Sie zu der Seite Define an assessment template (Bewertungsvorlage definieren)weitergeleitet. Navigieren Sie andernfalls zur Seite Assessment templates (Bewertungsvorlagen), und wählen Sie dann Create (Erstellen) aus.

2. Geben Sie unter Name den Namen für Ihre Bewertungsvorlage ein. Geben Sie für dieses Tutorial **`MyFirstTemplateUbuntu`** ein.
3. Wählen Sie für Target name das Bewertungsziel aus, das Sie oben erstellt haben: **`MyTargetUbuntu`**.
4. Wählen Sie für Rules packages (Regelpakete) im Dropdown-Menü die Regelpakete aus, die Sie für diese Bewertungsvorlage verwenden möchten.

   Wählen Sie für dieses Tutorial Common Vulnerabilities and Exposures-1.1 aus.
5. Geben Sie unter Duration die Dauer für Ihre Bewertungsvorlage an.

   Wählen Sie für dieses Tutorial 15 minutes (15 Minuten) aus.
6. Wenn Sie Advanced setup verwenden, wählen Sie Next aus. Klicken Sie auf der Seite Review auf Create. Wählen Sie andernfalls Create and run (Erstellen und Ausführen) aus.

Schritt 4: Finden und analysieren Sie die generierten Ergebnisse

Ein abgeschlossener Bewertungslauf führt zu einer Reihe von Ergebnissen oder potenziellen Sicherheitsproblemen, die Amazon Inspector Classic in Ihrem Bewertungsziel entdeckt. Sie können die Ergebnisse überprüfen und die empfohlenen Schritte zur Behebung der potenziellen Sicherheitsprobleme befolgen.

1. Navigieren Sie zur Seite Assessment Runs (Bewertungsläufe). Vergewissern Sie sich, dass der Status des Laufs für die Bewertungsvorlage mit dem Namen MyFirstTemplateUbuntu, die Sie im vorherigen Schritt erstellt haben, auf Daten sammeln gesetzt ist. Dies zeigt an, dass der Bewertungslauf derzeit läuft und die Telemetriedaten für Ihr Ziel gesammelt und gegen die ausgewählten Regelpakete analysiert werden.
2. Sie können die vom Bewertungslauf generierten Ergebnisse nicht anzeigen, während er noch läuft. Lassen Sie den Bewertungslauf vollständig ausführen.

   Der Status von MyFirstTemplateUbuntuändert sich zunächst in Stopp, dann in ein paar Minuten in Analysieren und schließlich in Analyse abgeschlossen. Um diese Statusänderung zu sehen, können Sie das Symbol Refresh auswählen.
3. Navigieren Sie zur Seite Findings (Ergebnisse).

   Um die Ansicht zu erweitern und die Details eines Ergebnisses anzuzeigen, klicken Sie auf den Pfeil links neben dem Ergebnis. Die Details des Fundes schließen folgendes mit ein:

- ARN des Ergebnisses
- Name des Bewertungslaufs, der dieses Ergebnis generiert hat
- Name des Bewertungsziels, das dieses Ergebnis generiert hat
- Name der Bewertungsvorlage, die dieses Ergebnis generiert hat
- Startzeit des Bewertungslaufs
- Endzeitpunkt des Bewertungslaufs
- Status des Bewertungslaufs
- Name des Regelpakets, das die Regel enthält, die den Befund ausgelöst hat
- Amazon Inspector Classic-Agenten-ID
- Name des Ergebnisses
- Schweregrad des Ergebnisses
- Beschreibung des Ergebnisses
- Empfohlene Korrekturmaßnahmen, die Sie ergreifen können, um das potenzielle Sicherheitsproblem zu beheben, das durch das Ergebnis beschrieben wird

Schritt 5: Wenden Sie die empfohlene Lösung auf Ihr Bewertungsziel an

Bei diesem Verfahren wenden Sie ein Update an, um die aufgedeckten Probleme zu beheben.

1. Connect zu Ihrer Instance **`InspectorEC2InstanceUbuntu`** her und führen Sie ein Paket-Update durch.
2. Wählen Sie auf der Seite Bewertungsvorlagen die Option und anschließend Ausführen aus MyFirstTemplateUbuntu, um einen neuen Lauf mit dieser Vorlage zu starten.
3. Folgen Sie den Schritten unterSchritt 4: Finden und analysieren Sie die generierten Ergebnisse, um die Ergebnisse zu sehen, die sich aus dieser nachfolgenden Ausführung der MyFirstTemplateUbuntuVorlage ergeben.

   Das Paket-Update sollte die Ergebnisse aus der ersten Ausführung der Vorlage behoben haben.

Sicherheit in Amazon Inspector Classic

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon Inspector Classic gelten, finden Sie unter AWS-Services in Umfang nach Compliance-Programm .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon Inspector Classic anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon Inspector Classic konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS-Services nutzen können, die Ihnen helfen, Ihre Amazon Inspector Classic-Ressourcen zu überwachen und zu sichern.

Themen

Datenschutz in Amazon Inspector Classic

Das AWS Modell der gilt für den Datenschutz in Amazon Inspector Classic. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 Classic oder anderen AWS-Services über die Konsole AWS CLI, API oder arbeiten AWS SDKs. 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 gespeicherter Daten

Die Telemetriedaten, die ein Amazon Inspector Classic-Agent bei Bewertungsläufen generiert, sind in JSON-Dateien formatiert. Diese Dateien werden near-real-time über TLS an Amazon Inspector Classic übermittelt, wo sie mit einem kurzlebigen per-assessment-run, AWS KMS abgeleiteten Schlüssel verschlüsselt werden.

Die Dateien werden sicher in S3-Buckets gespeichert, die Amazon Inspector Classic gewidmet sind. Die Regel-Engine von Amazon Inspector Classic macht Folgendes:

- Zugriff auf die verschlüsselten Telemetriedaten im S3-Bucket
- Entschlüsseln der Telemetriedaten im Speicher
- Verarbeiten der Daten unter Anwendung der konfigurierten Bewertungsregeln, um Ergebnisse zu generieren

Verschlüsseln von Daten während der Übertragung.

Als verwalteter Service ist Amazon Inspector Classic durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon Inspector Classic 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.

Identity and Access Management für Amazon Inspector Classic

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon Inspector Inspector-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Amazon Inspector ausführen.

Servicebenutzer — Wenn Sie den Amazon Inspector-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Funktionen von Amazon Inspector verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in Amazon Inspector nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Amazon Inspector Classic: Identität und Zugriff.

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon Inspector-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon Inspector. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon Inspector Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Amazon Inspector verwenden kann, finden Sie unterSo funktioniert Amazon Inspector Classic mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon Inspector zu verwalten. Beispiele für identitätsbasierte Amazon Inspector Inspector-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector Classic

Authentifizierung mit Identitäten

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

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen

Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem

beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management

Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) 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 Methoden für die Übernahme einer Rolle 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 (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen

mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein

bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen

zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon Inspector Classic mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon Inspector zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Amazon Inspector verwendet werden können.

IAM-Funktionen, die Sie mit Amazon Inspector Classic verwenden können

IAM-Feature	Unterstützung für Amazon Inspector
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein

IAM-Feature	Unterstützung für Amazon Inspector
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Amazon Inspector und andere AWS Services mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Services, die mit IAM funktionieren.

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet

ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Amazon Inspector

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector Classic

Ressourcenbasierte Richtlinien in Amazon Inspector

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für Amazon Inspector

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Amazon Inspector-Aktionen finden Sie unter Von Amazon Inspector Classic definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in Amazon Inspector verwenden das folgende Präfix vor der Aktion:

```
inspector
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer Berechtigungen, um alle Operationen auszuführen, die mit `Describe` und `List` beginnen. Bei diesen Vorgängen werden Informationen über eine Amazon Inspector Inspector-Ressource angezeigt, z. B. ein Bewertungsziel oder ein Ergebnis. Das Platzhalterzeichen (*) in dem `Resource` Element gibt an, dass die Operationen für alle Amazon Inspector Inspector-Ressourcen zulässig sind, die dem Konto gehören:

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

```
            ],
         "Resource":"*"
      }
   ]
}
```

Beispiel 2: Erlauben Sie einem Benutzer, Beschreib- und Auflistungsvorgänge nur für Ergebnisse von Amazon Inspector durchzuführen

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer nur Berechtigungen zum Ausführen der Operationen `ListFindings` und `DescribeFindings`. Bei diesen Vorgängen werden Informationen zu den Ergebnissen von Amazon Inspector angezeigt. Das Platzhalterzeichen (*) in dem `Resource` Element gibt an, dass die Operationen für alle Amazon Inspector Inspector-Ressourcen zulässig sind, die dem Konto gehören.

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

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector Classic

Richtlinienressourcen für Amazon Inspector

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Eigenschaften finden Sie unter Von Amazon Inspector Classic definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon Inspector Classic definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector Classic

Schlüssel zu den Richtlinienbedingungen für Amazon Inspector

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Amazon Inspector-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon Inspector Classic in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Inspector Classic definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Amazon Inspector finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Inspector Classic

ACLs bei Amazon Inspector

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Amazon Inspector

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Temporäre Anmeldeinformationen mit Amazon Inspector verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

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

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Hauptberechtigungen für Amazon Inspector

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Amazon Inspector

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Amazon Inspector beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon Inspector Sie dazu anleitet.

Servicebezogene Rollen für Amazon Inspector

Unterstützt serviceverknüpfte Rollen: Ja

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

Einzelheiten zum Erstellen oder Verwalten von serviceverknüpften Amazon Inspector-Rollen finden Sie unterVerwenden von serviceverknüpften Rollen für Amazon Inspector Classic.

Beispiele für identitätsbasierte Richtlinien für Amazon Inspector Classic

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon Inspector Inspector-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon Inspector definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Inspector Classic in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

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

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden

Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Amazon Inspector Inspector-Konsole

Um auf die Amazon Inspector Classic-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon Inspector Inspector-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Amazon Inspector-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch den Amazon Inspector *ConsoleAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Erlauben Sie einem Benutzer, Beschreib- und Auflistungsvorgänge nur für Ergebnisse von Amazon Inspector durchzuführen

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer nur Berechtigungen zum Ausführen der Operationen `ListFindings` und `DescribeFindings`. Bei diesen Vorgängen werden Informationen zu den Ergebnissen von Amazon Inspector angezeigt. Das Platzhalterzeichen (*) in dem `Resource` Element gibt an, dass die Operationen für alle Amazon Inspector Inspector-Ressourcen zulässig sind, die dem Konto gehören.

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

Verwenden von serviceverknüpften Rollen für Amazon Inspector Classic

Amazon Inspector Classic verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon Inspector Classic verknüpft ist. Servicebezogene Rollen sind von Amazon Inspector Classic vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere in AWS-Services Ihrem Namen anzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon Inspector Classic, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon Inspector Classic definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur Amazon Inspector Classic seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch werden Ihre Amazon Inspector Classic-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Diensten, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS Services That Work with IAM. Suchen Sie in der Spalte Service-verknüpfte Rollen nach den Services, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rollenberechtigungen für Amazon Inspector Classic

Amazon Inspector Classic verwendet die serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForAmazonInspector— ServiceLinkedRoleDescription.

Die AWSService RoleForAmazonInspector servicebezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `inspector.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AmazonInspectorServiceRolePolicy ermöglicht es Amazon Inspector Classic, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

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

Sie müssen Berechtigungen konfigurieren, damit eine IAM-Entität (z. B. ein IAM-Benutzer, eine Gruppe oder eine Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Amazon Inspector Classic erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie CompleteThisCreateActionInThisService die AWS Management Console, oder die AWS API verwenden AWS CLI, erstellt Amazon Inspector Classic die serviceverknüpfte Rolle für Sie.

Bearbeiten einer serviceverknüpften Rolle für Amazon Inspector Classic

Amazon Inspector Classic erlaubt Ihnen nicht, die AWSService RoleForAmazonInspector serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. 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 Classic

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. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der Amazon Inspector Classic-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um Amazon Inspector Classic-Ressourcen zu löschen, die verwendet werden von **`AWSServiceRoleForAmazonInspector`**

- Löschen Sie Ihre Bewertungsziele dafür AWS-Konto in allen Bereichen, in AWS-Regionen denen Amazon Inspector Classic ausgeführt wird. Weitere Informationen finden Sie unter Bewertungsziele von Amazon Inspector Classic.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleForAmazonInspector serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Amazon Inspector Classic-Rollen

Amazon Inspector Classic unterstützt die Verwendung von servicebezogenen Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS -Regionen und -Endpunkte.

Fehlerbehebung bei Amazon Inspector Classic: Identität und Zugriff

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

Themen

- Ich bin nicht berechtigt, eine Aktion in Amazon Inspector durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon Inspector Inspector-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Amazon Inspector durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `inspector:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `inspector:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon Inspector übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon Inspector auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon Inspector Inspector-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon Inspector diese Funktionen unterstützt, finden Sie unterSo funktioniert Amazon Inspector Classic mit IAM.

- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Protokollierung und Überwachung in Amazon Inspector Classic

Amazon Inspector Classic ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Amazon Inspector Classic bereitstellt. CloudTrail erfasst alle API-Aufrufe für Amazon Inspector Classic als Ereignisse, einschließlich Aufrufe von der Amazon Inspector Classic-Konsole und Codeaufrufen an die Amazon Inspector Classic-API-Operationen.

Informationen zur Verwendung der CloudTrail Protokollierung in Amazon Inspector Classic finden Sie unterProtokollieren von Amazon Inspector Classic API-Aufrufen mit AWS CloudTrail.

Sie können Amazon Inspector Classic mithilfe von Amazon überwachen CloudWatch, das Rohdaten sammelt und zu lesbaren Metriken nahezu in Echtzeit verarbeitet. Standardmäßig sendet Amazon Inspector Classic Metrikdaten innerhalb von 5 Minuten CloudWatch an.

Informationen zur Verwendung CloudWatch mit Amazon Inspector Classic finden Sie unterÜberwachung von Amazon Inspector Classic mit Amazon CloudWatch.

Reaktion auf Vorfälle in Amazon Inspector Classic

Die Reaktion auf Vorfälle für Amazon Inspector Classic ist eine AWS Verantwortung. AWS verfügt über eine formelle, dokumentierte Richtlinie und ein Programm, die die Reaktion auf Vorfälle regeln.

AWS Betriebsprobleme mit weitreichenden Auswirkungen werden im AWS Service Health Dashboard veröffentlicht.

Operative Probleme werden über AWS Health Dashboard auch in den einzelnen Konten veröffentlicht. Informationen zur Verwendung von finden Sie im AWS Health Benutzerhandbuch. AWS Health Dashboard

Konformitätsprüfung für Amazon Inspector Classic

Externe Prüfer bewerten die Sicherheit und Konformität von Amazon Inspector Classic im Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS-Services in Umfang nach Compliance-Programm . Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung von Amazon Inspector Classic richtet sich nach der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften. AWS bietet die folgenden Ressourcen zur Unterstützung bei der Einhaltung von Vorschriften:

- Schnellstartanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von sicherheits- und konformitätsorientierten Basisumgebungen auf AWS angegeben.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen erstellen AWS können.
- AWS Ressourcen zur Einhaltung von — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen können AWS , ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Resilienz in Amazon Inspector Classic

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Amazon Inspector Classic ist hochverfügbar und führt Abfragen mithilfe von Rechenressourcen in mehreren Availability Zones aus. Die Abfragen werden automatisch weitergeleitet, wenn eine bestimmte Availability Zone nicht erreichbar ist.

Amazon Inspector Classic verwendet Amazon S3 als zugrunde liegenden Datenspeicher, wodurch Ihre Daten hochverfügbar und dauerhaft sind. Amazon S3 bietet eine stabile Infrastruktur zum Speichern wichtiger Daten. Sie ist für eine Beständigkeit von 99,999999999 % der Objekte ausgelegt. Ihre Daten werden redundant an mehreren Standorten und auf mehreren Geräten an jedem Standort gespeichert.

Infrastruktursicherheit in Amazon Inspector Classic

Als verwalteter Service ist Amazon Inspector Classic durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon Inspector Classic 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.

Weitere Informationen zur Netzwerk- und Agentensicherheit von Amazon Inspector Classic finden Sie unterthe section called “Netzwerk- und Amazon Inspector Classic-Agentensicherheit”.

Konfiguration und Schwachstellenanalyse in Amazon Inspector Classic

Amazon Inspector Classic bietet eine vordefinierte Software namens Agent, die Sie optional im Betriebssystem der EC2 Instances installieren können, die Sie bewerten möchten. Der Agent erfasst umfangreiche Konfigurationsdaten, die sogenannte Telemetrie. Weitere Informationen zu Amazon Inspector Classic-Agenten finden Sie unterAmazon Inspector Classic-Agenten.

Bewährte Sicherheitsmethoden für Amazon Inspector Classic

Amazon Inspector Classic bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Diese bewährten Methoden stellen allgemeine Leitlinien dar und bilden keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Eine Liste der bewährten Sicherheitsmethoden für Amazon Inspector Classic finden Sie unterthe section called “Bewährte Sicherheitsmethoden für Amazon Inspector Classic”.

Amazon Inspector Classic-Agenten

Der Amazon Inspector Classic-Agent ist eine Einheit, die Informationen zu installierten Paketen und Softwarekonfigurationen für eine EC2 Amazon-Instance sammelt. Obwohl nicht in allen Fällen erforderlich, sollten Sie den Amazon Inspector Classic-Agenten auf jeder Ihrer EC2 Amazon-Ziel-Instances installieren, um deren Sicherheit umfassend beurteilen zu können.

Weitere Informationen darüber, wie der Agent installiert, deinstalliert und neu installiert wird, wie Sie sicherstellen, dass der Agent ausgeführt wird, und wie Sie Proxy-Unterstützung für den Agenten konfigurieren, finden Sie unter Arbeiten mit Amazon Inspector Classic-Agenten auf Linux-basierten Betriebssystemen und Arbeiten mit Amazon Inspector Classic-Agenten auf Windows-basierten Betriebssystemen.

> **Note**
>
> Für die Ausführung des Regelpakets zur Netzwerkerreichbarkeit ist kein Amazon Inspector Classic-Agent erforderlich.

> **Important**
>
> Der Amazon Inspector Classic-Agent stützt sich auf EC2 Amazon-Instance-Metadaten, um korrekt zu funktionieren. Er greift mithilfe von Version 1 oder Version 2 des Instance-Metadaten-Service (IMDSv1 oder IMDSv2) auf Instance-Metadaten zu. Weitere Informationen zu Instanz-Metadaten und Zugriffsmethoden finden Sie unter EC2 Instanz-Metadaten und Benutzerdaten.

Themen

- Amazon Inspector Classic-Agenten installieren
- Arbeiten mit Amazon Inspector Classic-Agenten auf Linux-basierten Betriebssystemen
- Arbeiten mit Amazon Inspector Classic-Agenten auf Windows-basierten Betriebssystemen
- (Optional) Überprüfen Sie die Signatur des Amazon Inspector Classic-Agenteninstallationsskripts auf Linux-basierten Betriebssystemen
- (Optional) Überprüfen Sie die Signatur des Amazon Inspector Classic-Agenteninstallationsskripts auf Windows-basierten Betriebssystemen

Agentenrechte für Amazon Inspector Classic

Sie benötigen Administrator- oder Root-Rechte, um den Amazon Inspector Classic-Agenten zu installieren. Auf unterstützten Linux-basierten Betriebssystemen besteht der Agent aus einer ausführbaren Datei im Benutzermodus, die mit Root-Zugriff ausgeführt wird. Auf unterstützten Windows-basierten Betriebssystemen besteht der Agent aus einem Updater Service und einem Agent Service. Beide werden im Benutzermodus mit `LocalSystem`-Berechtigungen ausgeführt.

Netzwerk- und Amazon Inspector Classic-Agentensicherheit

Der Amazon Inspector Classic-Agent initiiert die gesamte Kommunikation mit dem Amazon Inspector Classic-Service. Dies bedeutet, dass der Agent über einen ausgehenden Netzwerkpfad an öffentliche Endpunkte verfügen muss, um Telemetriedaten an sie senden zu können. Beispielsweise könnte der Agent eine Verbindung zu `arsenal.<region>.amazonaws.com` einem Amazon S3-Bucket herstellen oder der Endpunkt könnte ein Amazon S3 S3-Bucket sein`s3.dualstack.<region>.amazonaws.com`. Stellen Sie sicher, dass Sie es durch die tatsächliche AWS Region `<region>` ersetzen, in der Sie Amazon Inspector Classic ausführen. Weitere Informationen finden Sie unter AWS IP-Adressbereiche. Da alle Verbindungen vom Agenten ausgehend hergestellt werden, ist es nicht erforderlich, Ports in Ihren Sicherheitsgruppen zu öffnen, um eingehende Kommunikation mit dem Agenten von Amazon Inspector Classic aus zu ermöglichen.

Der Agent kommuniziert regelmäßig mit Amazon Inspector Classic über einen TLS-geschützten Kanal, der entweder anhand der AWS Identität authentifiziert wird, die der Rolle der EC2 Instance zugeordnet ist, oder, falls keine Rolle zugewiesen ist, anhand des Metadatendokuments der Instance. Sobald er authentifiziert ist, sendet der Agent Heartbeat-Nachrichten an den Service und empfängt Anweisungen vom Service als Antworten auf die Heartbeat-Nachrichten. Wenn eine Bewertung geplant wurde, erhält der Agent die Anweisungen für diese Bewertung. Diese Anleitungen sind strukturierte JSON-Dateien und informieren den Agenten, um bestimmte vorkonfigurierte Sensoren

im Agenten zu aktivieren oder zu deaktivieren. Jede Anweisungsaktion ist innerhalb des Agenten vorab definiert. Es können keine beliebigen Anweisungen ausgeführt werden.

Während einer Bewertung sammelt der Agent Telemetriedaten aus dem System, um sie über einen TLS-geschützten Kanal an Amazon Inspector Classic zurückzuschicken. Der Agent macht keine Änderungen am System, von dem er Daten sammelt. Nachdem der Agent die Telemetriedaten erfasst hat, sendet er die Daten zur Verarbeitung an Amazon Inspector Classic zurück. Über die von ihm generierten Telemetriedaten hinaus ist der Agent nicht in der Lage, andere Daten über das System oder die Bewertungsziele zu sammeln oder zu übermitteln. Derzeit gibt es beim Agenten keine Methode zum Abfangen und Untersuchen von Telemetriedaten.

Agenten-Updates für Amazon Inspector Classic

Sobald Updates für den Amazon Inspector Classic-Agenten verfügbar sind, werden sie automatisch von Amazon S3 heruntergeladen und angewendet. Dadurch werden auch alle erforderlichen Abhängigkeiten aktualisiert. Dank der automatischen Aktualisierungsfunktion müssen Sie die Versionierung der Agenten, die Sie auf Ihren EC2 Instances installiert haben, nicht mehr nachverfolgen und manuell verwalten. Alle Updates unterliegen den geprüften Amazon-Change-Control-Prozessen, um die Einhaltung der geltenden Sicherheitsstandards zu gewährleisten.

Um die Sicherheit des Agenten weiter zu gewährleisten, wird die gesamte Kommunikation zwischen dem Agenten und der Auto-Update Release Site (S3) über eine TLS-Verbindung durchgeführt und der Server authentifiziert. Alle Binärdateien, die an dem automatischen Update beteiligt sind, werden digital signiert, und die Signaturen werden vor der Installation vom Updater überprüft. Der automatische Aktualisierungsprozess wird nur während der Nicht-Bewertungsperioden ausgeführt. Wenn Fehler erkannt werden, kann der Aktualisierungsvorgang einen Rollback und Neuversuch der Aktualisierung durchführen. Schließlich dient der Aktualisierungsvorgang des Agenten zum Aktualisieren nur der Fähigkeiten des Agenten. Keine Ihrer spezifischen Informationen wird im Rahmen des Aktualisierungs-Workflows jemals vom Agenten an Amazon Inspector Classic gesendet. Die einzige Information, die als Teil des Aktualisierungsprozesses übertragen wird, ist die grundlegende Installations-Erfolgs-/Fehler-Telemetrie und ggf. eine Update-Fehler-Diagnoseinformation.

Telemetriedaten-Lebenszyklus

Die Telemetriedaten, die vom Amazon Inspector Classic-Agenten während der Bewertungsläufe generiert werden, sind in JSON-Dateien formatiert. Die Dateien werden near-real-time über TLS

an Amazon Inspector Classic übermittelt, wo sie mit einem kurzlebigen per-assessment-run, von KMS abgeleiteten Schlüssel verschlüsselt werden. Die Dateien werden sicher in einem Amazon S3 S3-Bucket gespeichert, der speziell für Amazon Inspector Classic vorgesehen ist. Die Regel-Engine von Amazon Inspector Classic greift auf die verschlüsselten Telemetriedaten im S3-Bucket zu, entschlüsselt sie im Speicher und verarbeitet die Daten anhand der konfigurierten Bewertungsregeln, um Ergebnisse zu generieren. Die Telemetriedaten, die in S3 gespeichert werden, werden nur beibehalten, um Hilfe bei Supportanfragen zuzulassen. Sie werden von Amazon nicht für andere Zwecke verwendet oder aggregiert. Nach 30 Tagen werden Telemetriedaten gemäß einer standardmäßigen S3-Bucket-Lebenszyklusrichtlinie für Amazon Inspector Classic-Daten dauerhaft gelöscht. Derzeit bietet Amazon Inspector Classic weder eine API noch einen S3-Bucket-Zugriffsmechanismus für gesammelte Telemetriedaten.

Zugriffskontrolle von Amazon Inspector Classic auf AWS Konten

Als Sicherheitsservice greift Amazon Inspector Classic nur dann auf Ihre AWS Konten und Ressourcen zu, wenn es EC2 Instances zur Bewertung finden muss, indem es nach Tags fragt. Dies erfolgt über den standardmäßigen IAM-Zugriff über die Rolle, die bei der Ersteinrichtung des Amazon Inspector Classic-Service erstellt wurde. Während einer Bewertung wird die gesamte Kommunikation mit Ihrer Umgebung durch den Amazon Inspector Classic-Agenten initiiert, der lokal auf den EC2 Instances installiert ist. Die erstellten Serviceobjekte von Amazon Inspector Classic, wie z. B. Bewertungsziele, Bewertungsvorlagen und vom Service generierte Ergebnisse, werden in einer Datenbank gespeichert, die von Amazon Inspector Classic verwaltet wird und auf die nur Amazon Inspector Classic zugreifen kann.

Beschränkungen für Amazon Inspector Classic-Agenten

Informationen zu den Agentenlimits von Amazon Inspector Classic finden Sie unterAmazon Inspector Classic-Servicebeschränkungen.

Amazon Inspector Classic-Agenten installieren

Sie können den Amazon Inspector Classic-Agent mithilfe des Systems Manager Run Command auf mehreren Instances installieren (einschließlich Linux- und Windows-basierter Instances). Alternativ können Sie den Agenten einzeln installieren, indem Sie sich bei jeder Instance anmelden. EC2 Die Verfahren in diesem Kapitel enthalten Anweisungen für beide Methoden.

Als weitere Option können Sie den Agenten schnell auf allen EC2 Amazon-Instances installieren, die in einem Bewertungsziel enthalten sind, indem Sie auf der Seite „Bewertungsziel definieren“ in der Konsole das Kontrollkästchen Agents installieren aktivieren.

Themen

> **Note**
>
> Die Verfahren in diesem Kapitel gelten für alle AWS Regionen, die von Amazon Inspector Classic unterstützt werden.

Installation des Agenten auf mehreren EC2 Instanzen mithilfe des Systems Manager Manager-Befehls Run

Sie können den Amazon Inspector Classic-Agent mit dem Systems Manager Run Command auf Ihren EC2 Instances installieren. Dadurch können Sie den Agenten remote und auf mehreren Instances (sowohl Linux- als auch Windows-basierte Instances mit demselben Befehl) gleichzeitig installieren.

> **Important**
>
> Agent-Installation mithilfe des Systems Manager Run Command wird derzeit für das Debian Betriebssystem nicht unterstützt.

> **Important**
>
> Um diese Option zu verwenden, stellen Sie sicher, dass auf Ihrer EC2 Instance der SSM-Agent installiert ist und dass sie über eine IAM-Rolle verfügt, die Run Command ermöglicht. Der SSM-Agent ist standardmäßig auf Amazon EC2 Windows-Instances und Amazon Linux-Instances installiert. Amazon EC2 Systems Manager benötigt eine IAM-Rolle für

EC2 Instances, die Befehle verarbeiten, und eine separate Rolle für Benutzer, die Befehle ausführen. Weitere Informationen finden Sie unter SSM-Agent installieren und konfigurieren und Sicherheitsrollen für SSM konfigurieren.

So installieren Sie den Agenten mit dem Systems Manager Run Command auf mehreren EC2 Instanzen

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich unter Node Tools die Option Run Command aus.
3. Wählen Sie die Option Run a command.
4. Wählen Sie als Befehlsdokument das Dokument mit dem Namen AmazonInspector-Manage ausAWSAgent, das Amazon gehört. Dieses Dokument enthält das Skript für die Installation des Amazon Inspector Classic-Agenten auf EC2 Instances.
5. Für Targets können Sie EC2 Instances mit verschiedenen Methoden auswählen. Um den Agenten auf allen Instances im Bewertungsziel zu installieren, können Sie Tags angeben, die für die Erstellung des Bewertungsziels verwendet wurden.
6. Treffen Sie Ihre Auswahl für die übrigen verfügbaren Optionen mithilfe der Anweisungen unter Ausführen von Befehlen mit der Konsole und wählen Sie Run (Ausführen).

> **Note**
>
> Sie können den Agenten auch auf mehreren EC2 Instanzen (sowohl auf Linux- als auch auf Windows-Basis) installieren, wenn Sie ein Bewertungsziel erstellen, oder Sie können die Schaltfläche Agenten mit Befehl ausführen für ein vorhandenes Ziel verwenden. Weitere Informationen finden Sie unter Erstellen eines Bewertungsziels.

Den Agenten auf einer Linux-basierten Instanz installieren EC2

Gehen Sie wie folgt vor, um den Amazon Inspector Classic-Agent auf einer Linux-basierten EC2 Instance zu installieren.

Um den Agenten auf einer Linux-basierten EC2 Instance zu installieren

1. Melden Sie sich bei Ihrer EC2 Instance an, auf der ein Linux-basiertes Betriebssystem ausgeführt wird, auf dem Sie den Amazon Inspector Classic-Agent installieren möchten.

   > **Note**
   >
   > Informationen zu den Betriebssystemen, die Amazon Inspector Classic unterstützt, finden Sie unterVon Amazon Inspector Classic unterstützte Betriebssysteme und Regionen.

2. Laden Sie das Agent-Installationsskript herunter, indem Sie einen der folgenden Befehle ausführen:

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

3. (Optional) Überprüfen Sie, ob das -Agent-Installationsskript geändert wurde oder beschädigt ist. Weitere Informationen finden Sie unter (Optional) Überprüfen Sie die Signatur des Amazon Inspector Classic-Agenteninstallationsskripts auf Linux-basierten Betriebssystemen.

4. Führen Sie sudo bash install aus, um den Agenten zu installieren.

   > **Note**
   >
   > Wenn Sie den Agenten in einer SELinux Umgebung installieren, wird Amazon Inspector Classic möglicherweise als unbegrenzter Daemon erkannt. Sie können dies vermeiden, indem Sie die Domäne des Agentenprozesses von der `initrc_t` Standarddomain auf ändern. `bin_t` Verwenden Sie die folgenden Befehle, um den Amazon Inspector Classic-Ausführungsskripten den `bin_t` Kontext zuzuweisen, bevor Sie den Agenten für installieren SELinux:
   > sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
   > sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent

> **Note**
>
> Sobald Updates für den -Agenten verfügbar sind, werden sie automatisch von Amazon S3 heruntergeladen und angewendet. Weitere Informationen finden Sie unter Agenten-Updates für Amazon Inspector Classic.
> Wenn Sie diese automatische Aktualisierung überspringen möchten, führen Sie den folgenden Befehl bei der Installation des Agenten aus:
> sudo bash install -u false

> **Note**
>
> (Optional) Um das Agent-Installationsskript zu entfernen, führen Sie rm install aus.

5. Stellen Sie sicher, dass die folgenden für den Agenten erforderlichen Dateien installiert sind und ordnungsgemäß funktionieren:

   - `libcurl4` (erforderlich für die Installation des Agenten auf Ubuntu 18.04)
   - `libcurl3`
   - `libgcc1`
   - `libc6`
   - `libstdc++6`
   - `libssl1.0.1`
   - `libssl1.0.2` (erforderlich für die Installation des Agenten auf Debian 9)
   - `libssl1.1`(erforderlich, um den Agenten auf Ubuntu 20.04 LTS zu installieren)
   - `libpcap0.8`

Installation des Agenten auf einer Windows-basierten Instanz EC2

Gehen Sie wie folgt vor, um den Amazon Inspector Classic-Agent auf einer Windows-basierten EC2 Instance zu installieren.

Um den Agenten auf einer Windows-basierten Instance zu installieren EC2

1. Melden Sie sich bei Ihrer EC2 Instanz an, auf der ein Windows-basiertes Betriebssystem ausgeführt wird, auf dem Sie den Agenten installieren möchten.

   > **Note**
   >
   > Weitere Informationen zu den Betriebssystemen, die Amazon Inspector Classic unterstützt, finden Sie unterVon Amazon Inspector Classic unterstützte Betriebssysteme und Regionen.

2. Laden Sie die folgende Datei herunter:

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

3. Öffnen Sie ein Befehlszeilenfenster (mit administrativen Berechtigungen), navigieren Sie zum Speicherort der heruntergeladenen Datei `AWSAgentInstall.exe` und führen Sie die EXE-Datei aus, um den Agenten zu installieren.

   > **Note**
   >
   > Sobald Updates für den -Agenten verfügbar sind, werden sie automatisch von Amazon S3 heruntergeladen und angewendet. Weitere Informationen finden Sie unter Agenten-Updates für Amazon Inspector Classic.
   > Wenn Sie diese automatische Aktualisierung überspringen möchten, führen Sie den folgenden Befehl bei der Installation des Agenten aus:
   > AWSAgentInstall.exe AUTOUPDATE=No

Arbeiten mit Amazon Inspector Classic-Agenten auf Linux-basierten Betriebssystemen

Sie können das Verhalten von Amazon Inspector Classic-Agenten installieren, entfernen, überprüfen und ändern. Melden Sie sich bei Ihrer EC2 Amazon-Instance an, auf der ein Linux-basiertes Betriebssystem ausgeführt wird, und führen Sie eines der folgenden Verfahren aus. Weitere Informationen zu den Betriebssystemen, die für Amazon Inspector Classic unterstützt werden, finden Sie unterVon Amazon Inspector Classic unterstützte Betriebssysteme und Regionen.

Important

Der Amazon Inspector Classic-Agent stützt sich auf EC2 Amazon-Instance-Metadaten, um korrekt zu funktionieren. Er greift mithilfe von Version 1 oder Version 2 des Instance-Metadaten-Service (IMDSv1 oder IMDSv2) auf Instance-Metadaten zu. Weitere Informationen zu Instanz-Metadaten und Zugriffsmethoden finden Sie unter EC2 Instanz-Metadaten und Benutzerdaten.

Note

Die Befehle in diesem Abschnitt funktionieren in allen AWS Regionen, die von Amazon Inspector Classic unterstützt werden.

Themen

Überprüfen, ob der Amazon Inspector Classic-Agent läuft

- Um zu überprüfen, ob der Agent installiert ist und läuft, melden Sie sich bei Ihrer EC2 Instance an und führen Sie den folgenden Befehl aus:

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

  Dieser Befehl gibt den Status des aktuell ausgeführten Agenten oder einen Fehler zurück, der angibt, dass der Agent nicht kontaktiert werden kann.

Den Amazon Inspector Classic-Agenten beenden

- Um den Agenten zu stoppen, führen Sie den folgenden Befehl aus:

sudo /etc/init.d/awsagent stop

Den Amazon Inspector Classic-Agenten starten

- Um den Agenten zu starten, führen Sie den folgenden Befehl aus:

  sudo /etc/init.d/awsagent start

Agenteneinstellungen von Amazon Inspector Classic ändern

Nachdem der Amazon Inspector Classic-Agent installiert ist und auf Ihrer EC2 Instance ausgeführt wird, können Sie die Einstellungen in der `agent.cfg` Datei ändern, um das Verhalten des Agenten zu ändern. Auf Linux-basierten Betriebssystemen befindet sich die Datei `agent.cfg` im Verzeichnis `/opt/aws/awsagent/etc`. Nachdem Sie die Datei `agent.cfg` geändert und gespeichert haben, müssen Sie den Agenten beenden und neu starten, damit die Änderungen wirksam werden.

> **Important**
>
> Wir empfehlen Ihnen dringend, die Datei `agent.cfg` nur mit Anleitung vom AWS Support zu modifizieren.

Konfiguration der Proxyunterstützung für einen Amazon Inspector Classic-Agenten

Um Proxy-Unterstützung für einen Agenten auf einem Linux-basierten Betriebssystem zu erhalten, verwenden Sie eine agentenspezifische Konfigurationsdatei mit bestimmten Umgebungsvariablen. Weitere Informationen finden Sie unter https://wiki.archlinux. org/index.php/proxy_Einstellungen.

Führen Sie einen der folgenden Schritte aus:

Um einen Agenten auf einer EC2 Instanz zu installieren, die einen Proxyserver verwendet

1. Erstellen Sie eine Datei namens `awsagent.env`, und speichern Sie sie im Verzeichnis `/etc/init.d/`.
2. Bearbeiten Sie `awsagent.env`, um diese Umgebungsvariablen im folgenden Format einzuschließen:

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

> **Note**
>
> Ersetzen Sie die Werte in den obigen Beispielen nur durch gültige Kombinationen aus Hostname und Portnummer. Geben Sie die IP-Adresse des Instance-Metadatenendpunkts (169.254.169.254) für die Variable `no_proxy` an.

3. Installieren Sie den Amazon Inspector Classic-Agenten, indem Sie die Schritte des Den Agenten auf einer Linux-basierten Instanz installieren EC2 Verfahrens ausführen.

Um die Proxyunterstützung auf einer EC2 Instance zu konfigurieren, auf der ein Agent ausgeführt wird

1. Um die Proxyunterstützung zu konfigurieren, muss die Version des Agenten, der auf Ihrer EC2 Instance ausgeführt wird, 1.0.800.1 oder höher sein. Wenn die automatische Aktualisierung für den Agenten aktiviert ist, können Sie überprüfen, ob die Agenten-Version 1.0.800.1 oder höher ist, indem Sie das Verfahren Überprüfen, ob der Amazon Inspector Classic-Agent läuft verwenden. Wenn Sie den automatischen Aktualisierungsprozess für den Agenten nicht aktiviert haben, müssen Sie den Agenten erneut auf dieser EC2 Instanz installieren, indem Sie das Den Agenten auf einer Linux-basierten Instanz installieren EC2 Verfahren befolgen.
2. Erstellen Sie eine Datei namens `awsagent.env` und speichern Sie sie im Verzeichnis `/etc/init.d/`.
3. Bearbeiten Sie `awsagent.env`, um diese Umgebungsvariablen im folgenden Format einzuschließen:

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

> **Note**
>
> Ersetzen Sie die Werte in den obigen Beispielen nur durch gültige Kombinationen aus Hostname und Portnummer. Geben Sie die IP-Adresse des Instance-Metadatenendpunkts (169.254.169.254) für die Variable `no_proxy` an.

4. Starten Sie den Agenten neu, indem Sie ihn zunächst mit dem folgenden Befehl stoppen:

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

   Die Proxy-Einstellungen werden sowohl vom Agenten als auch von der automatischen Aktualisierung verwendet.

Den Amazon Inspector Classic-Agenten deinstallieren

So deinstallieren Sie den Agenten

1. Melden Sie sich bei Ihrer EC2 Instance an, auf der ein Linux-basiertes Betriebssystem ausgeführt wird, auf dem Sie den Agenten deinstallieren möchten.

   > **Note**
   >
   > Weitere Informationen zu den Betriebssystemen, die für Amazon Inspector Classic unterstützt werden, finden Sie unterVon Amazon Inspector Classic unterstützte Betriebssysteme und Regionen.

2. Um den Agent zu deinstallieren, verwenden Sie einen der folgenden Befehle:

   - Führen Sie unter Amazon Linux, CentOS und Red Hat den folgenden Befehl aus:

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

   - Führen Sie auf Ubuntu Server den folgenden Befehl aus:

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

Arbeiten mit Amazon Inspector Classic-Agenten auf Windows-basierten Betriebssystemen

Sie können das Verhalten von Amazon Inspector Classic-Agenten starten, beenden und ändern. Melden Sie sich bei Ihrer EC2 Instance an, auf der ein Windows-basiertes Betriebssystem ausgeführt wird, und führen Sie eines der Verfahren in diesem Kapitel durch. Weitere Informationen zu den Betriebssystemen, die für Amazon Inspector Classic unterstützt werden, finden Sie unterVon Amazon Inspector Classic unterstützte Betriebssysteme und Regionen.

Important

Der Amazon Inspector Classic-Agent stützt sich auf EC2 Amazon-Instance-Metadaten, um korrekt zu funktionieren. Er greift mithilfe von Version 1 oder Version 2 des Instance-Metadaten-Service (IMDSv1or IMDSv2) auf Instance-Metadaten zu. Weitere Informationen zu Instanz-Metadaten und Zugriffsmethoden finden Sie unter EC2 Instanz-Metadaten und Benutzerdaten.

Note

Die Befehle in diesem Kapitel funktionieren in allen AWS Regionen, die von Amazon Inspector Classic unterstützt werden.

Themen

Einen Amazon Inspector Classic-Agenten starten oder beenden oder überprüfen, ob der Agent läuft

So starten, stoppen oder überprüfen Sie einen Agenten

1. Wählen Sie auf Ihrer EC2 Instance Start, Run und geben Sie dann die Eingabetaste ein**`services.msc`**.
2. Wenn der Agent erfolgreich ausgeführt wird, werden zwei Services mit ihrem Status auf Started (Gestartet) oder Running (Wird ausgeführt) im Service-Fenster aufgelistet: AWS Agent Service und AWS Agent Updater Service.
3. Um den Agenten zu starten, klicken Sie mit der rechten Maustaste auf AWS Agent Service und wählen Sie dann Start. Wenn der Service erfolgreich gestartet wurde, wird der Status auf Started (Gestartet) oder Running (Wird ausgeführt) aktualisiert.
4. Um den Agenten zu beenden, klicken Sie mit der rechten Maustaste auf AWS Agent Service und wählen Sie Stop (Stoppen) aus. Wenn der Service erfolgreich angehalten wird, wird der Status deaktiviert (wird leer angezeigt). Wir empfehlen nicht, den AWS Agent Updater Service zu beenden, da er dann die Installation aller künftigen Verbesserungen und Problembehebungen im Agent deaktiviert.
5. Um zu überprüfen, ob der Agent installiert ist und ausgeführt wird, melden Sie sich bei Ihrer EC2 Instance an und öffnen Sie eine Befehlszeile mit Administratorrechten. Navigieren Sie zu `C:\Program Files\Amazon Web Services\AWS Agent` und führen Sie den folgenden Befehl aus:

   AWSAgentStatus.exe

   Dieser Befehl gibt den Status des aktuell ausgeführten Agenten oder einen Fehler zurück, der angibt, dass der Agent nicht kontaktiert werden kann.

Agenteneinstellungen von Amazon Inspector Classic ändern

Nachdem der Amazon Inspector Classic-Agent installiert ist und auf Ihrer EC2 Instance ausgeführt wird, können Sie die Einstellungen in der `agent.cfg` Datei ändern, um das Verhalten des Agenten zu ändern. Auf Windows-basierten Betriebssystemen befindet sich die Datei im Verzeichnis `C:\ProgramData\Amazon Web Services\AWS Agent`. Nachdem Sie die Datei `agent.cfg` geändert und gespeichert haben, müssen Sie den Agenten beenden und neu starten, damit die Änderungen wirksam werden.

> **Important**
>
> Wir empfehlen Ihnen dringend, die Datei `agent.cfg` nur mit Anleitung vom AWS Support zu modifizieren.

Konfiguration der Proxyunterstützung für einen Amazon Inspector Classic-Agenten

Um Proxy-Support für einen Agenten auf einem Windows-basierten Betriebssystem aufzurufen, verwenden Sie den `WinHTTP`-Proxy. Informationen zum Einrichten des `WinHTTP`-Proxys mit dem `netsh`-Dienstprogramm finden Sie unter Netsh-Befehle für Windows Hypertext Transfer Protocol (WINHTTP).

> **Important**
>
> Für Windows-basierte Instances werden nur HTTPS-Proxys unterstützt.

Führen Sie einen der folgenden Schritte aus:

Um einen Agenten auf einer EC2 Instance zu installieren, die einen Proxy-Server verwendet

1. Laden Sie die folgende Datei herunter: `https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`
2. Öffnen Sie ein Befehlszeilenfenster oder ein PowerShell Fenster (mit Administratorrechten). Navigieren Sie zu dem Verzeichnis, in das Sie die Datei `AWSAgentInstall.exe` heruntergeladen haben, und führen Sie dann den folgenden Befehl aus:

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

Um die Proxyunterstützung auf einer EC2 Instanz zu konfigurieren, auf der ein Agent ausgeführt wird

1. Um die Proxyunterstützung zu konfigurieren, muss die Version des Amazon Inspector Classic-Agenten, der auf Ihrer EC2 Instance ausgeführt wird, 1.0.0.59 oder höher sein. Wenn die automatische Aktualisierung für den Agenten aktiviert ist, können Sie überprüfen, ob die Agenten-Version 1.0.0.59 oder höher ist, indem Sie das Verfahren Einen Amazon Inspector Classic-Agenten starten oder beenden oder überprüfen, ob der Agent läuft verwenden. Wenn Sie

den automatischen Aktualisierungsprozess für den Agenten nicht aktiviert haben, müssen Sie den Agenten erneut auf dieser EC2 Instanz installieren, indem Sie das Installation des Agenten auf einer Windows-basierten Instanz EC2 Verfahren befolgen.

2. Öffnen Sie den Registrierungs-Editor (`regedit.exe`).
3. Navigieren Sie zu folgendem Registrierungsschlüssel: `"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`.
4. Erstellen Sie innerhalb dieses Registrierungsschlüssels einen `DWORD(32bit)`-Registrierungswert mit dem Namen `"UseProxy"`.
5. Doppelklicken Sie auf den Wert und stellen Sie den Wert auf 1 ein.
6. Geben Sie **`services.msc`** ein, suchen Sie den AWS Agent Service und AWS Agent Updater Service im Fenster Services und starten Sie jeden Vorgang neu. Nachdem Sie beide Vorgänge erfolgreich neu gestartet haben, führen Sie die Datei `AWSAgentStatus.exe` aus (siehe Schritt 5 in Einen Amazon Inspector Classic-Agenten starten oder beenden oder überprüfen, ob der Agent läuft). Zeigen Sie den Status Ihres Agenten an und überprüfen Sie, ob er den konfigurierten Proxy verwendet.

Den Amazon Inspector Classic-Agenten deinstallieren

So deinstallieren Sie den Agenten

1. Melden Sie sich bei Ihrer EC2 Instance an, auf der ein Windows-basiertes Betriebssystem ausgeführt wird, auf dem Sie den Amazon Inspector Classic-Agent deinstallieren möchten.

   > **Note**
   >
   > Weitere Informationen zu den Betriebssystemen, die für Amazon Inspector Classic unterstützt werden, finden Sie unterVon Amazon Inspector Classic unterstützte Betriebssysteme und Regionen.

2. Navigieren Sie auf Ihrer EC2 Instance zu Systemsteuerung, Programme hinzufügen/entfernen.
3. Wählen Sie in der Liste der installierten Programme die Option AWS Agent aus und klicken Sie dann auf Deinstallieren.

(Optional) Überprüfen Sie die Signatur des Amazon Inspector Classic-Agenteninstallationsskripts auf Linux-basierten Betriebssystemen

In diesem Thema wird der empfohlene Prozess zur Überprüfung der Gültigkeit des Installationsskripts des Amazon Inspector Classic-Agenten für Linux-Dateien beschrieben.

Wenn Sie eine Anwendung aus dem Internet herunterladen, empfehlen wir Ihnen, die Identität des Softwareverlegers zu authentifizieren und zu überprüfen, ob die Anwendung seit ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Dies schützt Sie davor, eine Version der Anwendung zu installieren, die einen Virus oder einen anderen bösartigen Code enthält.

Wenn Sie nach dem Ausführen der Schritte in diesem Thema feststellen, dass die Software für den Amazon Inspector Classic-Agenten verändert oder beschädigt wurde, führen Sie die Installationsdatei NICHT aus. Kontaktieren Sie stattdessen den AWS Support.

Amazon Inspector Classic-Agenten für Linux-Dateien für Linux-Dateien werden unter Verwendung GnuPG einer Open-Source-Implementierung des Pretty Good Privacy (OpenPGP) -Standards für sichere digitale Signaturen, signiert. GnuPG(auch bekannt alsGPG) ermöglicht Authentifizierung und Integritätsprüfung mithilfe einer digitalen Signatur. Amazon EC2 veröffentlicht den öffentlichen Schlüssel und Signaturen zur Bestätigung der heruntergeladenen Amazon EC2 CLI-Tools. Weitere Informationen zu PGP und GnuPG (GPG) finden Sie unter http://www.gnupg.org.

Der erste Schritt besteht darin, eine Vertrauensstellung mit dem Software-Publisher zu schaffen. Laden Sie den öffentlichen Schlüssel des Softwareherausgebers herunter, überprüfen Sie, ob der Besitzer des öffentlichen Schlüssels derjenige ist, der er behauptet zu sein, und fügen Sie dann den öffentlichen Schlüssel zu Ihrem Schlüsselbund hinzu. Ihr Schlüsselbund ist eine Sammlung von bekannten öffentlichen Schlüsseln. Nachdem Sie die Echtheit des öffentlichen Schlüssels überprüft haben, können Sie ihn verwenden, um die Signatur der Anwendung zu überprüfen.

Themen

Installieren der GPG-Tools

Wenn Sie das Betriebssystem Linux oder Unix verwenden, sind die GPG-Tools wahrscheinlich bereits installiert. Um zu testen, ob die Tools auf Ihrem System installiert sind, geben Sie gpg in einer Eingabeaufforderung ein. Wenn die GPG-Tools installiert sind, sehen Sie eine Eingabeaufforderung. Wenn die GPG-Tools nicht installiert sind, sehen Sie eine Fehlermeldung, die anzeigt, dass der Befehl nicht gefunden werden kann. Sie können das GnuPG-Paket von einem Repository aus installieren.

So installieren Sie GPG-Tools auf Debian-basiertem Linux

- Führen Sie von einem Terminal folgenden Befehl aus: apt-get install gnupg.

So installieren Sie GPG-Tools unter Red-Hat-basiertem Linux

- Führen Sie von einem Terminal folgenden Befehl aus: yum install gnupg.

Authentifizieren und Importieren des öffentlichen Schlüssels

Der nächste Schritt des Vorgangs besteht darin, den öffentlichen Schlüssel von Amazon Inspector Classic zu authentifizieren und ihn als vertrauenswürdigen Schlüssel Ihrem GPG Schlüsselbund hinzuzufügen.

So authentifizieren und importieren Sie den öffentlichen Schlüssel von Amazon Inspector Classic

1. Besorgen Sie sich ein Exemplar unseres öffentlichen GPG-Schlüssels, indem Sie einen der folgenden Schritte ausführen:
   - Laden Sie es von https://d1wk0tztpsntt1.cloudfront herunter. net/linux/latest/inspector.gpg.
   - Kopieren Sie den Schlüssel aus dem folgenden Text und fügen Sie ihn in eine Datei namens `inspector.gpg` ein. Vergewissern Sie sich, alles Folgende einzubeziehen:

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

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
```

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

2. Verwenden Sie bei einer Eingabeaufforderung in dem Verzeichnis, in dem Sie inspector.gpg gespeichert haben, den folgenden Befehl zum Importieren des öffentlichen Schlüssels von Amazon Inspector Classic in den Schlüsselbund:

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

   Der Befehl gibt Ergebnisse wie die folgenden zurück:

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

   Notieren Sie sich den Schlüsselwert. Sie brauchen ihn im nächsten Schritt. Im vorangegangenen Beispiel ist der Schlüsselwert 58360418.

3. Überprüfen Sie den Fingerabdruck, indem Sie den folgenden Befehl ausführen und Schlüssel-Wert durch den Wert des vorherigen Schritts ersetzen:

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

Dieser Befehl gibt Ergebnisse wie die folgenden zurück:

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

Zusätzlich sollte der Fingerabdruck-String identisch mit `DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418` sein, wie im voranstehenden Beispiel angezeigt. Vergleichen Sie den Schlüssel-Fingerabdruck mit demjenigen, der auf dieser Seite veröffentlicht ist. Sie sollten übereinstimmen. Wenn sie nicht übereinstimmen, installieren Sie das Amazon Inspector Classic-Installationsskript nicht und wenden Sie sich an den AWS-Unterstützung Support.

Verifizieren der Signatur des Pakets

Nachdem Sie die GPG Tools installiert, den öffentlichen Schlüssel von Amazon Inspector Classic authentifiziert, importiert und überprüft haben, ob der öffentliche Schlüssel von vertrauenswürdig ist, sind Sie bereit, die Signatur des -Installationsskripts zu überprüfen.

So überprüfen Sie die Signatur des -Installationsskripts

1. Führen Sie bei einer Eingabeaufforderung den folgenden Befehl aus, um die Signaturdatei für das Installationsskript herunterzuladen:

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

2. Überprüfen Sie die Signatur, indem Sie den folgenden Befehl an einer Eingabeaufforderung in dem Verzeichnis ausführen, in dem Sie `install.sig` und die Amazon Inspector Classic-Installationsdatei gespeichert haben. Beide Dateien müssen vorhanden sein.

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

   Die Ausgabe sollte wie folgt aussehen:

   ```
   gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
   ```

```
gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
```

Wenn die Ausgabe den Begriff enthält`Good signature from "Amazon Inspector <inspector@amazon.com>"`, bedeutet dies, dass die Signatur erfolgreich überprüft wurde und Sie mit der Ausführung des Amazon Inspector Classic-Installationsskripts fortfahren können.

Wenn die Ausgabe die Bezeichnung `BAD signature`enthält, überprüfen Sie, ob Sie das Verfahren korrekt durchgeführt haben. Wenn Sie diese Antwort weiterhin erhalten, führen Sie die Installationsdatei, die Sie zuvor heruntergeladen haben, nicht aus, und kontaktieren Sie AWS Support.

Im Folgenden finden Sie Details zu den Warnungen, die möglicherweise angezeigt werden:

- WARNUNG: Dieser Schlüssel ist nicht mit einer vertrauenswürdigen Signatur zertifiziert! Es gibt keinen Hinweis darauf, dass die Signatur dem Besitzer gehört. Dies bezieht sich auf Ihr persönliches Vertrauen im Glauben, dass Sie einen authentischen öffentlichen Schlüssel für Amazon Inspector Classic besitzen. In einer idealen Welt würden Sie ein AWS-Büro aufsuchen und den Schlüssel persönlich erhalten. Doch häufiger laden Sie ihn von einer Website herunter. In diesem Fall handelt es sich bei der Website um eine AWS-Website.
- gpg: Keine endgültig vertrauenswürdigen Schlüssel gefunden Dies bedeutet, dass der bestimmte Schlüssel nicht "endgültig vertrauenswürdig" für Sie oder für andere Personen ist, denen Sie vertrauen.

Weitere Informationen finden Sie unter http://www.gnupg.org.

(Optional) Überprüfen Sie die Signatur des Amazon Inspector Classic-Agenteninstallationsskripts auf Windows-basierten Betriebssystemen

In diesem Thema wird das empfohlene Verfahren zur Überprüfung der Gültigkeit des Installationsskripts des Amazon Inspector Classic-Agenten für Windows-basierte Betriebssysteme beschrieben.

Wenn Sie eine Anwendung aus dem Internet herunterladen, empfehlen wir Ihnen, die Identität des Softwareverlegers zu authentifizieren und zu überprüfen, ob die Anwendung seit ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Dies schützt Sie davor, eine Version der Anwendung zu installieren, die einen Virus oder einen anderen bösartigen Code enthält.

Wenn Sie nach Ausführung der Schritte in diesem Thema feststellen, dass die Software für den Amazon Inspector Classic-Agent verändert oder beschädigt ist, führen Sie die Installationsdatei NICHT aus. Kontaktieren Sie stattdessen den AWS Support.

Um die Gültigkeit des heruntergeladenen Installationsskripts des Agenten auf Windows-Betriebssystemen zu überprüfen, müssen Sie sicherstellen, dass der Thumbprint des Amazon Services LLC-Ausstellerzertifikats folgendem Wert entspricht:

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

Um diesen Wert zu überprüfen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die heruntergeladen `AWSAgentInstall.exe`, und öffnen Sie das Eigenschaften-Fenster.
2. Wählen Sie die Registerkarte Digital Signatures aus.
3. Wählen Sie in der Signaturliste Amazon Web Services, Inc. und dann Details aus.
4. Falls die Registerkarte General nicht bereits ausgewählt ist, klicken Sie darauf und dann auf View Certificate.
5. Wählen Sie die Registerkarte Details aus, und anschließend die Option All (Alle) in der Dropdown-Liste Show (Zeigen), wenn diese nicht bereits ausgewählt ist.
6. Scrollen Sie nach unten zum Feld Thumbprint und wählen Sie Thumbprint aus. Der gesamte Thumbprint-Wert wird im unteren Fenster angezeigt.

   - Wenn der Thumbprint-Wert im unteren Fenster mit folgendem Wert identisch ist:

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

     ist Ihr heruntergeladenes Agenten-Installationsskript authentisch und kann sicher installiert werden.
   - Wenn der Thumbprint-Wert im unteren Detailfenster nicht mit dem obigen Wert übereinstimmt, führen Sie `AWSAgentInstall.exe` nicht aus.

Bewertungsziele von Amazon Inspector Classic

Sie können Amazon Inspector Classic verwenden, um zu bewerten, ob Ihre AWS Bewertungsziele (Ihre AWS Ressourcensammlungen) potenzielle Sicherheitsprobleme aufweisen, die Sie beheben sollten.

Important

Derzeit können Ihre Bewertungsziele nur aus EC2 Instances bestehen, die auf unterstützten Betriebssystemen ausgeführt werden. Weitere Informationen zu unterstützten Betriebssystemen und unterstützten AWS-Regionen finden Sie unter the section called “Unterstützte Betriebssysteme und Regionen”.

Note

Informationen zum Starten von EC2 Instances finden Sie in der Amazon Elastic Compute Cloud-Dokumentation.

Themen

Tagging von Ressourcen zum Erstellen eines Bewertungsziels

Um ein Bewertungsziel für Amazon Inspector Classic zur Bewertung zu erstellen, markieren Sie zunächst die EC2 Instances, die Sie in Ihr Ziel aufnehmen möchten. Tags sind Wörter oder Ausdrücke, die als Metadaten zur Identifizierung und Organisation Ihrer Instances und anderer AWS Ressourcen dienen. Amazon Inspector Classic verwendet die von Ihnen erstellten Tags, um die Instances zu identifizieren, die zu Ihrem Ziel gehören.

Jedes AWS Tag besteht aus einem Schlüssel- und Wertepaar Ihrer Wahl. Sie könnten Ihren Schlüssel beispielsweise „Name“ und Ihren Wert „MyFirstInstance“ nennen. Nachdem Sie Ihre

Instances markiert haben, verwenden Sie die Amazon Inspector Classic-Konsole, um die Instances Ihrem Bewertungsziel hinzuzufügen. Es ist nicht notwendig, dass irgendeine Instance mit mehr als einem Tag-Schlüssel-Wertepaar übereinstimmt.

Wenn Sie Ihre EC2 Instances taggen, um Bewertungsziele zu erstellen, können Sie Ihre eigenen benutzerdefinierten Tag-Schlüssel erstellen oder Tag-Schlüssel verwenden, die von anderen Benutzern desselben AWS Kontos erstellt wurden. Sie können auch die Tag-Keys verwenden, die AWS automatisch erstellt werden. Erstellt beispielsweise AWS automatisch einen Name-Tag-Schlüssel für die EC2 Instances, die Sie starten.

Sie können Tags zu EC2 Instances hinzufügen, wenn Sie sie erstellen, oder Sie können diese Tags einzeln auf der Konsolenseite für jede EC2 Instance hinzufügen, ändern oder entfernen. Mit dem Tag-Editor können Sie auch mehreren EC2 Instanzen gleichzeitig Tags hinzufügen.

Weitere Informationen hierzu finden Sie unter Tag Editor. Weitere Informationen zum Taggen von EC2 Instanzen finden Sie unter Ressourcen und Tags.

Zielgrenzwerte für die Amazon Inspector Classic-Bewertung

Sie können bis zu 50 Bewertungsziele pro AWS Konto erstellen. Weitere Informationen finden Sie unter Amazon Inspector Classic-Servicebeschränkungen.

Erstellen eines Bewertungsziels

Sie können die Amazon Inspector Classic-Konsole verwenden, um Bewertungsziele zu erstellen.

So erstellen Sie ein Bewertungsziel

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.
2. Wählen Sie im Navigationsbereich Assessment Targets und dann Create aus.
3. Geben Sie unter Name einen Namen für Ihr Bewertungsziel ein.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um alle EC2 Instances in diesem AWS Konto und dieser Region in dieses Bewertungsziel einzubeziehen, aktivieren Sie das Kontrollkästchen Alle Instances.

> **Note**
>
> Wenn Sie diese Option verwenden, gilt das Limit für die maximale Anzahl von Agenten, die Sie in einen Bewertungslauf einschließen können. Weitere Informationen finden Sie unter Amazon Inspector Classic-Servicebeschränkungen.

- Um die EC2 Instanzen auszuwählen, die Sie in dieses Bewertungsziel einbeziehen möchten, geben Sie unter Use Tags die Tag-Schlüsselnamen und Schlüssel-Wert-Paare ein.

5. (Optional) Beim Erstellen eines Ziels können Sie das Kontrollkästchen Agenten installieren aktivieren, um den Agenten auf allen EC2 Instances in diesem Ziel zu installieren. Um diese Option verwenden zu können, müssen auf Ihren EC2 Instances der SSM-Agent und eine IAM-Rolle installiert sein, die Run Command ermöglicht. Der SSM-Agent ist standardmäßig auf Amazon EC2 Windows-Instances und Amazon Linux-Instances installiert. Amazon EC2 Systems Manager benötigt eine IAM-Rolle für EC2 Instances, die Befehle verarbeiten, und eine separate Rolle für Benutzer, die Befehle ausführen. Weitere Informationen finden Sie unter Installieren und Konfigurieren eines SSM Agents und Konfigurieren von Sicherheitsrollen für System Manager.

> **Important**
>
> Wenn auf einer EC2 Instance bereits ein Agent ausgeführt wird, ersetzt die Verwendung dieser Option den Agenten, der derzeit auf der Instance ausgeführt wird, durch die neueste Agentenversion.

> **Note**
>
> Für Ihre bestehenden Bewertungsziele können Sie die Schaltfläche Agenten mit Befehl ausführen wählen, um den Agenten auf allen EC2 Instances in diesem Ziel zu installieren.

> **Note**
>
> Sie können den Agenten auch remote auf mehreren EC2 Instanzen (sowohl auf Linux- als auch auf Windows-basierten Instanzen mit demselben Befehl) installieren, indem Sie den Systems Manager Run Command verwenden. Weitere Informationen finden Sie

unter Installation des Amazon Inspector-Agenten auf mehreren EC2 Instances mithilfe des Systems Manager Run-Befehls.

6. Wählen Sie Save (Speichern) aus.

> **Note**
>
> Sie können die Schaltfläche „Zielvorschau“ auf der Seite „Bewertungsziele“ verwenden, um alle EC2 Instances zu überprüfen, die im Bewertungsziel enthalten sind. Für jede EC2 Instance können Sie den Hostnamen, die Instance-ID, die IP-Adresse und, falls zutreffend, den Status des Agenten überprüfen. Der Agentenstatus kann die folgenden Werte haben: HEALTHY, UNHEALTHY und UNKNOWN. Amazon Inspector Classic zeigt den Status UNBEKANNT an, wenn nicht festgestellt werden kann, ob auf der EC2 Instance ein Agent läuft.

Löschen eines Bewertungsziels

Zum Löschen eines Bewertungsziels gehen Sie wie folgt vor.

So löschen Sie ein Bewertungsziel

- Wählen Sie auf der Seite Assessment targets (Bewertungsziele) das zu löschende Ziel aus, und wählen Sie dann Delete (Löschen). Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja aus.

  > **Important**
  >
  > Wenn Sie ein Bewertungsziel löschen, werden alle Bewertungsvorlagen, Bewertungsläufe, Ergebnisse und Versionen der dem Ziel zugeordneten Berichte ebenfalls gelöscht.

Sie können ein Bewertungsziel auch mithilfe der `DeleteAssessmentTarget`-API löschen.

Amazon Inspector Classic: Regelpakete und Regeln

Sie können Amazon Inspector Classic verwenden, um Ihre Bewertungsziele (Sammlungen von AWS-Ressourcen) im Hinblick auf potenzielle Sicherheitsprobleme und Sicherheitslücken zu bewerten. Amazon Inspector Classic vergleicht das Verhalten und die Sicherheitskonfiguration der Bewertungsziele mit ausgewählten Sicherheitsregelpaketen. Im Kontext von Amazon Inspector Classic ist eine Regel eine Sicherheitsüberprüfung, die Amazon Inspector Classic während des Bewertungslaufs durchführt.

In Amazon Inspector Classic werden Regeln entweder nach Kategorie, Schweregrad oder Preis in unterschiedliche Regelpakete gruppiert. Dadurch haben Sie die Auswahl für die Art der Analysen, die Sie ausführen können. Amazon Inspector Classic bietet beispielsweise eine Vielzahl von Regeln, anhand derer Sie Ihre Anwendungen bewerten können. Aber vielleicht möchten Sie eine kleinere Teilmenge der verfügbaren Regeln aufnehmen, um ein bestimmtes Anliegen anzuvisieren oder spezifische Sicherheitsprobleme aufzudecken. Unternehmen mit großen IT-Abteilungen möchten vielleicht bestimmen, ob ihre Anwendung irgendwelchen Sicherheitsbedrohungen ausgesetzt ist. Andere dagegen möchten sich lieber nur auf Probleme mit dem Schweregrad Hoch konzentrieren.

Schweregrade für Regeln in Amazon Inspector Classic

Jeder Amazon Inspector Classic-Regel ist ein Schweregrad zugewiesen. Dies reduziert die Notwendigkeit, in Ihrer Analyse eine Regel einer anderen vorzuziehen. Es kann Ihnen auch dabei helfen, Ihre Antwort zu bestimmen, wenn eine Regel ein mögliches Problem hervorhebt.

Die Einstufungen Hoch, Medium und Niedrig zeigen jeweils ein Sicherheitsproblem an, das zu kompromittierter Informationsvertraulichkeit, Integrität und Verfügbarkeit innerhalb Ihres Bewertungsziels führen kann. Die Stufen unterscheiden sich danach, wie wahrscheinlich es ist, dass das Problem zu einem Kompromiss führt, und wie dringend es ist, das Problem zu beheben.

Die Kennzeichnung Informationen gibt lediglich ein Sicherheitskonfigurationsdetail Ihres Bewertungsziels an.

Je nach Schweregrad werden folgende Lösungsansätze für Probleme empfohlen:

- Hoch — Probleme mit hohem Schweregrad sind äußerst dringend. Amazon Inspector Classic empfiehlt, dieses Sicherheitsproblem als Notfall zu behandeln und sofort Abhilfe zu schaffen.
- Probleme mit mittlerem bis mittlerem Schweregrad sind etwas dringend. Amazon Inspector Classic empfiehlt, dieses Problem bei nächster Gelegenheit zu beheben, z. B. bei Ihrem nächsten Service-Update.
- Niedrig — Probleme mit geringem Schweregrad sind weniger dringend. Amazon Inspector Classic empfiehlt, dieses Problem im Rahmen eines Ihrer future Service-Updates zu beheben.
- Informativ — Diese Probleme haben rein informativen Charakter. Basierend auf Ihren Geschäfts- und Organisationszielen können Sie entweder einfach diese Informationen notieren oder sie nutzen, um die Sicherheit Ihres Bewertungsziels zu verbessern.

Regelpakete in Amazon Inspector Classic

Eine Amazon Inspector-Bewertung kann eine beliebige Kombination der folgenden Regelpakete verwenden:

Netzwerkbewertungen:

- Netzwerkerreichbarkeit

Hostbewertungen:

- Häufige Schwachstellen und Expositionen
- Center for Internet Security (CIS)-Benchmarks
- Bewährte Sicherheitsmethoden für Amazon Inspector Classic

Netzwerkerreichbarkeit

Die Regeln im Paket Network Reachability analysieren Ihre Netzwerkkonfigurationen, um Sicherheitslücken Ihrer Instances zu finden. EC2 Die Ergebnisse von Amazon Inspector dienen auch als Leitfaden bei der Einschränkung von Zugriff, der nicht sicher ist.

Das Regelpaket zur Netzwerkerreichbarkeit verwendet die neueste Technologie der Provable Security-Initiative. AWS

Die Ergebnisse dieser Regeln zeigen auf, ob Ihre Ports aus dem Internet über ein Internet-Gateway (einschließlich Instances hinter Application Load Balancern oder Classic Load Balancern), über eine VPC-Peering-Verbindung oder über ein VPN über ein virtuelles Gateway erreichbar sind. Diese Ergebnisse heben auch Netzwerkkonfigurationen hervor, die potenziell böswilligen Zugriff ermöglichen, wie z. B. schlecht verwaltete Sicherheitsgruppen, ACLs IGWs, usw.

Diese Regeln helfen dabei, die Überwachung Ihrer AWS-Netzwerke zu automatisieren und zu ermitteln, wo der Netzwerkzugriff auf Ihre EC2 Instances möglicherweise falsch konfiguriert ist. Wenn Sie dieses Paket in Ihren Bewertungslauf einbeziehen, können Sie detaillierte Netzwerksicherheitsprüfungen durchführen, ohne Scanner installieren und Pakete senden zu müssen, deren Wartung komplex und teuer ist, insbesondere für VPC-Peering-Verbindungen und. VPNs

> **Important**
>
> Ein Amazon Inspector Classic-Mitarbeiter ist nicht erforderlich, um Ihre EC2 Instances mit diesem Regelpaket zu bewerten. Ein installierter Agent kann aber Informationen zu vorhandenen Prozessen bereitstellen, mit denen Ports überwacht werden. Installieren Sie keinen Agenten auf einem Betriebssystem, das Amazon Inspector Classic nicht unterstützt. Wenn ein Agent auf einer Instance vorhanden ist, auf der ein nicht unterstütztes Betriebssystem ausgeführt wird, funktioniert das Regelpaket für die Netzwerkerreichbarkeit auf dieser Instance nicht.

Weitere Informationen finden Sie unter Amazon Inspector Classic-Regelpakete für unterstützte Betriebssysteme.

Analysierte Konfigurationen

Regeln für die Netzwerkerreichbarkeit analysieren die Konfiguration der folgenden Entitäten auf Schwachstellen:

- EC2 Amazon-Instanzen
- Application Load Balancer
- Direct Connect
- Elastic Load Balancers
- Elastic-Network-Schnittstellen

- Internet-Gateways () IGWs
- Listen zur Netzwerkzugriffskontrolle () ACLs
- Routing-Tabellen
- Sicherheitsgruppen (SGs)
- Subnets
- Virtuelle private Clouds (VPCs)
- Virtuelle private Gateways () VGWs
- VPC-Peering-Verbindungen

Erreichbarkeitsrouten

Regeln für die Netzwerkerreichbarkeit prüfen auf die folgenden Erreichbarkeitsrouten, die mögliche Wege für den Zugriff auf Ports von außerhalb Ihrer VPC darstellen:

- **`Internet`**: Internet-Gateways (einschließlich Application Load Balancern und Classic Load Balancern)
- **`PeeredVPC`** – VPC-Peering-Verbindungen
- **`VGW`**: Virtuelle private Gateways

Ergebnistypen

Eine Bewertung mit dem Regelpaket zur Netzwerkerreichbarkeit kann die folgenden Arten von Ergebnissen für jede einzelne Erreichbarkeitsroute zurückgeben:

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

`RecognizedPort`

Ein Port, der gewöhnlich für einen bekannten Service verwendet wird, ist erreichbar. Wenn ein Agent auf der EC2 Zielinstanz vorhanden ist, gibt das generierte Ergebnis auch an, ob auf dem Port ein aktiver Abhörprozess stattfindet. Ergebnissen dieser Art wird je nach den Auswirkungen auf die Sicherheit des bekannten Service ein Schweregrad zugewiesen:

- **`RecognizedPortWithListener`**— Ein erkannter Port ist über eine bestimmte Netzwerkkomponente extern vom öffentlichen Internet aus erreichbar, und ein Prozess überwacht den Port.
- **`RecognizedPortNoListener`**— Ein Port ist vom öffentlichen Internet aus über eine bestimmte Netzwerkkomponente extern erreichbar, und es gibt keine Prozesse, die den Port abhören.
- **`RecognizedPortNoAgent`**— Ein Port ist vom öffentlichen Internet aus über eine bestimmte Netzwerkkomponente extern erreichbar. Um erkennen zu können, ob ein den Port überwachender Prozess vorhanden ist, muss zuerst ein Agent auf der Ziel-Instance installiert werden.

Die folgende Tabelle zeigt eine Liste erkannter Ports:

Service	TCP-Ports	UDP-Ports
SMB	445	445
NetBIOS	137, 139	137, 138
LDAP	389	389
LDAP über TLS	636	
Global Catalog LDAP	3268	
Global Catalog LDAP über TLS	3269	
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752
RPC	111, 135, 530	111, 135, 530
WINS	1512, 42	1512, 42
DHCP	67, 68, 546, 547	67, 68, 546, 547
Syslog	601	514

Service	TCP-Ports	UDP-Ports
Druckdienste	515	
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017, 27018, 27019, 28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521, 1630	
Elasticsearch	9300, 9200	
HTTP	80	80
HTTPS	443	443

`UnrecogizedPortWithListener`

Ein Port, der nicht in der vorangegangenen Tabelle aufgelistet wird, ist erreichbar und auf ihm ist ein Überwachungsprozess aktiv. Da Ergebnisse dieser Art Informationen über Listening-Prozesse enthalten, können sie nur generiert werden, wenn ein Amazon Inspector-Agent auf der EC2 Ziel-Instance installiert ist. Ergebnisse diese Art erhalten den Schweregrad Low (Niedrig).

`NetworkExposure`

Ergebnisse dieses Typs zeigen zusammengefasste Informationen zu den Ports, die auf Ihrer EC2 Instance erreichbar sind. Für jede Kombination von Elastic Network-Schnittstellen und

Sicherheitsgruppen auf einer EC2 Instance zeigen diese Ergebnisse den erreichbaren Satz von TCP- und UDP-Portbereichen. Ergebnisse dieser Art haben den Schweregrad Informational (Zur Information).

Häufige Schwachstellen und Expositionen

Mithilfe der Regeln in diesem Paket können Sie überprüfen, ob die EC2 Instanzen in Ihren Bewertungszielen häufigen Sicherheitslücken und Risiken ausgesetzt sind (CVEs). Angriffe können ungepatchte Sicherheitslücken ausnutzen, um die Vertraulichkeit, Integrität oder Verfügbarkeit Ihrer Dienste oder Daten zu beeinträchtigen. Das CVE-System stellt eine Referenzmethode für öffentlich gemeldete Sicherheitslücken und -risiken bereit. Weitere Informationen finden Sie unter https://cve.mitre.org/.

Wenn ein bestimmter CVE in einem Ergebnis vorkommt, das durch eine Amazon Inspector Classic-Bewertung ermittelt wurde, können Sie unter https://cve.mitre.org/ nach der ID des CVE suchen (z. B.**`CVE-2009-0021`**). Die Suchergebnisse können detaillierte Informationen über dieses CVE bereitstellen, dem Schweregrad, und wie man es minimiert.

Für das Regelpaket Common Vulnerabilities & Exploits (CVE) hat Amazon Inspector die bereitgestellten CVSS Base Scoring- und ALAS-Schweregrade zugeordnet:

Amazon Inspector Schweregrad	CVSS-Basiswert	ALAS-Schweregrad (falls CVSS nicht bewertet wurde)
Hoch	>= 5	Kritisch oder wichtig
Mittelschwer	< 5 and >Kritisch oder wichtig ----sep----= 2.1	Mittelschwer
Niedrig	< 2.1 and >= 2,1 ----Sep----= 0,8	Niedrig
Informativ	< 0,8	N/A

Anhand der in diesem Paket enthaltenen Regeln können Sie beurteilen, ob Ihre EC2 Instances CVEs den folgenden regionalen Listen ausgesetzt sind:

- USA Ost (Nord-Virginia)

- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- EU (Irland)
- EU (Frankfurt)
- EU (London)
- EU (Stockholm)
- Asien-Pazifik (Tokio)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Sydney)
- AWS GovCloud West (USA)
- AWS GovCloud East (USA)

Das CVE-Regelpaket wird regelmäßig aktualisiert. Diese Liste enthält die Regeln CVEs , die in Bewertungsläufen enthalten sind, die gleichzeitig mit dem Abrufen dieser Liste durchgeführt werden.

Weitere Informationen finden Sie unter Amazon Inspector Classic-Regelpakete für unterstützte Betriebssysteme.

Center for Internet Security (CIS)-Benchmarks

Das CIS Security Benchmarks-Programm bietet klar definierte, unvoreingenommene und konsensbasierte Best Practices in der Branche, um Unternehmen bei der Bewertung und Verbesserung ihrer Sicherheit zu unterstützen. AWS ist ein Mitgliedsunternehmen von CIS Security Benchmarks. Eine Liste der Amazon Inspector Classic-Zertifizierungen finden Sie auf der Seite Amazon Web Services auf der CIS-Website.

Amazon Inspector Classic bietet derzeit die folgenden CIS-zertifizierten Regelpakete, mit denen Sie sichere Konfigurationen für die folgenden Betriebssysteme einrichten können:

Amazon Linux

- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1`
- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2`

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

CentOS Linux

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

Red Hat Enterprise Linux

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

Ubuntu

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

Windows

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

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

Wenn ein bestimmter CIS-Benchmark in einem Ergebnis vorkommt, das im Rahmen eines Amazon Inspector Classic-Bewertungslaufs ermittelt wurde, können Sie eine ausführliche PDF-Beschreibung des Benchmarks von https://benchmarks.cisecurity.org/ herunterladen (kostenlose Registrierung erforderlich). Das Benchmark-Dokument enthält detaillierte Informationen zu diesem CIS-Benchmark, seinem Schweregrad und seiner Vermeidung.

Weitere Informationen finden Sie unter Amazon Inspector Classic-Regelpakete für unterstützte Betriebssysteme.

Bewährte Sicherheitsmethoden für Amazon Inspector Classic

Verwenden Sie die Amazon Inspector Classic-Regeln, um festzustellen, ob Ihre Systeme sicher konfiguriert sind.

> **Important**
>
> Derzeit können Sie EC2 Instances, auf denen entweder Linux- oder Windows-basierte Betriebssysteme ausgeführt werden, in Ihre Bewertungsziele einbeziehen.
> Während eines Bewertungslaufs generieren die in diesem Abschnitt beschriebenen Regeln nur Ergebnisse für die EC2 Instances, auf denen Linux-basierte Betriebssysteme ausgeführt werden. Die Regeln generieren keine Ergebnisse für EC2 Instances, auf denen Windows-basierte Betriebssysteme ausgeführt werden.
> Weitere Informationen finden Sie unter Amazon Inspector Classic-Regelpakete für unterstützte Betriebssysteme.

Themen

Deaktivieren der Root-Anmeldung über SSH

Anhand dieser Regel können Sie feststellen, ob der SSH-Daemon so konfiguriert ist, dass Sie sich als Root-Benutzer bei Ihrer EC2 Instanz anmelden können.

Schweregrad

Mittel

Erkenntnis

In Ihrem Bewertungsziel gibt es eine EC2 Instanz, die so konfiguriert ist, dass sich Benutzer mit Root-Anmeldeinformationen über SSH anmelden können. Dies erhöht die Wahrscheinlichkeit eines erfolgreichen Brute-Force-Angriffs.

Resolution (Auflösung)

Wir empfehlen Ihnen, Ihre EC2 Instance so zu konfigurieren, dass Root-Kontoanmeldungen über SSH verhindert werden. Melden Sie sich stattdessen als Nicht-Root-Benutzer an und verwenden Sie `sudo`, um gegebenenfalls Berechtigungen auszuweiten. Um Anmeldungen am SSH-Root-Konto zu deaktivieren, stellen Sie `PermitRootLogin` in der Datei `/etc/ssh/sshd_config` auf `no` ein und starten Sie dann `sshd` neu.

Nur SSH-Version 2 unterstützen

Anhand dieser Regel können Sie feststellen, ob Ihre EC2 Instances so konfiguriert sind, dass sie das SSH-Protokoll Version 1 unterstützen.

Schweregrad

Mittel

Erkenntnis

Eine EC2 Instance in Ihrem Bewertungsziel ist so konfiguriert, dass sie SSH-1 unterstützt, das inhärente Designfehler enthält, die die Sicherheit erheblich beeinträchtigen.

Resolution (Auflösung)

Wir empfehlen, dass Sie EC2 Instances in Ihrem Bewertungsziel so konfigurieren, dass sie nur SSH-2 und höher unterstützen. Für OpenSSH können Sie dies erreichen, indem Sie `Protocol 2` in der `/etc/ssh/sshd_config`-Datei festlegen. Weitere Informationen finden Sie unter `man sshd_config`.

Deaktivieren der Passwortauthentifizierung über SSH

Anhand dieser Regel können Sie feststellen, ob Ihre EC2 Instances so konfiguriert sind, dass sie die Passwortauthentifizierung über das SSH-Protokoll unterstützen.

Schweregrad

Mittel

Erkenntnis

Eine EC2 Instance in Ihrem Bewertungsziel ist so konfiguriert, dass sie die Passwortauthentifizierung über SSH unterstützt. Die Passwortauthentifizierung ist anfällig für

Brute-Force-Angriffe und sollte nach Möglichkeit für eine schlüsselbasierte Authentifizierung deaktiviert werden.

Resolution (Auflösung)

Wir empfehlen, dass Sie die Passwortauthentifizierung über SSH auf Ihren EC2 Instances deaktivieren und stattdessen die Unterstützung für die schlüsselbasierte Authentifizierung aktivieren. Dies reduziert die Wahrscheinlichkeit eines erfolgreichen Brute-Force-Angriffs erheblich. Weitere Informationen finden Sie unter 1233/. https://aws.amazon.com/articles/ Wenn die Passwortauthentifizierung unterstützt wird, ist es wichtig, den Zugriff auf den SSH-Server auf vertrauenswürdige IP-Adressen zu beschränken.

Konfigurieren des maximalen Passwortalters

Diese Regel hilft zu bestimmen, ob das Höchstalter für Passwörter auf Ihren EC2 Instanzen konfiguriert ist.

Schweregrad

Mittel

Erkenntnis

Eine EC2 Instanz in Ihrem Bewertungsziel ist nicht für ein Höchstalter für Passwörter konfiguriert.

Resolution (Auflösung)

Wenn Sie Passwörter verwenden, empfehlen wir Ihnen, ein Höchstalter für Passwörter für alle EC2 Instances in Ihrem Bewertungsziel festzulegen. Dies erfordert, dass Benutzer regelmäßig ihre Passwörter ändern und die Chancen auf einen erfolgreichen Passwort-Rate-Angriff reduzieren. Um dieses Problem für bestehende Benutzer zu beheben, verwenden Sie den chage-Befehl. Um ein maximales Alter für Passwörter für alle zukünftigen Benutzer zu konfigurieren, bearbeiten Sie das Feld `PASS_MAX_DAYS` in der Datei `/etc/login.defs`.

Konfigurieren der Passwortmindestlänge

Anhand dieser Regel können Sie feststellen, ob für Ihre EC2 Instances eine Mindestlänge für Passwörter konfiguriert ist.

Schweregrad

Mittel

Erkenntnis

Eine EC2 Instanz in Ihrem Bewertungsziel ist nicht für eine Mindestlänge für Passwörter konfiguriert.

Resolution (Auflösung)

Wenn Sie Passwörter verwenden, empfehlen wir Ihnen, eine Mindestlänge für Passwörter für alle EC2 Instanzen in Ihrem Bewertungsziel zu konfigurieren. Durch die Erzwingung einer minimalen Passwort-Länge verringert sich das Risiko eines erfolgreichen Passwort-Rate-Angriffs. Sie können dies tun, indem Sie die folgende Option in der `pwquality.conf` Datei verwenden:`minlen`. Weitere Informationen finden Sie unter https://linux.die. net/man/5/pwquality.conf.

Wenn auf Ihrer Instance nicht verfügbar `pwquality.conf` ist, können Sie die `minlen` Option mithilfe des `pam_cracklib.so` Moduls festlegen. Weitere Informationen finden Sie unter `man pam_cracklib`.

Die `minlen` Option sollte auf 14 oder höher gesetzt sein.

Konfigurieren der Passwortkomplexität

Mithilfe dieser Regel können Sie feststellen, ob auf Ihren EC2 Instances ein Mechanismus zur Kennwortkomplexität konfiguriert ist.

Schweregrad

Mittel

Erkenntnis

Für EC2 Instances in Ihrem Bewertungsziel sind keine Mechanismen oder Einschränkungen zur Kennwortkomplexität konfiguriert. Dies ermöglicht es Benutzern, einfache Passwörter festzulegen, wodurch die Chancen erhöht werden, dass nicht autorisierte Benutzer Zugang erhalten und Konten missbrauchen.

Resolution (Auflösung)

Wenn Sie Passwörter verwenden, empfehlen wir Ihnen, alle EC2 Instanzen in Ihrem Bewertungsziel so zu konfigurieren, dass ein gewisses Maß an Passwortkomplexität erforderlich

ist. Sie können dies mit den folgenden Optionen in der Datei `pwquality.conf` durchführen: `lcredit`, `ucredit`, `dcredit` und `ocredit`. Weitere Informationen finden Sie unter https://linux.die. net/man/5/pwquality.conf.

Wenn `pwquality.conf` auf Ihrer Instance nicht verfügbar ist, können Sie die Optionen `lcredit`, `ucredit`, `dcredit` und `ocredit` mithilfe des `pam_cracklib.so`-Moduls festlegen. Weitere Informationen finden Sie unter `man pam_cracklib`.

Der erwartete Wert für jede dieser Optionen ist kleiner oder gleich -1, wie unten dargestellt:

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

Darüber hinaus muss die Option `remember` auf 12 oder höher eingestellt sein. Weitere Informationen finden Sie unter `man pam_unix`.

Aktivieren von ASLR

Anhand dieser Regel können Sie feststellen, ob die Randomisierung des Adressraum-Layouts (ASLR) auf den Betriebssystemen der EC2 Instances in Ihrem Bewertungsziel aktiviert ist.

Schweregrad

Mittel

Erkenntnis

Für eine EC2 Instance in Ihrem Bewertungsziel ist ASLR nicht aktiviert.

Resolution (Auflösung)

Um die Sicherheit Ihres Bewertungsziels zu erhöhen, empfehlen wir Ihnen, ASLR auf den Betriebssystemen aller EC2 Instances in Ihrem Ziel zu aktivieren, indem Sie Folgendes ausführen. echo 2 | sudo tee /proc/sys/kernel/randomize_va_space

DEP aktivieren

Anhand dieser Regel können Sie feststellen, ob Data Execution Prevention (DEP) auf den Betriebssystemen der EC2 Instances in Ihrem Bewertungsziel aktiviert ist.

> **Note**
>
> Diese Regel wird für EC2 Instances mit ARM-Prozessoren nicht unterstützt.

Schweregrad

Mittel

Erkenntnis

Für eine EC2 Instance in Ihrem Bewertungsziel ist DEP nicht aktiviert.

Resolution (Auflösung)

Wir empfehlen, DEP auf den Betriebssystemen aller EC2 Instances in Ihrem Bewertungsziel zu aktivieren. Die Aktivierung von DEP schützt Ihre Instances vor Sicherheitskompromissen mit Pufferüberlauftechniken.

Konfigurieren von Berechtigungen für Systemverzeichnisse

Diese Regelung überprüft Berechtigungen für Systemverzeichnisse, die Binärdateien und Systemkonfigurationsinformationen enthalten. Sie prüft, dass nur der Root-Benutzer (ein Benutzer, der sich mithilfe von Root-Konto-Anmeldeinformationen anmeldet) Schreibberechtigungen für diese Verzeichnisse erhält.

Schweregrad

Hoch

Erkenntnis

Eine EC2 Instance in Ihrem Bewertungsziel enthält ein Systemverzeichnis, das für Benutzer ohne Root-Rechte schreibbar ist.

Resolution (Auflösung)

Um die Sicherheit Ihres Bewertungsziels zu erhöhen und die Eskalation von Rechten durch böswillige lokale Benutzer zu verhindern, konfigurieren Sie alle Systemverzeichnisse auf allen EC2 Instances in Ihrem Ziel so, dass nur von Benutzern geschrieben werden kann, die sich mit Root-Kontoanmeldedaten anmelden.

Amazon Inspector Classic Bewertungsvorlagen und Bewertungsläufe

Amazon Inspector Classic hilft Ihnen dabei, potenzielle Sicherheitsprobleme zu erkennen, indem es Sicherheitsregeln verwendet, um Ihre AWS Ressourcen zu analysieren. Amazon Inspector Classic überwacht und sammelt Verhaltensdaten (Telemetrie) über Ihre Ressourcen. Die Daten umfassen Informationen über die Verwendung sicherer Kanäle, den Netzwerkverkehr zwischen laufenden Prozessen und Details zur Kommunikation mit AWS Diensten. Als Nächstes analysiert Amazon Inspector Classic die Daten und vergleicht sie mit einer Reihe von Sicherheitsregelpaketen. Schließlich erstellt Amazon Inspector Classic eine Liste mit Ergebnissen, die potenzielle Sicherheitsprobleme mit unterschiedlichem Schweregrad identifizieren.

Zu Beginn erstellen Sie ein Bewertungsziel (eine Sammlung der AWS Ressourcen, die Amazon Inspector Classic analysieren soll). Als Nächstes erstellen Sie eine Bewertungsvorlage (eine Blaupause für das Konfigurieren von Bewertungen). Sie verwenden die Vorlage zum Starten eines Bewertungslaufs, des Überwachungs- und Analyseprozesses, der in einem Satz Ergebnisse resultiert.

Themen

Amazon Inspector Classic — Bewertungsvorlagen

Mit einer Bewertungsvorlage können Sie eine Konfiguration für Ihre Bewertungsläufe angeben, einschließlich:

- Regelpakete, die Amazon Inspector Classic zur Bewertung Ihres Bewertungsziels verwendet

- Dauer des Bewertungslaufs — Sie können die Dauer eines Bewertungslaufs zwischen 3 Minuten und 24 Stunden festlegen. Wir empfehlen, die Dauer der Bewertungsläufe auf 1 Stunde festzulegen.
- Amazon SNS SNS-Themen, an die Amazon Inspector Classic Benachrichtigungen über den Status und die Ergebnisse Ihres Bewertungslaufs sendet
- Amazon Inspector Classic — Attribute (Schlüssel-Wert-Paare), die Sie durch einen Bewertungslauf mit dieser Bewertungsvorlage erzeugten Befund zuordnen können

Nachdem Amazon Inspector Classic die Bewertungsvorlage erstellt hat, können Sie sie wie jede andere AWS Ressource taggen. Weitere Informationen hierzu finden Sie unter Tag-Editor. Durch das Markieren von Bewertungsvorlagen können Sie sie organisieren und erhalten einen besseren Überblick über Ihre Sicherheitsstrategie. Amazon Inspector Classic bietet beispielsweise eine Vielzahl von Regeln, anhand derer Sie Ihre Bewertungsziele bewerten können. Evtl. möchten Sie jedoch verschiedene Subsets der verfügbaren Regeln in Ihre Bewertungsvorlagen einschließen, um auf spezielle Problembereiche abzuzielen oder spezielle Sicherheitsprobleme aufzudecken. Durch das Markieren von Bewertungsvorlagen können Sie sie jederzeit schnell gemäß Ihrer Sicherheitsstrategie und Ihren Sicherheitszielen lokalisieren und ausführen.

> **Important**
>
> Nach der Erstellung einer Bewertungsvorlage können Sie sie nicht ändern.

Amazon Inspector Classic — Einschränkungen bei Bewertungsvorlagen

Sie sind in der Lage, pro AWS Konto bis zu 500 Bewertungsvorlagen zu erstellen.

Weitere Informationen finden Sie unter Amazon Inspector Classic-Servicebeschränkungen.

Erstellen einer Bewertungsvorlage

So erstellen Sie eine Bewertungsvorlage

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

2. Wählen Sie im Navigationsbereich die Option Assessment Templates (Bewertungsvorlagen) und danach Create (Erstellen).
3. Geben Sie unter Name den Namen für Ihre Bewertungsvorlage ein.
4. Wählen Sie für Target name ein Bewertungsziel zum Analysieren aus.

> **Note**
>
> Wenn Sie eine Bewertungsvorlage erstellen, können Sie auf der Seite mit den Bewertungsvorlagen die Schaltfläche „Zielvorschau“ verwenden, um alle im Bewertungsziel enthaltenen EC2 Instanzen zu überprüfen. Für jede EC2 Instanz können Sie den Hostnamen, die Instanz-ID, die IP-Adresse und gegebenenfalls den Status des Agenten überprüfen. Der Agentenstatus kann die folgenden Werte haben: HEALTHY, UNHEALTHY und UNKNOWN. Amazon Inspector Classic zeigt den Status UNBEKANNT an, wenn nicht festgestellt werden kann, ob auf der EC2 Instance ein Agent läuft.
> Sie können auch die Schaltfläche „Zielvorschau“ auf der Seite „Bewertungsvorlagen“ verwenden, um EC2 Instances zu überprüfen, die zu den in Ihren zuvor erstellten Vorlagen enthaltenen Bewertungsziele gehören.

5. Wählen Sie für Rules packages mindestens ein Regelpaket aus, das in die Bewertungsvorlage aufgenommen werden soll.
6. Geben Sie unter Duration die Dauer für Ihre Bewertungsvorlage an.
7. (Optional) Geben Sie für SNS-Themen ein SNS-Thema an, an das Amazon Inspector Classic Benachrichtigungen über Status und Ergebnisse des Bewertungslaufs senden soll. Amazon Inspector Classic kann SNS-Benachrichtigungen über die folgenden Ereignisse senden:

   - Bewertungslauf hat begonnen
   - Bewertungslauf wurde beendet
   - Zustand eines Bewertungslaufs hat sich geändert
   - Ergebnis wurde generiert

   Weitere Informationen zum Einrichten eines SNS-Themas finden Sie unter Einrichten eines SNS-Themas für Amazon Inspector Classic.
8. (Optional) Geben Sie unter Tag Werte für Key (Schlüssel) und Value (Wert) ein. Sie können mehrere Tags zur Bewertungsvorlage hinzufügen.

9. (Optional) Geben Sie für Attribute, die zu Ergebnissen hinzugefügt wurden, Werte für Schlüssel und Wert ein. Amazon Inspector Classic wendet die Attribute auf alle durch die Bewertungsvorlage erzeugten Befund an. Sie können mehrere Attribute zur Bewertungsvorlage hinzufügen. Weitere Informationen zu Ergebnissen und Markierungsergebnissen finden Sie unter Ergebnisse von Amazon Inspector Classic.
10. (Optional) Um mithilfe dieser Vorlage einen Zeitplan für Ihre Bewertungsläufe aufzustellen, aktivieren Sie das Kontrollkästchen Set up recurring assessment runs once every <number_of_days>, starting now (Wiederkehrende Bewertungsläufe ab jetzt einmal alle <Anzahl_von_Tagen> einrichten) und geben Sie das Wiederholungsmuster (Anzahl von Tagen) mit den Pfeiltasten an.

> **Note**
>
> Wenn Sie dieses Kontrollkästchen verwenden, erstellt Amazon Inspector Classic automatisch eine Amazon CloudWatch Events-Regel für den Zeitplan für Bewertungsläufe, den Sie einrichten. Amazon Inspector Classic erstellt dann auch automatisch eine IAM-Rolle mit dem Namen`AWS_InspectorEvents_Invoke_Assessment_Template`. Diese Rolle ermöglicht CloudWatch Events, API-Aufrufe für die Amazon Inspector Classic-Ressourcen durchzuführen. Weitere Informationen finden Sie unter Was ist Amazon CloudWatch Events? und Verwendung ressourcenbasierter Richtlinien für CloudWatch Ereignisse.

> **Note**
>
> Sie können automatische Bewertungsläufe auch über eine AWS Lambda -Funktion einrichten. Weitere Informationen finden Sie unter Die Einrichtung der automatischen Bewertung läuft über eine Lambda-Funktion.

11. Wählen Sie Create and run oder Create aus.

Löschen einer Bewertungsvorlage

Zum Löschen einer Bewertungsvorlage gehen Sie wie folgt vor.

So löschen Sie eine Bewertungsvorlage

- Wählen Sie auf der Seite Assessment Templates (Bewertungsvorlagen) die zu löschende Vorlage aus und wählen Sie dann Delete (Löschen). Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja aus.

> **Important**
>
> Wenn Sie eine Bewertungsvorlage löschen, werden alle Bewertungsläufe, Ergebnisse und Versionen der dieser Vorlage zugeordneten Berichte ebenfalls gelöscht.

Sie können eine Bewertungsvorlage auch mithilfe der `DeleteAssessmentTemplate`-API löschen.

Bewertungsläufe

Nach dem Erstellen einer Bewertungsvorlage können Sie mit ihr Bewertungsläufe starten. Sie können mehrere Läufe mit derselben Vorlage starten, solange Sie das Durchlauflimit für jedes AWS Konto einhalten. Weitere Informationen finden Sie unter Amazon Inspector Classic — Einschränkungen .

Wenn Sie die Amazon Inspector Classic-Konsole verwenden, müssen Sie die erste Ausführung Ihrer neuen Bewertungsvorlage auf der Seite Bewertungsvorlagen starten. Nach dem Starten des Laufs können Sie auf der Seite Assessment runs den Fortschritt des Laufs überwachen. Verwenden Sie die Schaltflächen Run, Cancel und Delete für die jeweiligen Vorgänge. Sie können auch die Laufdetails anzuzeigen, u. a. den ARN des Laufs, die für den Lauf ausgewählten Regelpakete, die Tags und Attribute, die auf den Lauf angewendet werden, und vieles mehr.

Für nachfolgende Läufe der Bewertungsvorlage können Sie auf der Seite Assessment templates oder Assessment runs die Schaltflächen Run, Cancel und Delete verwenden.

Löschen eines Bewertungslaufs

Zum Löschen eines Bewertungslaufs gehen Sie wie folgt vor.

So löschen Sie einen Lauf

- Wählen Sie auf der Seite Assessment runs (Bewertungsläufe) den zu löschenden Lauf aus, und wählen Sie dann Delete (Löschen). Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja aus.

> **Important**
>
> Wenn Sie einen Lauf löschen, werden alle Ergebnisse und alle Versionen des Berichts von diesem Lauf ebenfalls gelöscht.

Sie können einen Lauf auch mithilfe der `DeleteAssessmentRun`-API löschen.

Amazon Inspector Classic — Einschränkungen

Sie sind in der Lage, pro AWS Konto bis zu 50.000 Bewertungsläufe zu erstellen.

Sie können mehrere Testläufe gleichzeitig ausführen, sofern die für die Testläufe verwendeten Ziele keine sich überschneidenden EC2 Instanzen enthalten.

Weitere Informationen finden Sie unter Amazon Inspector Classic-Servicebeschränkungen.

Die Einrichtung der automatischen Bewertung läuft über eine Lambda-Funktion

Wenn Sie einen wiederkehrenden Zeitplan für Ihre Bewertung einrichten möchten, können Sie Ihre Bewertungsvorlage so konfigurieren, dass sie automatisch ausgeführt wird, indem Sie in der AWS Lambda Konsole eine Lambda-Funktion erstellen. Weitere Informationen erhalten Sie unter Lambda-Funktionen.

Zum Einrichten von automatischen Bewertungsläufen unter Verwendung der AWS Lambda Konsole führen Sie die folgenden Schritte aus.

So richten Sie automatische Läufe über eine Lambda-Funktion ein

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Lambda - Konsole.
2. Wählen Sie im Navigationsbereich entweder Dashboard oder Funktionen und dann Lambda-Funktion erstellen aus.
3. Wählen Sie auf der Seite Create function (Funktion erstellen) die Option Browse serverless app repository (Serverloses App-Repository durchsuchen) aus. Geben Sie dann **`inspector`** in das Suchfeld ein.

4. Wählen Sie den Plan inspector-scheduled-run aus.
5. Richten Sie auf der Seite Überprüfen, konfigurieren und bereitstellen einen wiederkehrenden Zeitplan für automatisierte Läufe ein, indem Sie ein CloudWatch Ereignis angeben, das Ihre Funktion auslöst. Geben Sie dazu einen Namen und eine Beschreibung für die Regel ein und wählen Sie dann einen Zeitplanausdruck. Der Zeitplanausdruck legt fest, wie oft der Lauf erfolgt, z. B. alle 15 Minuten oder einmal täglich. Weitere Informationen zu CloudWatch Veranstaltungen und Konzepten finden Sie unter Was ist Amazon CloudWatch Events?

   Wenn Sie das Kontrollkästchen Enable trigger (Auslöser aktivieren) aktivieren, startet der Lauf, sobald die Erstellung Ihrer Funktion abgeschlossen wurde. Nachfolgende automatische Läufe folgen dem Wiederholungsmuster, das Sie im Feld Schedule expression (Zeitplanausdruck) angeben. Wenn Sie das Kontrollkästchen Enable trigger während der Erstellung der Funktion nicht aktivieren, können Sie die Funktion später bearbeiten, um diesen Auslöser zu aktivieren.
6. Geben Sie auf der Seite Configure function Folgendes ein:

   - Geben Sie unter Name einen Namen für die Funktion ein.
   - (Optional) Geben Sie unter Description (Beschreibung) eine Beschreibung zur späteren Identifizierung Ihrer Funktion ein.
   - Behalten Sie zur Laufzeit den Standardwert von bei**`Node.js 8.10`**. AWS Lambda unterstützt den inspector-scheduled-runBlueprint nur für die **`Node.js 8.10`** Laufzeit.
   - Bewertungsvorlage, die Sie automatisch unter Verwendung dieser Funktion ausführen möchten. Geben Sie dazu den Wert der Umgebungsvariable assessmentTemplateArn an.
   - Behalten Sie für den Handler den Standardwert **`index.handler`** bei.
   - Legen Sie Berechtigungen für Ihre Funktion mithilfe des Felds Role fest. Weitere Informationen finden Sie unter AWS Lambda -Berechtigungsmodell.

     Um diese Funktion auszuführen, benötigen Sie eine IAM-Rolle, die es ermöglicht, die Läufe AWS Lambda zu starten und Protokollmeldungen über die Läufe, einschließlich aller Fehler, in Amazon CloudWatch Logs zu schreiben. AWS Lambda übernimmt diese Rolle für jeden wiederkehrenden automatisierten Lauf. Sie können beispielsweise die folgende Musterrichtlinie an diese IAM-Rolle anfügen:

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

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

7. Prüfen Sie Ihre Auswahl und klicken Sie dann auf Create function.

Einrichten eines SNS-Themas für Amazon Inspector Classic

Amazon Simple Notification Service (Amazon SNS) ist ein Web-Service, der Nachrichten an Abonnenten (Endpunkte oder Clients) sendet. Sie können Amazon SNS verwenden, um Benachrichtigungen für Amazon Inspector Classic einzurichten.

So richten Sie ein SNS-Thema für Benachrichtigungen ein

1. Erstellen Sie ein SNS-Thema. Weitere Informationen finden Sie unter Tutorial: Erstellen eines Amazon SNS-Themas. Wenn Sie das Thema erstellt haben, erweitern Sie den Abschnitt Zugriffsrichtlinie. Führen Sie anschließend die folgenden Schritte aus, um die Prüfung zum Senden von Nachrichten an das Thema zu erlauben:

   a. Wählen Sie unter Choose method (Methode auswählen) Basic (Grundlegend) aus.

   b. Wählen Sie unter Definieren, wer Nachrichten zu dem Thema veröffentlichen kann die Option Nur die angegebenen AWS Konten aus, und geben Sie dann den ARN für das Konto in der Region ein, in der Sie das Thema erstellen:

      - `US East (Ohio)` - arn:aws:iam::646659390643:root
      - `US East (N. Virginia)`- arn:aws:iam::316112463485:root
      - `US West (N. California)` - arn:aws:iam::166987590008:root
      - `US West (Oregon)` - arn:aws:iam::758058086616:root
      - `Asia Pacific (Mumbai)` - arn:aws:iam::162588757376:root
      - `Asia Pacific (Seoul)` - arn:aws:iam::526946625049:root
      - `Asia Pacific (Sydney)` - arn:aws:iam::454640832652:root

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

c. Wählen Sie unter Definieren, wer dieses Thema abonnieren kann die Option Nur die angegebenen AWS Konten aus, und geben Sie dann den ARN für das Konto in der Region ein, in der Sie das Thema erstellen.

d. Gehen Sie wie folgt vor, um sich davor zu schützen, dass Inspector als verwirrter Stellvertreter eingesetzt wird, wie unter Problem mit verwirrtem Stellvertreter im IAM-Benutzerhandbuch beschrieben:

i. Wählen Sie Erweitert aus. Dadurch gelangen Sie zum JSON-Editor.

ii. Fügen Sie die folgende Bedingung hinzu:

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

e. (Optional) Weitere Informationen zu aws: SourceAccount und aws: SourceArn finden Sie unter Global condition context keys im IAM-Benutzerhandbuch.

f. Aktualisieren Sie andere Einstellungen für das Thema nach Bedarf, und wählen Sie dann Create topic (Thema erstellen).

2. (Optional) Informationen zum Erstellen eines verschlüsselten SNS-Themas finden Sie unter Verschlüsselung im Ruhezustand im SNS-Entwicklerhandbuch.

3. Gehen Sie wie folgt vor, um sich davor zu schützen, dass Inspector als verwirrter Stellvertreter für Ihren KMS-Schlüssel verwendet wird:

a. Gehen Sie in der KMS-Konsole zu Ihrem CMK.

b. Wählen Sie Bearbeiten aus.

c. Fügen Sie die folgende Bedingung hinzu:

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

4. Erstellen Sie ein Abonnement für das Thema, das Sie erstellt haben. Weitere Informationen finden Sie unter Tutorial: Abonnieren eines Endpunkts für ein Amazon SNS-Thema.
5. Um zu bestätigen, dass das Abonnement ordnungsgemäß konfiguriert ist, veröffentlichen Sie eine Nachricht an das Thema. Weitere Informationen finden Sie unter Tutorial: Veröffentlichen einer Nachricht an ein Amazon SNS-Thema.

Ergebnisse von Amazon Inspector Classic

Bei den Ergebnissen handelt es sich um potenzielle Sicherheitsprobleme, die Amazon Inspector Classic bei einer Bewertung Ihres Bewertungsziels entdeckt. Die Ergebnisse werden auf der Amazon Inspector Classic-Konsole oder über die API angezeigt. Ergebnisse enthalten detaillierte Beschreibungen der Sicherheitsprobleme und Empfehlungen für die Lösung dieser Probleme.

Nachdem Amazon Inspector die Ergebnisse generiert hat, können Sie sie verfolgen, indem Sie ihnen Amazon Inspector Classic-Attribute zuweisen. Diese Attribute bestehen aus Schlüssel-Wert-Paaren.

Das Verfolgen Ihrer Ergebnisse mit Attributen kann zum Verwalten des Workflows Ihrer Sicherheitsstrategie nützlich sein. Nachdem Sie beispielsweise eine Bewertung erstellt und ausgeführt haben, generiert sie eine Liste von Ergebnissen mit unterschiedlichen Einstufungen für Schweregrad, Dringlichkeit und Interesse für Sie, basierend auf Ihren Sicherheitszielen und Ihrer Vorgehensweise. Wenn Sie wollen, können Sie den Empfehlungsschritten eines Ergebnisses folgen, um ein potenziell dringendes Sicherheitsproblem zu lösen. Sie könnten auch eine weitere Behebung eines Ergebnisses bis zu Ihrem nächsten anstehenden Service-Update verschieben. Wenn Sie beispielsweise ein Ergebnis sofort beheben möchten, können Sie für das Ergebnis ein Attribut mit einem Schlüssel-Wert-Paar **`Status`** / **`Urgent`** erstellen und zuordnen. Sie können auch Attribute verwenden, um die Arbeitslast der Lösung von potenziellen Sicherheitsproblemen zu verteilen. Wenn Sie beispielsweise Bob (ein Sicherheits-Ingenieur in Ihrem Team) die Aufgabe erteilen, eine Lösung für ein Ergebnis zu finden, können Sie einem Ergebnis ein Attribut mit Schlüssel-Wert-Paar **`Assigned Engineer`** / **`Bob`** zuordnen.

Arbeiten mit Ergebnissen

Führen Sie das folgende Verfahren für jedes der generierten Amazon Inspector Classic-Ergebnisse durch.

So finden und analysieren Sie Ergebnisse und ordnen ihnen Attribute zu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.
2. Nachdem Sie eine Bewertung durchgeführt haben, navigieren Sie zur Seite Ergebnisse in der Amazon Inspector Classic-Konsole, um Ihre Ergebnisse einzusehen.

   Sie können Ihre Ergebnisse auch im Abschnitt Bemerkenswerte Ergebnisse auf der Dashboard-Seite der Amazon Inspector Classic-Konsole einsehen.

> **Note**
>
> Sie können die von einem Bewertungslauf generierten Ergebnisse nicht anzeigen, während er noch läuft. Sie können jedoch eine Teilmenge der Ergebnisse ansehen, wenn Sie die Bewertung vor Abschluss der Laufzeit beenden. In einer Produktionsumgebung empfehlen wir Ihnen, jeden Bewertungslauf vollständig durchlaufen zu lassen, damit alle Ergebnisse produziert werden können.

3. Um die Details eines bestimmten Ergebnisses anzuzeigen, wählen Sie das Erweiterungswidget neben dem Ergebnis. Die Details des Fundes schließen folgendes mit ein:

   - Name des Bewertungsziels, das die EC2 Instanz enthält, in der dieses Ergebnis registriert wurde.
   - Name der Bewertungsvorlage, die verwendet wurde, um dieses Ergebnis zu erzeugen.
   - Startzeit des Bewertungslaufs.
   - Endzeitpunkt des Bewertungslaufs.
   - Status des Bewertungslaufs.
   - Name des Regelpakets, das die Regel enthält, die dieses Ergebnis ausgelöst hat.
   - Name des Ergebnisses.
   - Schweregrad des Ergebnisses.
   - Native Schweregraddaten aus dem Common Vulnerability Scoring System (CVSS). Hierzu gehören CVSS-Vektor und CVSS-Score-Kennzahlen (inklusive CVSS Version 2.0 und 3.0) für die Ergebnisse, die von den Regeln im Regelpaket "Häufige Schwachstellen und Aufdeckungen" ausgelöst werden. Weitere Details zu CVSS erhalten Sie unter https://www.first.org/cvss/.
   - Informationen zum systemeigenen Schweregrad vom Center for Internet Security (CIS). Hierzu gehört die CIS-Gewichtung für die Ergebnisse, die von den Regeln im CIS Benchmarks-Paket ausgelöst werden. Weitere Informationen zur CIS-Gewichtung erhalten Sie unter https://www.cisecurity.org/.
   - Beschreibung des Ergebnisses.
   - Empfohlene Schritte, die Sie ausführen können, um das potenzielle Sicherheitsproblem zu beheben, das durch das Ergebnis beschrieben wird.

4. Um einem Ergebnis Attribute zuzuordnen, wählen Sie ein Ergebnis aus und klicken Sie auf Add/Edit Attributes.

Sie können den Ergebnissen auch Attribute durch Erstellung einer neuen Bewertungsvorlage zuordnen. Hierzu konfigurieren Sie die neue Vorlage so, dass sie Attributen automatisch allen Ergebnissen zuordnet, die durch den Bewertungslauf erzeugt wurden. Sie können die Felder Schlüssel und Wert aus dem Feld Tags for findings from this assessment (Tags für Ergebnisse von dieser Bewertung) verwenden. Weitere Informationen finden Sie unter Amazon Inspector Classic Bewertungsvorlagen und Bewertungsläufe.

5. Um die Ergebnisse in eine Tabelle zu exportieren, wählen Sie den Abwärtspfeil rechts oben auf der Seite Findings (Ergebnisse). Wählen Sie im Dialogfeld die Option Export all columns (Alle Spalten exportieren) oder Export visible columns (Sichtbare Spalten exportieren).

   Beachten Sie, dass im exportierten Inhalt alle Datum/Uhrzeit-Werte Epoch-Zeitstempel sind.

6. Um Ihre aktuellen Ergebnisse zu filtern, geben Sie in die Filterleiste über der Ergebnistabelle eine einzelne Zeichenfolge ein, nach der Sie filtern möchten, z. B. eine Instanz-ID oder CVE-Nummer. Um zusätzliche Informationsspalten ein- oder auszublenden, wählen Sie das Einstellungssymbol in der oberen rechten Ecke der Ergebnisseite.

7. Um Ergebnisse zu löschen, wechseln Sie zur Seite Assessment runs (Bewertungsläufe) und wählen Sie den Lauf, der die zu löschenden Ergebnisse erzeugt hat. Wählen Sie dann Löschen aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja aus.

   > **Important**
   >
   > Sie können einzelne Ergebnisse in Amazon Inspector Classic nicht löschen. Wenn Sie einen Bewertungslauf löschen, werden alle Ergebnisse und alle Versionen des Berichts aus diesem Lauf ebenfalls gelöscht.

   Sie können einen Bewertungslauf auch unter Verwendung der DeleteAssessmentRun-API löschen.

Bewertungsberichte

Ein Amazon Inspector Classic-Bewertungsbericht ist ein Dokument, in dem detailliert beschrieben wird, was im Bewertungslauf getestet wurde und welche Ergebnisse der Bewertung erzielt wurden. Sie können die Berichte speichern, sie für Ihr Team für Abhilfemaßnahmen freigeben oder sie verwenden, um Ihre Compliance-Prüfungsdaten zu erweitern. Sie können einen Bericht für einen Bewertungslauf erstellen, nachdem die Ausführung erfolgreich abgeschlossen wurde.

> **Note**
>
> Sie können Berichte nur für Bewertungsläufe generieren, die nach dem 25. April 2017 stattfinden. Zu diesem Zeitpunkt wurden Bewertungsberichte in Amazon Inspector Classic verfügbar.

Sie können folgende Arten von Bewertungsberichten abrufen:

- Ergebnisbericht — Dieser Bericht enthält die folgenden Informationen:
  - Zusammenfassung der Bewertung
  - EC2 Instanzen, die während des Bewertungslaufs bewertet wurden
  - Regelpakete des Bewertungslaufs
  - Detaillierte Informationen zu jedem Ergebnis, einschließlich aller EC2 Instanzen, bei denen das Ergebnis festgestellt wurde
- Vollständiger Bericht — Dieser Bericht enthält alle Informationen, die in einem Ergebnisbericht enthalten sind, und enthält zusätzlich eine Liste der Regeln, die anhand der Fälle im Bewertungsziel überprüft wurden.

Erstellen Sie einen Bewertungsbericht wie folgt:

1. Suchen Sie auf der Seite Assessment runs (Bewertungsläufe) den Bewertungslauf, für den Sie für einen Bericht erstellen möchten. Stellen Sie sicher, dass der Status Analysis complete (Analyse abgeschlossen) lautet.
2. Wählen Sie in der Spalte Berichte dieses Bewertungslaufs das Berichtsymbol aus.

> **Important**
>
> Ab dem 24. März 2025 werden Bewertungsberichte keine Informationen mehr zum Schweregrad von Ergebnissen zur Netzwerkerreichbarkeit enthalten. Diese Information ist in der Amazon Inspector Inspector-Konsole verfügbar.

3. Wählen Sie im Dialogfeld Assessment report (Bewertungsbericht), den Berichtstyp, den Sie anzeigen möchten (entweder Ergebnisbericht oder Vollständiger Bericht) sowie das Berichtsformat (HTML oder PDF). Wählen Sie dann Bericht erstellen.

Sie können Bewertungsberichte auch mithilfe der GetAssessmentReport-API erstellen.

Zum Löschen eines Bewertungsberichts gehen Sie wie folgt vor.

So löschen Sie einen Bericht

- Wählen Sie auf der Seite Assessment runs (Bewertungsläufe) die Ausführung, auf welcher der zu löschende Bericht basiert, und wählen Sie dann Delete (Löschen). Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Ja aus.

  > **Important**
  >
  > In Amazon Inspector Classic können Sie keine einzelnen Berichte löschen. Wenn Sie einen Bewertungslauf löschen, werden alle Versionen des Berichts aus diesem Lauf sowie alle Ergebnisse ebenfalls gelöscht.

  Sie können einen Bewertungslauf auch unter Verwendung der DeleteAssessmentRun-API löschen.

Ausschlüsse in Amazon Inspector Classic

Ausschlüsse sind das Ergebnis von Amazon Inspector Classic-Bewertungsläufen. Ausnahmen zeigen, welche Ihrer Sicherheitskontrollen nicht durchgeführt werden können und wie Sie die entsprechenden Fehler beheben. Probleme können beispielsweise durch das Fehlen eines Agenten auf den EC2 Instances des angegebenen Ziels, die Verwendung eines nicht unterstützten Betriebssystems oder durch unerwartete Fehler verursacht werden.

Ausnahmen zeigen Sie auf der Seite Assessment runs (Bewertungsläufe) in der Konsole an. Weitere Informationen finden Sie unter Anzeigen der Ausnahmen nach der Bewertung.

Um unnötige AWS Gebühren zu vermeiden, können Sie mit Amazon Inspector Classic eine Vorschau der Ausschlüsse anzeigen, bevor Sie eine Bewertung durchführen. Die Ausnahmevorschauen finden Sie auf der Seite Assessment templates (Bewertungsvorlagen) in der Konsole. Weitere Informationen finden Sie unter Anzeigen einer Vorschau der Ausnahmen.

> **Note**
>
> Sie können Ausnahmen nach der Bewertung nur für Läufe erstellen, die nach dem 25. Juni 2018 ausgeführt wurden. Zu diesem Zeitpunkt wurden Ausschlüsse in Amazon Inspector Classic verfügbar. Vorschauen für Ausnahmen stehen jedoch für alle Bewertungsvorlagen unabhängig vom Datum zur Verfügung.

Themen

Ausnahmetypen

Amazon Inspector Classic kann die folgenden Ausschlusstypen erstellen.

Ausnatyp	Beschreibung	Empfehlung
Keine Instan im Ziel	Es gibt keine EC2 Instanzen mit den im Bewertungsziel angegebenen Tags.	Vergewissern Sie sich, dass die Tags in Ihrem Bewertungsziel mit den Tags Ihrer EC2 Zielinstanz übereinstimmen.
Agent wird bereits ausgeführt	Auf der EC2 Ziel-Instance ist bereits ein Testlauf im Gange.	Warten Sie, bis der aktuelle Bewertungslauf auf der EC2 Zielinstanz abgeschlossen ist.
Agent konnte nicht gefunden werde	Auf der EC2 Ziel-Instance wurde kein Amazon Inspector Classic-Agent gefunden.	Installieren Sie einen Amazon Inspector Classic-Agenten auf der EC2 Ziel-Instance oder installieren Sie

Ausnahmetyp	Beschreibung	Empfehlung
		ihn erneut. Weitere Informationen finden Sie unter Amazon Inspector Classic-Agenten installieren.
Agent ist fehlerhaft	Der Amazon Inspector Classic — Agent auf der EC2 Ziel-Instance hat einen fehlerhaften Status.	Überprüfen Sie den Status des Amazon Inspector Classic-Agenten auf dieser Instance und ergreifen Sie die erforderlichen Maßnahmen. Weitere Informationen finden Sie unter Inspector-Agenten.

Ausnahmetyp	Beschreibung	Empfehlung
Nicht unterstützte Betriebssystem ion	Das Betriebssystem der EC2 Ziel-Instance wird für Amazon Inspector Classic-Bewertungen nicht unterstützt.	Entfernen Sie die EC2 Ziel-Instance aus dem Bewertungsziel oder erstellen Sie ein Ziel, das diese Instance nicht enthält. Eine Liste der unterstützten Betriebssysteme finden Sie unter Amazon Inspector Classic — Unterstützte Betriebssysteme und Regionen.

Ausnahmetyp	Beschreibung	Empfehlung
Veraltetes Regelpaket	Die Bewertungsvorlage enthält ein veraltetes Regelpaket.	Erstellen Sie eine Bewertungsvorlage ohne das veraltete Regelpaket und verwenden Sie es für zukünftige Bewertungsläufe.

Ausnahmetyp	Beschreibung	Empfehlung
Regelt wird vom Betriebssystem nicht unterstützt	Das Betriebssystem der EC2 Ziel-Instance wird von einem Regelpaket, das in der Bewertungsvorlage enthalten ist, nicht unterstützt.	Erstellen Sie eine Bewertungsvorlage ohne die widersprüchlichen Regelpakete oder entfernen Sie die EC2 Zielinstanz aus der Bewertungsvorlage. Eine Liste der Regelpakete und Betriebssysteme finden Sie unter Verfügbarkeit von Regelpaketen bei unterstützten

Ausnahmetyp	Beschreibung	Empfehlung
		Betriebssystemen.
Regelauswertungsfehler für einzelne Instanz	Ein interner Fehler hat die Regelauswertung für diese Instance fehlschlagen lassen.	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Ausnahmetyp	Beschreibung	Empfehlung
Fehler bei der Regelauswertung	Ein interner Fehler hat die Regelauswertung für die Bewertung fehlschlagen lassen.	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Ausnahmetyp	Beschreibung	Empfehlung
Fehler bei der Erreichbarkeit des Netzwerks — Intern	Ein interner Fehler hat zu einem Fehlschlag der Netzwerkerreichbarkeits-Untersuchung beim Überprüfen von Ports geführt, die über das Internet erreichbar sind. Möglicherweise erhalten Sie Ergebnisse für andere Netzwerkerreichbarkeitstypen.	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Ausnahmetyp	Beschreibung	Empfehlung
Netzwerkerreichbarkeitsfehler — Internet über einen Application Load Balancer	Ein interner Fehler hat dazu geführt, dass eine Bewertung der Netzwerkerreichbarkeit bei der Suche nach Ports, die über einen Application Load Balancer aus dem Internet erreichbar sind, fehlschlug. Möglicherweise erhalten Sie Ergebnisse für andere Netzwerkerreichbarkeitstypen.	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Ausnahmetyp	Beschreibung	Empfehlung
Netzwerkerreichbarkeitsfehler — Internet über einen Elastic Load Balancing Load Balancer	Ein interner Fehler hat dazu geführt, dass eine Bewertung der Netzwerkerreichbarkeit bei der Suche nach Ports, die über einen Elastic Load Balancing Load Balancer vom Internet aus erreichbar sind, fehlschlug. Möglicherweise erhalten Sie Ergebnisse für andere Netzwerke	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Ausnahmetyp	Beschreibung	Empfehlung
	rreichbarkeitstypen.	
Fehler bei der Erreichbarkeit des Netzwerks — VPN	Ein interner Fehler hat zu einem Fehlschlag der Netzwerkerreichbarkeits-Untersuchung beim Überprüfen von Ports geführt, die über ein VPN erreichbar sind. Möglicherweise erhalten Sie Ergebnisse für andere Netzwerkerreichbarkeitstypen.	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Ausnahmetyp	Beschreibung	Empfehlung
Fehler bei der Erreichbarkeit des Netzwerks — AWS Direct Connect	Ein interner Fehler hat dazu geführt, dass eine Bewertung der Netzwerkerreichbarkeit bei der Überprüfung von Ports, über die erreichbar ist, fehlschlug. AWS Direct Connect Möglicherweise erhalten Sie Ergebnisse für andere Netzwerkerreichbarkeitstypen.	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Ausnahmetyp	Beschreibung	Empfehlung
Fehler bei der Netzwerkerreichbarkeit — VPC-Peering	Ein interner Fehler hat zu einem Fehlschlag der Netzwerkerreichbarkeits-Untersuchung beim Überprüfen von Ports geführt, die über eine per Peering verbundenen VPC erreichbar sind. Möglicherweisen erhalten Sie Ergebnisse für andere Netzwerkerreichbarkeitstypen.	Versuchen Sie, die Bewertung erneut auszuführen. Nehmen Sie Kontakt mit dem Support auf, falls die Ausnahme weiterhin besteht, wenn Sie die Prüfung erneut ausführen.

Anzeigen einer Vorschau der Ausnahmen

Mit Amazon Inspector Classic können Sie eine Vorschau potenzieller Ausschlüsse anzeigen, bevor Sie eine Bewertung durchführen.

Zeigen Sie Vorschauen zu Bewertungsausnahmen wie folgt an:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.
2. Wählen Sie im Navigationsbereich Bewertungsvorlagen aus.
3. Erweitern Sie eine Vorlage und wählen Sie im Bereich Assessment templates (Bewertungsvorlagen) die Option Preview exclusions (Ausnahmenvorschauen anzeigen).
4. Prüfen Sie die Beschreibungen aller erkannten Ausnahmen und die Empfehlungen, wie diese zu behandeln sind.

   Sie können Ausnahmen auch jeweils mit den Operationen `ListExclusions` und `DescribeExclusions` auflisten und beschreiben.

Anzeigen der Ausnahmen nach der Bewertung

Nach einem Bewertungslaufs können Sie Details zu beliebigen Ausnahmen anzeigen.

So zeigen Sie Details zu Ausnahmen an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon Inspector Classic-Konsole unter https://console.aws.amazon.com/inspector/.
2. Wählen Sie im Navigationsbereich Bewertungsläufe aus.
3. Wählen Sie in der Spalte Exclusions (Ausnahmen) den aktiven Link aus, der mit einem Bewertungslauf verknüpft ist.
4. Prüfen Sie die Beschreibungen aller erkannten Ausnahmen und die Empfehlungen, wie diese zu behandeln sind.

   Sie können Ausnahmen auch jeweils mit den Operationen `ListExclusions` und `DescribeExclusions` auflisten und beschreiben.

Amazon Inspector Classic-Regelpakete für unterstützte Betriebssysteme

Sie können Amazon Inspector Classic-Regelpakete für die EC2 Instances ausführen, die in Ihren Bewertungszielen enthalten sind. Die folgende Tabelle zeigt die Verfügbarkeit von Regelpaketen für unterstützte Betriebssysteme.

Important

Sie können eine agentenlose Bewertung mit dem Regelpaket für Network Reachability auf jeder EC2 Instance unabhängig vom Betriebssystem durchführen.

Note

Weitere Informationen über unterstützte Betriebssysteme finden Sie unter Von Amazon Inspector Classic unterstützte Betriebssysteme und Regionen.

Unterzte Betriesystem	Häufige Schwachstellen und Aufdeckungen	CIS Benchmarks	Netzwerkerreichbarkeit	Bewährte Methoden für die Sicherheit	Laufzeitverhaltens-Analyse
Amaz Linux 2	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Amaz Linux 2018.	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Amaz Linux 2017.	Unterstützt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet

Unter zte Betrie ystem	Häufige Schwachst ellen und Aufdeckun gen	CIS Benchmarks	Netzwerke rreichbarkeit	Bewährte Methoden für die Sicherheit	Laufzeitv erhaltens-Analyse
Amaz Linux 2017.	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Amaz Linux 2016.	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Amaz Linux 2016.	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Amaz Linux 2015.	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Amaz Linux 2015.	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Amaz Linux 2014.	Unterstüt zt		Unterstützt	Unterstützt	
Amaz Linux 2014.	Unterstüt zt		Unterstützt	Unterstützt	
Amaz Linux 2013.	Unterstüt zt		Unterstützt	Unterstützt	

Unter zte Betrie ysten	Häufige Schwachst ellen und Aufdeckun gen	CIS Benchmarks	Netzwerke rreichbarkeit	Bewährte Methoden für die Sicherheit	Laufzeitv erhaltens-Analyse
Amaz Linux 2013.	Unterstüt zt		Unterstützt	Unterstützt	
Amaz Linux 2012.	Unterstüt zt		Unterstützt	Unterstützt	
Amaz Linux 2012.	Unterstüt zt		Unterstützt	Unterstützt	
Ubun 20.04 LTS	Unterstüt zt		Unterstützt	Unterstützt	
Ubun 18.04 LTS	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Ubun 16.04 LTS	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Ubun 14.04 LTS	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Debia 10.x, 9.0-9 8.0-8	Unterstüt zt		Unterstützt	Unterstützt	

Unter zte Betrie ysten	Häufige Schwachst ellen und Aufdeckun gen	CIS Benchmarks	Netzwerke rreichbarkeit	Bewährte Methoden für die Sicherheit	Laufzeitv erhaltens-Analyse
RHEL 8.x	Unterstüt zt		Unterstützt	Unterstützt	
RHEL 7,6 — 7.x	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	
RHEL 6.2 - 6.9, 7.2 - 7.5	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet
Cent(7.6 – 7.X	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	
Cent(6.2 - 6.9, 7.2 - 7.5	Unterstüt zt	Unterstützt	Unterstützt	Unterstützt	Als veraltet gekennzeichnet

Unter zte Betrie ystem	Häufige Schwachst ellen und Aufdeckun gen	CIS Benchmarks	Netzwerke rreichbarkeit	Bewährte Methoden für die Sicherheit	Laufzeitv erhaltens-Analyse
Wind Serve 2019 Base	Unterstüt zt		Unterstützt		
Wind Serve 2016 Base	Unterstüt zt	Unterstützt	Unterstützt		Als veraltet gekennzeichnet
Wind Serve 2012 R2	Unterstüt zt	Unterstützt	Unterstützt		Als veraltet gekennzeichnet
Wind Serve	Unterstüt zt	Unterstützt	Unterstützt		Als veraltet gekennzeichnet
Wind Serve 2008 R2	Unterstüt zt	Unterstützt	Unterstützt		Als veraltet gekennzeichnet

Protokollieren von Amazon Inspector Classic API-Aufrufen mit AWS CloudTrail

Amazon Inspector Classic ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in Amazon Inspector Classic ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Amazon Inspector Classic als Ereignisse, einschließlich Aufrufe von der Amazon Inspector Classic-Konsole und Codeaufrufen an die Amazon Inspector Classic-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon Inspector Classic. Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an Amazon Inspector Classic, die IP-Adresse, von der die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und vieles mehr ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch. Eine vollständige Liste der Amazon Inspector Classic-API-Operationen finden Sie unter Aktionen in der Amazon Inspector Classic API-Referenz.

Informationen zu Amazon Inspector Classic in CloudTrail

CloudTrail ist für Ihr AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn in Amazon Inspector Classic eine Aktivität auftritt, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Ereignissen für Amazon Inspector Classic, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser standardmäßig für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails

- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

CloudTrail protokolliert alle Amazon Inspector Classic-Operationen, einschließlich schreibgeschützter Operationen wie `ListAssessmentRuns` und `DescribeAssessmentTargets` und Verwaltungsoperationen wie `AddAttributesToFindings` und. `CreateAssessmentTemplate`

> **Note**
>
> CloudTrail protokolliert nur die Anforderungsinformationen von schreibgeschützten Amazon Inspector Classic-Vorgängen. Sowohl Anfrage- als auch Antwortinformationen werden für alle anderen Amazon Inspector Classic-Vorgänge protokolliert.

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 Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu Amazon Inspector Classic-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie andere Anforderungsparameter. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der den Amazon Inspector `CreateResourceGroup` Classic-Vorgang demonstriert:


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
```

```
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

Überwachung von Amazon Inspector Classic mit Amazon CloudWatch

Sie können Amazon Inspector Classic mithilfe von Amazon überwachen CloudWatch, das Rohdaten sammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit verfügbar sind. Standardmäßig sendet Amazon Inspector Classic Metrikdaten innerhalb von 5 Minuten CloudWatch an. Sie können die AWS Management Console, oder eine API verwenden AWS CLI, um die Metriken anzuzeigen, an die Amazon Inspector Classic sendet CloudWatch.

Weitere Informationen zu Amazon CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Amazon Inspector CloudWatch Classic-Metriken

Der Amazon Inspector Classic-Namespace umfasst die folgenden Metriken.

`AssessmentTargetARN`-Metriken:

Metrik	Beschreibung
`TotalMatchingAgents`	Anzahl der Agenten, die diesem Ziel entsprechen
`TotalHealthyAgents`	Anzahl der Agenten, die diesem Ziel entsprechen und stabil sind
`TotalAssessmentRuns`	Anzahl der Bewertungsläufe für dieses Ziel
`TotalAssessmentRun Findings`	Anzahl der Ergebnisse für dieses Ziel

`AssessmentTemplateARN`-Metriken:

Metrik	Beschreibung
`TotalMatchingAgents`	Anzahl der Agenten, die dieser Vorlage entsprechen
`TotalHealthyAgents`	Anzahl der Agenten, die dieser Vorlage entsprechen und stabil sind

Metrik	Beschreibung
`TotalAssessmentRuns`	Anzahl der Bewertungsläufe für diese Vorlage
`TotalAssessmentRunFindings`	Anzahl der Ergebnisse für diese Vorlage

Gesamtmetriken

Metrik	Beschreibung
`TotalAssessmentRuns`	Anzahl der Bewertungsläufe in diesem Konto AWS

Konfiguration von Amazon Inspector Classic mit AWS CloudFormation

Referenzinformationen zu Amazon Inspector Classic-Ressourcen, die von unterstützt werden AWS CloudFormation, finden Sie in den folgenden Themen:

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

> **Important**
>
> Eine Liste ARNs der Amazon Inspector Classic-Regelpakete in unterstützten AWS Regionen finden Sie unterAmazon Inspector Classic ARNS für Regelpakete.

Integration mit AWS Security Hub

AWS Security Hubbietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Industriestandards und Best Practices zu überprüfen. Security Hub sammelt Sicherheitsdaten von AWS Konten, Diensten und unterstützten Partnerprodukten von Drittanbietern und hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

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

Inhalt

So sendet Amazon Inspector Ergebnisse an Security Hub

Im Security Hub werden Sicherheitsprobleme als Erkenntnisse verfolgt. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder 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 Listen mit Erkenntnissen anzeigen und filtern und Details zu einer Erkenntnis anzeigen. Siehe .Ergebnisse anzeigen im AWS Security Hub -Leitfaden. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Siehe Ergreifen von Maßnahmen zu Ergebnissen im AWS Security Hub -Leitfaden.

Alle Ergebnisse in Security Hub verwenden ein standardmäßiges JSON-Format, das AWS Security Finding Format (ASFF). Das ASFF enthält Details über die Ursache des Problems, die betroffenen Ressourcen und den aktuellen Status der Erkenntnis. Weitere Informationen finden Sie im AWS Security Hub Benutzerhandbuch unter AWS Security Finding Format (ASFF).

Amazon Inspector ist einer der AWS Dienste, der Ergebnisse an Security Hub sendet.

Arten von Ergebnissen, die Amazon Inspector sendet

Amazon Inspector sendet alle von ihm generierten Ergebnisse an Security Hub.

Amazon Inspector sendet die Ergebnisse mithilfe des AWS Security Finding Formats (ASFF) an Security Hub. In ASFF gibt das `Types`-Feld die Art der Erkenntnis an. Ergebnisse von Amazon Inspector können die folgenden Werte für haben`Types`.

- Software und Konfiguration Checks/Vulnerabilities/CVE
- Checks/AWS Security Best Practices/NetworkErreichbarkeit von Software und Konfiguration
- Benchmarks zur Checks/Industry and Regulatory Standards/CIS Host-Hardening-Lösung für Software und Konfiguration

Latenz für das Senden von Erkenntnissen

Wenn Amazon Inspector ein neues Ergebnis erstellt, wird es normalerweise innerhalb von fünf Minuten an Security Hub gesendet.

Wiederholen, wenn der Security Hub nicht verfügbar ist

Wenn Security Hub nicht verfügbar ist, versucht Amazon Inspector erneut, die Ergebnisse zu senden, bis sie eingegangen sind.

Aktualisieren von vorhandenen Erkenntnissen in Security Hub

Nachdem Amazon Inspector ein Ergebnis an Security Hub gesendet hat, aktualisiert es das Ergebnis, um zusätzliche Beobachtungen der Findungsaktivität widerzuspiegeln. Dies führt zu weniger Ergebnissen von Amazon Inspector in Security Hub als in Amazon Inspector.

Typisches Ergebnis von Amazon Inspector

Amazon Inspector sendet Ergebnisse mithilfe des AWS Security Finding Formats (ASFF) an Security Hub.

Hier ist ein Beispiel für ein typisches Ergebnis von Amazon Inspector.


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

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

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

Aktivieren und Konfigurieren der Integration

Um die Integration mit Security Hub verwenden zu können, müssen Sie den 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. Amazon Inspector beginnt, Ergebnisse an Security Hub zu senden.

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.

Weitere Informationen finden Sie unter Deaktivieren und Aktivieren des Ergebnisflusses aus einer Integration (Konsole) oder Deaktivieren des Ergebnisflusses aus einer Integration (Security Hub Hub-API, AWS-CLI) im AWS Security Hub Benutzerhandbuch.

Amazon Inspector Classic ARNs

Jedem Ressourcentyp und jedem Regelpaket in Amazon Inspector Classic ist ein eindeutiger Amazon-Ressourcenname (ARN) zugeordnet.

Inhalt

ARNs für Amazon Inspector Classic-Ressourcen

In Amazon Inspector Classic sind die Hauptressourcen Ressourcengruppen, Bewertungsziele, Bewertungsvorlagen, Bewertungsläufe und Ergebnisse. Diesen Ressourcen sind eindeutige Amazon-Ressourcennamen (ARNs) zugeordnet, wie in der folgenden Tabelle dargestellt.

Ressourcentyp	ARN-Format
Ressourcengruppe	`arn:aws:inspector:` *region*`:`*account-id* `:resource group/` *ID*
Bewertungsziel	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*
Bewertungsvorlage	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`:template:` *ID*
Bewertungslauf	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`/template/` *ID*`/run/`*ID*
Erkenntnis	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`/template/` *ID*`/run/`*ID*`/finding/` *ID*

Amazon Inspector Classic ARNS für Regelpakete

Die folgenden Tabellen zeigen die Regelpakete ARNs für Amazon Inspector Classic in allen unterstützten Regionen.

Themen

- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

USA Ost (Ohio)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85`
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh`
Netzwerkerreichbarkeit	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30`
Bewährte Methoden für die Sicherheit	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX`

USA Ost (Nord-Virginia)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7`

Name des Regelpakets	ARN
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8`
Netzwerkerreichbarkeit	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd`
Bewährte Methoden für die Sicherheit	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q`

USA West (Nordkalifornien)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa`
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX`
Netzwerkerreichbarkeit	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF`

Name des Regelpakets	ARN
Bewährte Methoden für die Sicherheit	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-byoQRFYm`

USA West (Oregon)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p`
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc`
Netzwerkerreichbarkeit	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl`
Bewährte Methoden für die Sicherheit	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ`

Asien-Pazifik (Mumbai)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9dO`
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m`
Netzwerkerreichbarkeit	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1`
Bewährte Methoden für die Sicherheit	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj`

Asien-Pazifik (Seoul)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc`
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws:inspector:ap-northeast-2:526`

Name des Regelpakets	ARN
	946625049:rulespac kage/0-T9srhg1z
Netzwerkerreichbarkeit	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-s3OmLzhL
Bewährte Methoden für die Sicherheit	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n

Asien-Pazifik (Sydney)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-D5TGAxiR
Benchmarks für die Sicherheitskonfiguration des CIS Betriebss ystems	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-Vkd2Vxjq
Netzwerkerreichbarkeit	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-FLcuV4Gz
Bewährte Methoden für die Sicherheit	arn:aws:inspector: ap-southeast-2:454

Name des Regelpakets	ARN
	640832652:rulespac kage/0-asL6HRgN

Asien-Pazifik (Tokio)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-gHP9oWNT
Benchmarks für die Sicherheitskonfiguration des CIS Betriebss ystems	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-7WNjqgGu
Netzwerkerreichbarkeit	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-YI95DVd7
Bewährte Methoden für die Sicherheit	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-bBUQnxMq

Europa (Frankfurt)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	arn:aws:inspector: eu-central-1:53750

Name des Regelpakets	ARN
	3971621:rulespackage/0-wNqHa8M9
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-nZrAVuv8
Netzwerkerreichbarkeit	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
Bewährte Methoden für die Sicherheit	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

Europa (Irland)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
Netzwerkerreichbarkeit	arn:aws:inspector:eu-west-1:35755712

Name des Regelpakets	ARN
	9151:rulespackage/0-SPzU33xe
Bewährte Methoden für die Sicherheit	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SnojL3Z6

Europa (London)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
Netzwerkerreichbarkeit	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
Bewährte Methoden für die Sicherheit	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

Europa (Stockholm)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd`
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f`
Netzwerkerreichbarkeit	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu`
Bewährte Methoden für die Sicherheit	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf`

AWS GovCloud (US-Ost)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	`arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFu0b`
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	`arn:aws-us-gov:inspector:us-gov-east`

Name des Regelpakets	ARN
	-1:206278770380:rulespackage/0-pTLCdIww
Bewährte Methoden für die Sicherheit	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

AWS GovCloud (US-West)

Name des Regelpakets	ARN
Häufige Schwachstellen und Aufdeckungen	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
Benchmarks für die Sicherheitskonfiguration des CIS Betriebssystems	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc
Bewährte Methoden für die Sicherheit	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G

Dokumentverlauf

In der folgenden Tabelle wird der Versionsverlauf der Amazon Inspector Classic -Dokumentation nach Mai 2018 beschrieben.

Änderung	Beschreibung	Datum
Ende des Support-Hinweises	Hinweis zum Ende des Supports: Am 20. Mai 2026 AWS wird der Support für Amazon Inspector Classic eingestellt. Nach dem 20. Mai 2026 können Sie nicht mehr auf die Amazon Inspector Classic-Konsole oder die Amazon Inspector Classic-Ressourcen zugreifen. Weitere Informationen erhalten Sie unter Ende des Supports für Amazon Inspector Classic.	20. Mai 2025
Bewährte Sicherheitsmethoden für Passwörter wurden aktualisiert	Die Best Practice-Sicherheitsanforderungen von Amazon Inspector Classic in Bezug auf die Länge und Komplexität von EC2 Instanzkennwörtern wurden aktualisiert. Weitere Informationen finden Sie unter Mindestlänge für Kennwörter konfigurieren und Kennwortkomplexität konfigurieren	8. März 2021
Unterstützung für neuere Betriebssystemversionen wurde hinzugefügt	Amazon Inspector Classic unterstützt jetzt die folgenden Betriebssystemversionen: Ubuntu 20.4 LTS, Debian	15. Oktober 2020

	10.x, RHEL 8.x und Windows Server 2019 Base.	
Die Sicherheitsinformationen wurden in einem neuen Sicherheitskapitel zusammengefasst	Sicherheitsinformationen für Amazon Inspector Classic, einschließlich Informationen zur Verwaltung der Identitäts- und Zugriffsverwaltung, sind in einem Sicherheitskapitel zusammengefasst. Weitere Informationen finden Sie unter Sicherheit in Amazon Inspector Classic.	7. April 2020
Die Dokumentation wurde aktualisiert, um die Unterstützung für das Runtime Behavior Analysis-Regelpaket zu entfernen.	Mehrere Themen wurden aktualisiert, um Informationen zum Regelpaket zur Laufzeitverhaltens-Analyse zu entfernen, das nicht mehr unterstützt wird.	5. September 2019
Betriebssystemunterstützung hinzugefügt	Amazon Inspector Classic-Unterstützung für CentOS 7.6 wurde hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Betriebssysteme und Regionen von Amazon Inspector Classic und Regeln für die Verfügbarkeit von Paketen auf allen unterstützten Betriebssystemen.	3. Dezember 2018

Neuer Inhalt	Das Regelpaket Amazon Inspector Classic Network Reachability wurde hinzugefügt, mit dem Benutzer agentenlose Bewertungen durchführen können, bei denen die Netzwerkkonfiguration auf Sicherheitslücken analysiert wird. Weitere Informationen finden Sie unter Netzwerkerreichbarkeit.	9. November 2018
Betriebssystemunterstützung hinzugefügt	Amazon Inspector Classic-Unterstützung für RHEL 7.6 wurde hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Betriebssysteme und Regionen von Amazon Inspector Classic und Regeln für die Verfügbarkeit von Paketen auf allen unterstützten Betriebssystemen.	30. Oktober 2018
Betriebssystemunterstützung hinzugefügt	Unterstützung für verschiedene Betriebssysteme zum CIS Benchmark-Regelpaket hinzugefügt. Weitere Informationen finden Sie unter Center for Internet Security (CIS) Benchmarks und Verfügbarkeit von Regelpaketen bei unterstützten Betriebssystemen.	13. August 2018
Zusätzliche Unterstützung für Regionen hinzugefügt	Unterstützung für die Region `AWS GovCloud (US)` hinzugefügt.	13. Juni 2018

In der folgenden Tabelle wird der Versionsverlauf der Amazon Inspector Classic -Dokumentation vor Juni 2018 beschrieben.

Änderung	Beschreibung	Datum
Neuer Inhalt	Es wurde die Möglichkeit hinzugefügt, alle EC2 Amazon-Instances in einem Konto als Ziel anzusprechen. Weitere Informationen finden Sie unter Bewertungsziele von Amazon Inspector Classic.	24. Mai 2018
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic-Unterstützung für Amazon Linux 2018.03 und Ubuntu 18.04 wurde hinzugefügt.	15. Mai 2018
Neuer Inhalt	Es wurde die Möglichkeit hinzugefügt, wiederkehrende Amazon Inspector Classic-Bewertungen einzurichten.	30. April 2018
Neuer Inhalt	Es wurde die Möglichkeit hinzugefügt, einen Amazon Inspector Classic-Agenten über die Konsole zu installieren.	30. April 2018
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic Support für Amazon Linux 2 hinzugefügt.	13. März 2018
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic Assessment Support für Windows Server 2016 Base hinzugefügt.	20. Februar 2018

Änderung	Beschreibung	Datum
Zusätzliche Unterstützung für Regionen hinzugefügt	Amazon Inspector Classic-Unterstützung für die `US East (Ohio)` Region hinzugefügt.	7. Februar 2018
Neuer Inhalt	Amazon Inspector Classic-Bewertungen können jetzt ausgeführt werden, wenn das Kernelmodul nicht verfügbar ist.	11. Januar 2018
Zusätzliche Unterstützung für Regionen hinzugefügt	Amazon Inspector Classic-Unterstützung für die `EU (Frankfurt)` Region hinzugefügt.	19. Dezember 2017
Neuer Inhalt	Es wurde die Möglichkeit hinzugefügt, den Zustand von Amazon Inspector Classic-Agenten mit der Amazon Inspector Classic-API und -Konsole zu überprüfen.	15. Dezember 2017
Neuer Inhalt	Folgende Funktionen wurden hinzugefügt: • Nutzung serviceverknüpfter Rollen • Amazon Inspector Classic Agent-AMI im AWS Marketplace verfügbar • Amazon Inspector Classic — AWS CloudFormation Vorlagen	5. Dezember 2017

Änderung	Beschreibung	Datum
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic-Assessment-Unterstützung für CentOS 7.4 wurde hinzugefügt.	9. November 2017
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic Assessment Support für Amazon Linux 2017.09 hinzugefügt.	11. Oktober 2017
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic-Assessment-Unterstützung für RHEL 7.4 wurde hinzugefügt.	20. Februar 2018
HIPAA-Qualifikation hinzugefügt	Amazon Inspector Classic ist jetzt HIPAA-fähig.	31. Juli 2017
Neuer Inhalt	Es wurde die Möglichkeit hinzugefügt, die Amazon Inspector Classic-Sicherheitsbewertung mit Amazon CloudWatch Events automatisch auszulösen.	27. Juli 2017
Zusätzliche Unterstützung für Regionen hinzugefügt	Amazon Inspector Classic-Unterstützung für die `US West (N. California)` Region hinzugefügt.	6. Juni 2018
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic-Assessment-Unterstützung für RHEL 6.2-6.9, RHEL 7.2-7.3, CentOS 6.9 und CentOS 7.2-7.3 wurde hinzugefügt.	23. Mai 2017

Änderung	Beschreibung	Datum
Unterstützung für Betriebssystem hinzugefügt	Amazon Inspector Classic Assessment Support für Amazon Linux 2017.03 hinzugefügt.	25. April 2017
Neue Inhalte und zusätzliche Betriebssystemunterstützung	Hinzugefügt: • Amazon Inspector Classic-Unterstützung für Ubuntu 16.04. • Verfügbarkeit von Lambda Blueprint für die Automatisierung von Amazon Inspector Classic-Vorgängen.	5. Januar 2017
Neue Betriebssystemunterstützung	Amazon Inspector Classic Support für Microsoft Windows hinzugefügt.	26. August 2016
Zusätzliche Unterstützung für Regionen hinzugefügt	Amazon Inspector Classic-Unterstützung für die `Asia Pacific (Seoul)` Region hinzugefügt.	26. August 2016
Zusätzliche Unterstützung für Regionen hinzugefügt	Amazon Inspector Classic-Unterstützung für die `Asia Pacific (Mumbai)` Region hinzugefügt.	25. April 2016
Zusätzliche Unterstützung für Regionen hinzugefügt	Amazon Inspector Classic-Unterstützung für die `Asia Pacific (Sydney)` Region hinzugefügt.	25. April 2016

Änderung	Beschreibung	Datum
Servicestart	Amazon Inspector Classic: Service eingeführt.	7. Oktober 2015

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.