aws

Benutzer-Leitfaden

AWS Audit-Manager

AWS Audit-Manager: Benutzer-Leitfaden

Table of Contents

Was ist AWS Audit Manager?

Willkommen im AWS Audit Manager Benutzerhandbuch.

AWS Audit Manager hilft Ihnen dabei, Ihre AWS Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen. Audit Manager automatisiert die Erhebung von Beweisen, um die Bewertung zu erleichtern, ob Ihre Richtlinien, Verfahren und Aktivitäten – auch als Kontrollen bezeichnet – effektiv funktionieren. Wenn es Zeit für ein Audit ist, hilft Audit Manager Ihnen, Beteiligtenüberprüfungen bei Ihren Kontrollen zu verwalten. Das bedeutet, dass Sie mit deutlich weniger manuellem Aufwand audittaugliche Berichte erstellen können.

Audit Manager bietet vorgefertigte Frameworks, die Bewertungen für einen bestimmten Compliance-Standard oder eine bestimmte Verordnung strukturieren und automatisieren. Frameworks umfassen eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind nach den Anforderungen des angegebenen Compliance-Standards oder der jeweiligen Verordnung gruppiert. Sie können Frameworks und Kontrollen zur Unterstützung interner Audits auch an Ihre konkreten Anforderungen anpassen.

Sie können eine Bewertung anhand eines beliebigen Frameworks erstellen. Wenn Sie eine Bewertung erstellen, führt Audit Manager automatisch Ressourcenbewertungen durch. Bei diesen Bewertungen werden Daten für diejenigen erfasst AWS-Konten , die Sie als Umfang für Ihr Audit definieren. Die erhobenen Daten werden automatisch in prüfungsfreundliche Beweise umgewandelt. Anschließend werden sie den entsprechenden Kontrollen zugeordnet, sodass Sie die Einhaltung der Vorschriften in den Bereichen Sicherheit, Änderungsmanagement, Geschäftskontinuität und Softwarelizenzierung nachweisen können. Dieser Prozess der Beweissuche ist fortlaufend und beginnt, wenn Sie Ihre Bewertung erstellen. Nachdem Sie ein Audit abgeschlossen haben und Audit Manager nicht mehr zum Erheben von Beweisen benötigen, können Sie die Beweissuche beenden. Ändern Sie dazu den Status Ihrer Bewertung auf inaktiv.

Funktionen von Audit Manager

Mit AWS Audit Manager können Sie die folgenden Aufgaben ausführen:

- Schneller Einstieg – Erstellen Sie Ihre erste Bewertung, indem Sie aus einer Galerie vorgefertigter Frameworks auswählen, die eine Reihe von Compliance-Standards und Vorschriften unterstützen.

Initiieren Sie anschließend die automatische Erfassung von Nachweisen, um Ihre AWS-Service Nutzung zu überprüfen.

- Beweise aus Hybrid- oder Multi-Cloud-Umgebungen hochladen und verwalten – Zusätzlich zu den Beweisen, die Audit Manager aus Ihrer AWS -Umgebung erhebt, können Sie auch Beweise aus Ihrer lokalen oder Multi-Cloud-Umgebung hochladen und zentral verwalten.
- Unterstützung gängiger Compliance-Standards und Vorschriften – Wählen Sie eines der AWS Audit Manager Standard-Frameworks. Diese Frameworks bieten vorgefertigte Kontrollzuordnungen für gängige Compliance-Standards und -Vorschriften. Dazu gehören der CIS Foundation Benchmark, PCI DSS, GDPR, HIPAA SOC2, GxP und AWS betriebliche Best Practices.
- Überwachen Sie Ihre aktiven Bewertungen – Verwenden Sie das Audit Manager-Dashboard, um Analysedaten für Ihre aktiven Bewertungen einzusehen und schnell nicht konforme Beweise zu identifizieren, die behoben werden müssen.
- Suche nach Beweisen — Verwenden Sie die Beweissuche Funktion, um schnell Beweise zu finden, die für Ihre Suchanfrage relevant sind. Sie können aus Ihren Suchergebnissen einen Bewertungsbericht erstellen oder Ihre Suchergebnisse im CSV-Format exportieren.
- Erstellen Sie benutzerdefinierte Steuerelemente — Erstellen Sie Ihr eigenes Steuerelement von Grund auf neu oder erstellen Sie eine bearbeitbare Kopie eines vorhandenen Standardsteuerelements oder benutzerdefinierten Steuerelements. Sie können auch das Feature für benutzerdefinierte Kontrollen verwenden, um Fragen zur Risikobewertung zu erstellen und die Antworten auf diese Fragen als manuelle Beweise zu speichern.
- Ordnen Sie Ihre Unternehmenskontrollen vordefinierten Gruppierungen von AWS Datenquellen zu — Wählen Sie die allgemeinen Kontrollen aus, die Ihren Zielen entsprechen, und verwenden Sie sie, um benutzerdefinierte Kontrollen zu erstellen, die Belege für Ihr Portfolio an Compliance-Anforderungen sammeln.
- Erstellen Sie benutzerdefinierte Frameworks — Erstellen Sie Ihre eigenen Frameworks mit Standard- oder benutzerdefinierten Kontrollen, die auf Ihren spezifischen Anforderungen für interne Audits basieren.
- Teilen Sie benutzerdefinierte Frameworks — Teilen Sie Ihre benutzerdefinierten Audit Manager Manager-Frameworks mit anderen AWS-Konto oder replizieren Sie sie in ein anderes AWS-Region unter Ihrem eigenen Konto.
- Support der teamübergreifenden Zusammenarbeit – Delegieren Sie Kontrollsätze an Fachexpertenko, die entsprechende Beweise überprüfen, Kommentare hinzufügen und den Status der einzelnen Kontrollen aktualisieren können.

- Berichte für Prüfer erstellen – Generieren Sie Bewertungsberichte, in denen die relevanten Beweise zusammengefasst sind, die für Ihr Audit erhoben wurden, und Links zu Ordnern enthalten, welche die detaillierten Beweise enthalten.
- Stellen Sie die Integrität der Beweise sicher – Speichern Sie Beweise an einem sicheren Ort, wo sie unverändert bleiben.

> **Note**
>
> AWS Audit Manager hilft beim Sammeln von Nachweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Standards und -Vorschriften relevant sind. Ihre Einhaltung wird jedoch nicht bewertet. Die auf diese Weise gesammelten Nachweise enthalten AWS Audit Manager daher möglicherweise nicht alle Informationen über Ihre AWS Nutzung, die für Audits erforderlich sind. AWS Audit Manager ist kein Ersatz für Rechtsbeistand oder Compliance-Experten.

Preise für Audit Manager

Weitere Informationen über die Preise finden Sie unter AWS Audit Manager – Preise.

Verwenden Sie Audit Manager zum ersten Mal?

Wenn Sie erstmaliger Benutzer von Audit Manager sind, empfehlen wir Ihnen, mit den folgenden Seiten zu beginnen:

1. AWS Audit Manager Konzepte und Terminologie verstehen— Erfahren Sie mehr über die wichtigsten Konzepte und Begriffe, die in Audit Manager verwendet werden, wie z. B. Bewertungen, Frameworks und Kontrollen.
2. Verstehen, wie Beweise AWS Audit Manager gesammelt werden— Erfahren Sie, wie Audit Manager Beweise für eine Ressourcenbewertung sammelt.
3. Einrichtung AWS Audit Manager mit den empfohlenen Einstellungen— Erfahren Sie mehr über die Einrichtungsanforderungen für Audit Manager.
4. Erste Schritte mit AWS Audit Manager— Folgen Sie einem Tutorial, um Ihr erstes Audit Manager Manager-Assessment zu erstellen.
5. AWS Audit Manager API-Referenz — Machen Sie sich mit den API-Aktionen und Datentypen von Audit Manager vertraut.

Verwandt AWS-Services

AWS Audit Manager lässt sich in mehrere Funktionen integrieren AWS-Services , um automatisch Beweise zu sammeln, die Sie in Ihre Bewertungsberichte aufnehmen können.

AWS Security Hub CSPM

AWS Security Hub CSPM überwacht Ihre Umgebung mithilfe automatisierter Sicherheitsprüfungen, die auf AWS bewährten Verfahren und Industriestandards basieren. Audit Manager erfasst Schnappschüsse Ihrer Ressourcensicherheit, indem er die Ergebnisse von Sicherheitsüberprüfungen direkt aus Security Hub CSPM meldet. Weitere Informationen zu Security Hub CSPM finden Sie unter Was ist? AWS Security Hub CSPM im AWS Security Hub CSPM Benutzerhandbuch.

AWS CloudTrail

AWS CloudTrail hilft Ihnen dabei, die Aufrufe von AWS Ressourcen in Ihrem Konto zu überwachen. Dazu gehören Aufrufe von der AWS Management Console, der AWS CLI und anderen AWS-Services. Audit Manager sammelt Protokolldaten CloudTrail direkt von und wandelt die verarbeiteten Protokolle in Nachweise für Benutzeraktivitäten um. Weitere Informationen zu CloudTrail finden Sie unter Was ist AWS CloudTrail? im AWS CloudTrail Benutzerhandbuch.

AWS Config

AWS Config bietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie konfiguriert wurden. Audit Manager erfasst Schnappschüsse Ihrer Ressourcensicherheit, indem die Ergebnisse direkt von AWS Config gemeldet werden. Weitere Informationen zu finden Sie AWS Config unter Was ist AWS Config? im AWS Config Benutzerhandbuch.

AWS License Manager

AWS License Manager optimiert den Prozess der Bereitstellung von Lizenzen von Softwareanbietern in die Cloud. Beim Aufbau einer Cloud-Infrastruktur können Sie Kosten sparen AWS, indem Sie Ihr vorhandenes Lizenzinventar für die Nutzung mit Cloud-Ressourcen wiederverwenden. Audit Manager bietet ein License Manager-Framework, das Sie bei der Vorbereitung Ihrer Audits unterstützt. Dieses Framework ist in License Manager integriert, um Informationen zur Lizenznutzung auf der Grundlage von kundendefinierten Lizenzregeln zu aggregieren. Weitere Informationen zu License Manager finden Sie unter Was ist AWS License Manager? im AWS License Manager Benutzerhandbuch.

AWS Control Tower

AWS Control Tower setzt präventive und detektivische Schutzmaßnahmen für die Cloud-Infrastruktur durch. Audit Manager bietet ein AWS Control Tower Guardrails-Framework, das Sie bei Ihrer Prüfungsvorbereitung unterstützt. Dieses Framework enthält alle AWS Config Regeln, die auf Guardrails von basieren. AWS Control Tower Weitere Informationen zu finden Sie AWS Control Tower unter Was ist? AWS Control Tower im AWS Control Tower Benutzerhandbuch.

AWS Artifact

AWS Artifact ist ein Self-Service-Portal zum Abrufen von Prüfartefakten, das bei Bedarf Zugriff auf die Compliance-Dokumentation und Zertifizierungen für die Infrastruktur bietet. AWS AWS Artifact bietet Nachweise dafür, dass die AWS Cloud-Infrastruktur die Compliance-Anforderungen erfüllt. Im Gegensatz dazu AWS Audit Manager hilft es Ihnen, Nachweise zu sammeln, zu überprüfen und zu verwalten, um nachzuweisen, dass Ihre Nutzung von gesetzeskonform AWS-Services ist. Weitere Informationen zu AWS Artifact finden Sie unter Was ist AWS Artifact? im AWS Artifact Benutzerhandbuch. Sie können eine Liste von AWS Berichten in der herunterladen AWS-Managementkonsole.

Amazon EventBridge

Amazon EventBridge hilft Ihnen dabei, Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu automatisieren AWS-Services und automatisch darauf zu reagieren. Sie können EventBridge Regeln verwenden, um Audit Manager Manager-Ereignisse zu erkennen und darauf zu reagieren. Ruft auf der Grundlage der von Ihnen erstellten EventBridge Regeln eine oder mehrere Zielaktionen auf, wenn ein Ereignis den Werten entspricht, die Sie in einer Regel angeben. Weitere Informationen finden Sie unter Überwachung AWS Audit Manager mit Amazon EventBridge.

Eine Liste der einzelnen Compliance-Programme AWS-Services im Geltungsbereich finden Sie unter AWS-Services Umfang nach Compliance-Programmen. Allgemeine Informationen finden Sie unter AWS -Compliance-Programme.

Weitere Ressourcen für den Audit Manager

Lesen Sie die folgenden Ressourcen, um weitere Informationen über den Audit Manager zu erhalten.

- Sammeln Sie Beweise und verwalten Sie Prüfungsdaten mit AWS Audit Manager
- Integrieren Sie das Drei-Lines-Modell (Teil 2): Verwandeln Sie AWS Config Konformitätspakete in AWS Audit Manager Bewertungen aus dem AWS Management & Governance-Blog

AWS Audit Manager Konzepte und Terminologie verstehen

In diesem Thema werden die wichtigsten Konzepte vorgestellt, um Ihnen den Einstieg in AWS Audit Manager zu erleichtern.

A

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Bewertung

Sie können eine Audit Manager-Bewertung verwenden, um automatisch Beweise zu erheben, die für ein Audit relevant sind.

Eine Bewertung basiert auf einem Framework, bei dem es sich um eine Gruppierung von Kontrollen handelt, die sich auf Ihr Audit beziehen. Sie können eine Bewertung anhand eines Standard-Frameworks oder eines benutzerdefinierten Frameworks erstellen. Standard-Frameworks enthalten vorgefertigte Kontrollsätze, die einen bestimmten Compliance-Standard oder eine bestimmte Compliance-Verordnung unterstützen. Im Gegensatz dazu enthalten benutzerdefinierte Frameworks Steuerelemente, die Sie entsprechend Ihren spezifischen Prüfanforderungen anpassen und gruppieren können. Wenn Sie ein Framework als Ausgangspunkt verwenden, können Sie eine Bewertung erstellen, in der festgelegt wird AWS-Konten , welche Elemente Sie in den Umfang Ihres Audits aufnehmen möchten.

Wenn Sie eine Bewertung erstellen, beginnt Audit Manager automatisch mit der Bewertung der Ressourcen in Ihrem System auf der AWS-Konten Grundlage der im Framework definierten Kontrollen. Als Nächstes erhebt er die relevanten Beweise und wandelt sie in ein prüferfreundliches Format um. Danach fügt er die Beweise den Kontrollen in Ihrer Bewertung bei. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die erhobenen Beweise überprüfen und sie dann einem Bewertungsbericht hinzufügen. Mit diesem Bewertungsbericht können Sie nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Erhebung von Beweisen ist ein fortlaufender Prozess, der mit der Erstellung Ihrer Bewertung beginnt. Sie können die Beweissuche beenden, indem Sie den Bewertungsstatus auf inaktiv ändern. Alternativ können Sie die Beweissuche auf Kontrollebene beenden. Sie können dies tun, indem Sie den Status einer bestimmten Kontrolle in Ihrer Bewertung auf inaktiv ändern.

Anweisungen zum Erstellen und Verwalten von Bewertungen finden Sie unter Verwaltung von Bewertungen in AWS Audit Manager.

Bewertungsbericht

Ein Bewertungsbericht ist ein abgeschlossenes Dokument, das auf der Grundlage einer Bewertung durch den Audit Manager generiert wird. Diese Berichte fassen die relevanten Beweise zusammen, die für Ihr Audit erhoben wurden. Sie sind mit den entsprechenden Beweisordnern verknüpft. Die Ordner sind entsprechend den Kontrollen benannt und organisiert, die in Ihrer Bewertung festgelegt wurden. Für jede Bewertung können Sie die von Audit Manager erhobenen Beweise überprüfen und entscheiden, welche Beweise Sie in den Bewertungsbericht aufnehmen möchten.

Weitere Informationen über Bewertungsberichte finden Sie unter Bewertungsberichte. Informationen zur Erstellung eines Bewertungsberichts finden Sie unter Erstellung eines Bewertungsberichts in AWS Audit Manager.

Zielort des Bewertungsberichts

Ein Zielort für Bewertungsberichte ist der standardmäßige S3-Bucket, in dem Audit Manager Ihre Bewertungsberichte speichert. Weitere Informationen hierzu finden Sie unter Konfiguration Ihres Standardziels für Bewertungsberichte.

Audit

Ein Audit ist eine unabhängige Prüfung der Vermögenswerte, der Abläufe oder der Geschäftsintegrität Ihres Unternehmens. Bei einem Informationstechnologie-Audit (IT-Audit) werden speziell die Kontrollen innerhalb der Informationssysteme Ihres Unternehmens untersucht. Das Ziel eines IT-Audits besteht darin, festzustellen, ob Informationssysteme Vermögenswerte schützen, effektiv funktionieren und die Datenintegrität wahren. All dies ist wichtig, um die regulatorischen Anforderungen zu erfüllen, die durch einen Compliance-Standard oder eine Verordnung vorgeschrieben sind.

Audit-Verantwortlicher

Der Begriff Audit-Verantwortlicher hat je nach Kontext zwei verschiedene Bedeutungen.

Im Kontext von Audit Manager ist ein Audit-Verantwortlicher ein Benutzer oder eine Rolle, die eine Bewertung und die zugehörigen Ressourcen handhabt. Zu den Aufgaben dieser Person als Audit-Verantwortlicher gehören die Erstellung von Bewertungen, die Überprüfung von Beweisen und die Erstellung von Bewertungsberichten. Audit Manager ist ein kollaborativer Service, und Audit-Verantwortlicher profitieren davon, wenn andere Interessengruppen an ihren Bewertungen teilnehmen. Sie können beispielsweise weitere Audit-Verantwortlicher zu Ihrer Bewertung hinzufügen, um gemeinsam Verwaltungsaufgaben zu übernehmen. Oder, wenn Sie

ein Audit-Verantwortlicher sind und Hilfe bei der Interpretation der für eine Kontrolle erhobenen Beweise benötigen, können Sie diesen Kontrollsatz an einen Beteiligten delegieren, der über Fachkenntnisse in diesem Bereich verfügt. Eine solche Person wird als Delegierter bezeichnet.

In geschäftlicher Hinsicht ist ein Audit-Verantwortlicher jemand, der die Bemühungen seines Unternehmens zur Vorbereitung auf die Prüfung koordiniert und überwacht und einem Prüfer Beweise vorlegt. In der Regel handelt es sich dabei um einen Experten für Unternehmensführung, Risiko und Compliance (GRC), beispielsweise einen Compliance-Beauftragten oder einen DSGVO-Datenschutzbeauftragten. GRC-Experten verfügen über das Fachwissen und die Befugnis, die Auditvorbereitung zu verwalten. Insbesondere verstehen sie die Compliance-Anforderungen und können Berichtsdaten analysieren, interpretieren und aufbereiten. Auch andere betriebliche Rollen können jedoch die Rolle eines Audit-Verantwortlichen übernehmen – nicht nur GRC-Experten übernehmen diese Rolle. Sie könnten sich beispielsweise dafür entscheiden, Ihre Audit-Manager-Bewertungen von einem technischen Experten aus einem der folgenden Teams einrichten und verwalten zu lassen:

- SecOps
- IT/ DevOps
- Reaktion auf Sicherheitsoperationen Center/Incident
- Ähnliche Teams, die Cloud-Ressourcen besitzen, entwickeln, korrigieren und bereitstellen und die Cloud-Infrastruktur Ihres Unternehmens verstehen

Wen Sie in Ihrer Audit-Manager-Bewertung als Audit-Verantwortlichen benennen, hängt stark von Ihrer Organisation ab. Es hängt auch davon ab, wie Sie Ihre Sicherheitsabläufe strukturieren und wie das Audit konkret abläuft. In Audit Manager kann dieselbe Person in einer Prüfung die Rolle des Audit-Verantwortlichen und in einer anderen die Rolle des Delegierten annehmen.

Unabhängig davon, wie Sie Audit Manager verwenden, können Sie die Aufgabentrennung in Ihrem Unternehmen mithilfe der owner/delegate Audit-Persona und der Gewährung spezifischer IAM-Richtlinien für jeden Benutzer verwalten. Durch diesen zweistufigen Ansatz stellt Audit Manager sicher, dass Sie die volle Kontrolle über alle Einzelheiten einer individuellen Bewertung haben. Weitere Informationen finden Sie unter Empfohlene Richtlinien für Benutzerrollen in AWS Audit Manager.

AWS verwaltete Quelle

Eine AWS verwaltete Quelle ist eine Beweisquelle, die AWS für Sie aufbewahrt wird.

Jede AWS verwaltete Quelle ist eine vordefinierte Gruppierung von Datenquellen, die einem bestimmten gemeinsamen Steuerelement oder zentralen Steuerelement zugeordnet ist. Wenn

Sie ein gemeinsames Steuerelement als Beweisquelle verwenden, sammeln Sie automatisch Beweise für alle Kernkontrollen, die dieses gemeinsame Steuerelement unterstützen. Sie können auch einzelne Kernkontrollen als Beweisquelle verwenden.

Immer wenn eine AWS verwaltete Quelle aktualisiert wird, werden dieselben Updates automatisch auf alle benutzerdefinierten Kontrollen angewendet, die diese AWS verwaltete Quelle verwenden. Das bedeutet, dass Ihre benutzerdefinierten Kontrollen Beweise anhand der neuesten Definitionen dieser Beweisquelle sammeln. Auf diese Weise können Sie die kontinuierliche Einhaltung der Vorschriften sicherstellen, wenn sich die Cloud-Compliance-Umgebung ändert.

Siehe auch:customer managed source,evidence source.

C

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Änderungsprotokoll

Für jede Kontrolle in einer Bewertung verfolgt Audit Manager die Benutzeraktivitäten für diese Kontrolle. Anschließend können Sie einen Audit Trail mit Aktivitäten überprüfen, die sich auf eine bestimmte Kontrolle beziehen. Weitere Informationen darüber, welche Benutzeraktivitäten im Changelog erfasst werden, finden Sie unterRegisterkarte „Änderungsprotokoll“.

Cloud-Compliance

Cloud-Compliance ist der allgemeine Grundsatz, dass in der Cloud bereitgestellte Systeme den Standards entsprechen müssen, mit denen Cloud-Kunden konfrontiert sind.

Gemeinsame Steuerung

Siehe control.

Compliance-Vorschriften

Eine Compliances-Vorschrift ist ein Gesetz, eine Regel oder eine andere Anordnung, die von einer Behörde vorgeschrieben wird, in der Regel zur Regulierung des Verhaltens. Ein Beispiel ist die DSGVO.

Compliance-Standard

Ein Compliance-Standard ist ein strukturierter Satz von Richtlinien, in denen die Prozesse eines Unternehmens zur Einhaltung festgelegter Vorschriften, Spezifikationen oder Gesetze detailliert beschrieben werden. Beispiele hierfür sind PCI DSS und HIPAA.

Kontrolle

Eine Kontrolle ist eine Schutz- oder Gegenmaßnahme, die für ein Informationssystem oder ein Unternehmen vorgeschrieben ist. Die Kontrollen dienen dazu, die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Informationen zu schützen und eine Reihe definierter Anforderungen zu erfüllen. Sie bieten die Gewissheit, dass Ihre Ressourcen wie vorgesehen funktionieren, Ihre Daten zuverlässig sind und Ihr Unternehmen die geltenden Gesetze und Vorschriften einhält.

In Audit Manager kann eine Kontrolle auch eine Frage in einem Fragebogen zur Lieferantenrisikobewertung darstellen. In diesem Fall handelt es sich bei einer Kontrolle um eine konkrete Frage, mit der Informationen zum Sicherheits- und Compliance-Status eines Unternehmens abgefragt werden.

Kontrollen erheben kontinuierlich Beweise, wenn sie in Ihren Audit Manager-Bewertungen aktiv sind. Sie können zu jeder Kontrolle auch manuell Beweise hinzufügen. Bei jedem Nachweis handelt es sich um eine Aufzeichnung, anhand derer Sie die Einhaltung der Kontrollanforderungen nachweisen können.

Audit Manager bietet die folgenden Arten von Kontrollen:

Art der Kontrolle	Description
Gemeinsame Steuerung	Sie können sich eine gemeinsame Kontrolle als eine Maßnahme vorstellen, die Ihnen hilft, ein Kontrollziel zu erreichen. Da gemeinsame Kontrollen nicht spezifisch für einen Compliance-Standard sind, helfen sie Ihnen dabei, Nachweise zu sammeln, die eine Reihe sich überschneidender Compliance-Verpflichtungen belegen können. Nehmen wir zum Beispiel an, Sie haben ein Kontrollziel namens Datenklassifizierung und -verarbeitung. Um dieses Ziel zu erreichen, könnten Sie eine gemeinsame Steuerung namens Zugriffskontrollen implementieren, um unbefugten Zugriff auf Ihre Ressourcen zu überwachen und zu erkennen. • Automatisierte gemeinsame Kontrollen sammeln Beweise für Sie. Sie bestehen aus einer Gruppierung einer oder mehrerer verwandter Kernkontrollen. Jede dieser Kernkontrollen sammelt wiederum automatisch relevante Nachweise aus einer vordefinierten Gruppe von AWS Datenquellen. AWS verwaltet diese zugrunde liegenden Datenquellen für Sie und aktualisiert

Art der Kontrolle	Description
	sie, wenn sich Vorschriften und Standards ändern und neue Datenquellen identifiziert werden. • Bei den üblichen manuellen Kontrollen müssen Sie Ihre eigenen Nachweise hochladen. Dies liegt daran, dass sie in der Regel physische Aufzeichn ungen oder Informationen über Ereignisse erfordern, die sich außerhalb Ihrer AWS Umgebung ereignen. Aus diesem Grund gibt es häufig keine AWS Datenquellen, die die Anforderungen der manuellen gemeinsamen Kontrolle belegen könnten. Sie können ein allgemeines Steuerelement nicht bearbeiten. Sie können jedoch jedes gängige Steuerelement als Beweisquelle verwenden, wenn Sie ein benutzerdefiniertes Steuerelement erstellen.
Zentrale Steuerung	Dies ist eine verbindliche Richtlinie für Ihre AWS Umgebung. Sie können sich eine zentrale Steuerung als eine Maßnahme vorstellen, die Ihnen hilft, die Anforderungen einer gemeinsamen Steuerung zu erfüllen. Nehmen wir zum Beispiel an, Sie verwenden ein allgemeines Steuerelement namens Zugriffskontrollen, um den unbefugten Zugriff auf Ihre Ressourcen zu überwachen. Um diese allgemeine Kontrolle zu unterstützen, könnten Sie das zentrale Steuerelement namens Block public read access in S3-Buckets verwenden. Da zentrale Kontrollen nicht spezifisch für einen Compliance-Standard sind, sammeln sie Nachweise, die eine Reihe sich überschneidender Complianc e-Verpflichtungen belegen können. Jede zentrale Kontrolle verwendet eine oder mehrere Datenquellen, um Beweise für eine bestimmte AWS-Service Datenquelle zu sammeln. AWS verwaltet diese zugrunde liegenden Datenquel len für Sie und aktualisiert sie, wenn sich Vorschriften und Standards ändern und neue Datenquellen identifiziert werden. Sie können ein zentrales Steuerelement nicht bearbeiten. Sie können jedoch jedes zentrale Steuerelement als Beweisquelle verwenden, wenn Sie ein benutzerdefiniertes Steuerelement erstellen.

Art der Kontrolle	Description
Standards teuerung	Dies ist ein vordefiniertes Steuerelement, das Audit Manager bereitstellt. Sie können Standardkontrollen verwenden, um Sie bei der Prüfungsv orbereitung für einen bestimmten Compliance-Standard zu unterstützen. Jede Standardkontrolle bezieht sich auf einen bestimmten Standard framework in Audit Manager und sammelt Nachweise, anhand derer Sie die Einhaltun g dieses Frameworks nachweisen können. Standardkontrollen sammeln Nachweise aus zugrunde liegenden Datenquellen, die AWS verwaltet werden. Diese Datenquellen werden automatisch aktualisiert, wenn sich Vorschriften und Standards ändern und neue Datenquellen identifiziert werden. Standardsteuerelemente können nicht bearbeitet werden. Sie können jedoch von jedem Standardsteuerelement eine bearbeitbare Kopie erstellen.
Benutzerd efiniertes Steuerele ment	Dies ist ein Steuerelement, das Sie in Audit Manager erstellen, um Ihre spezifischen Compliance-Anforderungen zu erfüllen. Sie können ein benutzerdefiniertes Steuerelement von Grund auf neu erstellen oder eine bearbeitbare Kopie eines vorhandenen Standardsteuerelements erstellen. Wenn Sie ein benutzerdefiniertes Steuerelement erstellen, können Sie bestimmte evidence source s definieren, die bestimmen, woher Audit Manager Beweise sammelt. Nachdem Sie ein benutzerdefiniertes Steuerele ment erstellt haben, können Sie dieses Steuerelement bearbeiten oder es einem benutzerdefinierten Framework hinzufügen. Sie können auch eine bearbeitbare Kopie eines beliebigen benutzerdefinierten Steuerelements erstellen.

Kontrolldomäne

Sie können sich eine Kontrolldomäne als eine Kategorie von Kontrollen vorstellen, die nicht spezifisch für einen Compliance-Standard ist. Ein Beispiel für eine Kontrolldomäne ist Datenschutz.

Aus einfachen organisatorischen Gründen werden Kontrollen häufig nach Domänen gruppiert. Jede Domäne hat mehrere Ziele.

Kontrolldomänengruppierungen sind eine der leistungsstärksten Funktionen des Audit Manager-Dashboards. Audit Manager hebt die Kontrollen in Ihren Bewertungen hervor, die nachweislich nicht konform sind, und gruppiert sie nach Kontrolldomänen. Auf diese Weise können Sie sich bei der Vorbereitung eines Audits auf bestimmte Themenbereiche konzentrieren.

Ziel der Kontrolle

Ein Kontrollziel beschreibt das Ziel der gemeinsamen Kontrollen, die unter dieses Ziel fallen. Für jedes Ziel können mehrere gemeinsame Kontrollen gelten. Wenn diese gemeinsamen Kontrollen erfolgreich implementiert werden, helfen sie Ihnen, das Ziel zu erreichen.

Jedes Kontrollziel fällt unter einen Kontrollbereich. Beispielsweise könnte die Kontrolldomäne Datenschutz ein Kontrollziel mit dem Namen Datenklassifizierung und -verarbeitung haben. Um dieses Kontrollziel zu unterstützen, könnten Sie ein allgemeines Steuerelement namens Zugriffskontrollen verwenden, um unbefugten Zugriff auf Ihre Ressourcen zu überwachen und zu erkennen.

Zentrale Steuerung

Siehe control.

Benutzerdefinierte Steuerung

Siehe control.

Vom Kunden verwaltete Quelle

Eine vom Kunden verwaltete Quelle ist eine von Ihnen definierte Beweisquelle.

Wenn Sie in Audit Manager ein benutzerdefiniertes Steuerelement erstellen, können Sie diese Option verwenden, um Ihre eigenen individuellen Datenquellen zu erstellen. Dies gibt Ihnen die Flexibilität, automatisierte Nachweise aus einer unternehmensspezifischen Ressource, z. B. einer benutzerdefinierten AWS Config Regel, zu sammeln. Sie können diese Option auch verwenden, wenn Sie Ihrem benutzerdefinierten Steuerelement manuelle Beweise hinzufügen möchten.

Wenn Sie vom Kunden verwaltete Quellen verwenden, sind Sie dafür verantwortlich, alle von Ihnen erstellten Datenquellen zu verwalten.

Siehe auch:AWS managed source,evidence source.

D

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Datenquelle

Audit Manager verwendet Datenquellen, um Beweise für eine Kontrolle zu sammeln. Eine Datenquelle hat die folgenden Eigenschaften:

- Ein Datenquellentyp definiert, aus welcher Art von Datenquelle Audit Manager Beweise sammelt.
  - Bei automatisierten Nachweisen kann es sich bei dem Typ um AWS Security Hub CSPMAWS Config, AWS CloudTrail, oder AWS API-Aufrufe handeln.
  - Wenn Sie Ihre eigenen Beweise hochladen, ist der Typ Manuell.
  - Die Audit Manager Manager-API bezeichnet einen Datenquellentyp als sourceType.
- Eine Datenquellenzuordnung ist ein Schlüsselwort, das festlegt, woher Beweise für einen bestimmten Datenquellentyp gesammelt werden.
  - Dies kann beispielsweise der Name eines CloudTrail Ereignisses oder der Name einer AWS Config Regel sein.
  - Die Audit Manager Manager-API bezeichnet eine Datenquellenzuordnung als SourceKeyword.
- Ein Datenquellenname kennzeichnet die Kombination von Datenquellentyp und Zuordnung.
  - Für Standardkontrollen stellt Audit Manager einen Standardnamen bereit.
  - Für benutzerdefinierte Steuerelemente können Sie Ihren eigenen Namen angeben.
  - Die Audit Manager-API bezeichnet einen Datenquellennamen als SourceName.

Eine einzelne Kontrolle kann mehrere Datenquellentypen und mehrere Zuordnungen haben. Beispielsweise kann ein Steuerelement Beweise aus einer Mischung von Datenquellentypen (wie AWS Config Security Hub CSPM) sammeln. Ein anderes Steuerelement könnte AWS Config den einzigen Datenquellentyp mit mehreren AWS Config Regeln als Zuordnungen haben.

Die folgende Tabelle listet die automatisierten Datenquellentypen auf und zeigt Beispiele für einige entsprechende Zuordnungen.

Datenquellentyp	Description	Beispiel für Zuweisungen
AWS Security Hub CSPM	Verwenden Sie diesen Datenquellentyp, um einen Snapshot Ihrer Ressource nsicherheit zu erstellen.	`EC2.1`

Datenquellentyp	Description	Beispiel für Zuweisungen
	Audit Manager verwendet den Namen eines Security Hub CSPM-Steuerelements als Zuordnungsschlüsselwort und meldet das Ergebnis dieser Sicherheitsprüfung direkt vom Security Hub CSPM.	
AWS Config	Verwenden Sie diesen Datenquellentyp, um einen Snapshot Ihrer Ressource nsicherheit zu erstellen. Audit Manager verwendet den Namen einer AWS Config Regel als Zuordnung sschlüsselwort und meldet das Ergebnis dieser Regelprüfung direkt von AWS Config.	`SNS_ENCRYPTED_KMS`
AWS CloudTrail	Verwenden Sie diesen Datenquellentyp, um eine bestimmte Benutzeraktivität nachzuverfolgen, die für Ihr Audit erforderlich ist. Audit Manager verwendet den Namen eines CloudTrai l Ereignisses als Zuordnung sschlüsselwort und erfasst die entsprechenden Benutzeraktivitäten aus Ihren CloudTrail Protokollen.	`CreateAccessKey`

Datenquellentyp	Description	Beispiel für Zuweisungen
AWS API-Aufrufe	Verwenden Sie diesen Datenquellentyp, um über einen API-Aufruf an eine bestimmte Ressource einen Snapshot Ihrer Ressource nkonfiguration zu erstellen AWS-Service. Audit Manager verwendet den Namen des API-Aufrufs als Zuordnungsschlüsselwort und sammelt die API-Antwo rt.	`kms_ListKeys`

Delegierter

Ein Delegierter ist ein AWS Audit Manager Benutzer mit eingeschränkten Berechtigungen. Delegierte verfügen in der Regel über spezialisiertes geschäftliches oder technisches Fachwissen. Diese Fachkenntnisse können beispielsweise in den Bereichen Datenaufbewahrungsrichtlinien, Schulungspläne, Netzwerkinfrastruktur oder Identitätsmanagement liegen. Die Delegierten helfen den Audit-Verantwortlichen dabei, die erhobenen Beweise auf Kontrollen zu überprüfen, die in ihren Zuständigkeitsbereich fallen. Delegierte können Kontrollsätze und die zugehörigen Beweise überprüfen, Kommentare hinzufügen, zusätzliche Beweise hochladen und den Status der einzelnen Kontrollen, die Sie ihnen zur Überprüfung zuweisen, aktualisieren.

Die Audit-Verantwortlichen weisen den Delegierten bestimmte Kontrollsätze zu, nicht ganze Bewertungen. Aus diesem Grund haben Delegierte nur begrenzten Zugriff auf Bewertungen. Anweisungen zum Delegieren eines Kontrollsatzes finden Sie unter Delegationen in AWS Audit Manager.

E

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Beweise

Beweise sind Aufzeichnungen, welche die Informationen enthalten, die erforderlich sind, um die Einhaltung der Anforderungen einer Kontrolle nachzuweisen. Zu den Beweisen gehören beispielsweise eine von einem Benutzer aufgerufene Änderungsaktivität und ein Snapshot der Systemkonfiguration.

In Audit Manager gibt es zwei Hauptarten von Beweisen: Automatisierte Beweise und manuelle Beweise.

Art des Nachweises	Description
Automatisierte Beweise	Dies sind die Nachweise, die Audit Manager automatisch sammelt. Dies umfasst die folgenden drei Kategorien automatisierter Beweise: 1. Konformitätsprüfung — Das Ergebnis einer Konformitätsprüfung wird von AWS Security Hub CSPM oder beiden erfasst. AWS Config Beispiele für Konformitätsprüfungen sind ein Sicherheitsprüfungsergebnis von Security Hub CSPM für eine PCI-DSS-Kontrolle und eine AWS Config Regelauswertung für eine HIPAA-Kontrolle. Weitere Informationen erhalten Sie unter AWS-Config-Regeln unterstützt von AWS Audit Manager und AWS Security Hub CSPM Steuerelemente, die unterstützt werden von AWS Audit Manager. 2. Benutzeraktivität — Benutzeraktivitäten, die eine Ressourcenkonfiguration ändern, werden in CloudTrail Protokollen erfasst, sobald diese Aktivität stattfindet. Beispiele für Benutzeraktivitäten sind eine Aktualisierung der Routing-Tabelle, eine Änderung der Backup-Einstellungen für Amazon RDS-Instances und eine Änderung der S3-Bucket-Verschlüsselungsrichtlinie. Weitere Informationen finden Sie unter AWS CloudTrail Eventnamen werden unterstützt von AWS Audit Manager. 3. Konfigurationsdaten – Ein Snapshot der Ressourcenkonfiguration wird direkt von einem AWS-Service auf täglicher, wöchentlicher oder monatlicher Basis erfasst.

Art des Nachweises	Description
	Beispiele für Konfigurations-Snapshots sind eine Liste von Routen für eine VPC-Routing-Tabelle, eine Amazon RDS-Instance-Backup-Einstellung und eine S3-Bucket-Verschlüsselungsrichtlinie. Weitere Informationen finden Sie unter AWS API-Aufrufe werden unterstützt von AWS Audit Manager.
Manueller Nachweis	Dies ist der Nachweis, den Sie selbst zu Audit Manager hinzufügen. Es gibt drei Möglichkeiten, eigene Beweise hinzuzufügen: 1. Importieren einer Datei aus Amazon S3 2. Laden Sie eine Datei von Ihrem Browser hoch 3. Geben Sie eine Textantwort auf eine Frage zur Risikobeurteilung ein Weitere Informationen finden Sie unter Manuelle Nachweise hinzufügen in AWS Audit Manager.

Die automatische Erfassung von Beweisen beginnt, wenn Sie eine Bewertung erstellen. Dies ist ein fortlaufender Prozess, und Audit Manager sammelt Beweise je nach Art der Beweise und der zugrunde liegenden Datenquelle mit unterschiedlichen Intervallen. Weitere Informationen finden Sie unter Verstehen, wie Beweise AWS Audit Manager gesammelt werden.

Anweisungen zum Überprüfen von Beweisen in einer Bewertung finden Sie unter Überprüfung von Nachweisen in AWS Audit Manager.

Quelle der Beweise

Eine Evidenzquelle definiert, woher eine Kontrolle Beweise sammelt. Dabei kann es sich um eine einzelne Datenquelle oder um eine vordefinierte Gruppierung von Datenquellen handeln, die einem gemeinsamen Steuerelement oder einem zentralen Steuerelement zugeordnet ist.

Wenn Sie ein benutzerdefiniertes Steuerelement erstellen, können Sie Beweise aus AWS verwalteten Quellen, kundenverwalteten Quellen oder beidem sammeln.

> **Tip**
>
> Wir empfehlen, AWS verwaltete Quellen zu verwenden. Immer wenn eine AWS verwaltete Quelle aktualisiert wird, werden dieselben Updates automatisch auf alle benutzerdefinierten Steuerelemente angewendet, die diese Quellen verwenden. Das bedeutet, dass Ihre benutzerdefinierten Kontrollen immer Beweise anhand der neuesten Definitionen dieser Beweisquelle sammeln. Auf diese Weise können Sie die kontinuierliche Einhaltung der Vorschriften sicherstellen, wenn sich die Cloud-Compliance-Umgebung ändert.

Siehe auch:AWS managed source,customer managed source.

Methode zur Beweissuche

Es gibt zwei Möglichkeiten, wie eine Kontrolle Beweise sammeln kann.

Methode zur Beweissuche	Description
Automatisiert	Automatisierte Kontrollen sammeln automatisch Beweise aus AWS Datenquellen. Diese automatisierten Beweise können Ihnen helfen, die vollständige oder teilweise Einhaltung der Kontrolle nachzuweisen.
Manuell	Bei manuellen Kontrollen müssen Sie Ihre eigenen Nachweise hochladen, um die Einhaltung der Kontrollen nachzuweisen.

> **Note**
>
> Sie können jeder automatisierten Kontrolle manuelle Beweise beifügen. In vielen Fällen ist eine Kombination aus automatisierten und manuellen Beweisen erforderlich, um die vollständige Einhaltung einer Kontrolle nachzuweisen. Audit Manager kann zwar automatisierte Beweise bereitstellen, die hilfreich und relevant sind, einige automatisierte Beweise weisen jedoch möglicherweise nur auf eine teilweise Einhaltung der Vorschriften hin. In diesem Fall können Sie die automatisierten Beweise, die Audit Manager bereitstellt, durch Ihre eigenen Beweise ergänzen.
> Beispiel:

- Das AWS Framework für bewährte Methoden für generative KI v2 enthält ein Steuerelement namens`Error analysis`. Bei dieser Kontrolle müssen Sie feststellen, wann Ungenauigkeiten bei der Verwendung Ihres Modells festgestellt werden. Außerdem müssen Sie eine gründliche Fehleranalyse durchführen, um die Ursachen zu ermitteln und Abhilfemaßnahmen zu ergreifen.
- Um diese Kontrolle zu unterstützen, sammelt Audit Manager automatisierte Nachweise, aus denen hervorgeht, ob CloudWatch Alarme für den AWS-Konto Ort aktiviert sind, an dem Ihre Bewertung ausgeführt wird. Anhand dieser Beweise können Sie nachweisen, dass die Kontrolle teilweise eingehalten wird, indem Sie nachweisen, dass Ihre Alarme und Prüfungen korrekt konfiguriert sind.
- Um die vollständige Einhaltung der Vorschriften nachzuweisen, können Sie die automatisierten Beweise durch manuelle Beweise ergänzen. Sie können beispielsweise eine Richtlinie oder ein Verfahren hochladen, das Ihren Fehleranalyseprozess, Ihre Schwellenwerte für Eskalationen und Berichte sowie die Ergebnisse Ihrer Ursachenanalyse aufzeigt. Anhand dieses manuellen Beweises können Sie nachweisen, dass die festgelegten Richtlinien gelten und dass auf Aufforderung hin Abhilfemaßnahmen ergriffen wurden.

Ein detaillierteres Beispiel finden Sie unter Kontrollen mit gemischten Datenquellen.

Exportzielort

Ein Exportzielort ist der standardmäßige S3-Bucket, in dem Audit Manager die Dateien speichert, die Sie aus dem Evidence Finder exportieren. Weitere Informationen finden Sie unter Konfiguration Ihres Standardexportziels für Evidence Finder.

F

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Framework

Ein Audit Manager Manager-Framework strukturiert und automatisiert Bewertungen für einen bestimmten Standard oder ein bestimmtes Prinzip der Risikosteuerung. Diese Frameworks umfassen eine Sammlung vordefinierter oder kundenspezifischer Kontrollen und helfen Ihnen dabei, Ihre AWS Ressourcen den Anforderungen dieser Kontrollen zuzuordnen.

In Audit Manager gibt es zwei Arten von Frameworks.

Typ des Frameworks	Description
Standardrahmen	Dies ist ein vorgefertigtes Framework, das auf AWS bewährten Verfahren für verschiedene Compliance-Standards und -Vorschriften basiert. Sie können Standard-Frameworks verwenden, um Sie bei der Vorbereitung von Audits für einen bestimmten Compliance-Standard oder eine Verordnung wie PCI DSS oder HIPAA zu unterstützen.
Benutzerdefiniertes Framework	Dies ist ein benutzerdefiniertes Framework, das Sie als Audit Manager Manager-Benutzer definieren. Sie können benutzerdefinierte Frameworks verwenden, um Sie bei der Vorbereitung von Audits gemäß Ihren spezifischen GRC-Anforderungen zu unterstützen.

Anweisungen zum Erstellen und Verwalten von Frameworks finden Sie unter Verwendung der Framework-Bibliothek zur Verwaltung von Frameworks in AWS Audit Manager.

> **Note**
>
> AWS Audit Manager hilft bei der Erfassung von Nachweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Standards und -Vorschriften relevant sind. Ihre Einhaltung wird jedoch nicht bewertet. Die auf diese Weise gesammelten Nachweise enthalten AWS Audit Manager daher möglicherweise nicht alle Informationen über Ihre AWS Nutzung, die für Audits erforderlich sind. AWS Audit Manager ist kein Ersatz für Rechtsbeistand oder Compliance-Experten.

Gemeinsame Nutzung von Frameworks

Sie können die Teilen eines benutzerdefinierten Frameworks in AWS Audit Manager Funktion verwenden, um Ihre benutzerdefinierten Frameworks schnell AWS-Konten und regional gemeinsam zu nutzen. Um ein benutzerdefiniertes Framework gemeinsam zu nutzen, erstellen Sie eine Freigabeanfrage. Der Empfänger hat dann 120 Tage Zeit, um die Anfrage anzunehmen

oder abzulehnen. Wenn er zustimmt, repliziert Audit Manager das gemeinsam genutzte benutzerdefinierte Framework in sein Framework-Bibliothek. Audit Manager repliziert nicht nur das benutzerdefinierte Framework, sondern auch alle benutzerdefinierten Kontrollsätze und Kontrollen, die in diesem Framework enthalten sind. Diese benutzerdefinierten Kontrollen werden der Kontrollbibliothek des Empfängers hinzugefügt. Audit Manager repliziert keine Standard-Frameworks oder -Kontrollen. Dies liegt daran, dass diese Ressourcen bereits standardmäßig in jedem Konto und jeder Region verfügbar sind.

I

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Unschlüssige Beweise

AWS Audit Manager kennzeichnet Beweise als nicht eindeutig, wenn eine automatisierte Compliance-Bewertung nicht möglich ist. Dies kann in folgenden Situationen auftreten:

- Sie haben AWS Config oder AWS Security Hub CSPM, das sind wichtige Datenquellen, nicht aktiviert.
- Beweise werden direkt von AWS Diensten über API-Aufrufe, AWS CloudTrail Protokolle oder manuelle Uploads gesammelt.

Wenn es keinen Mechanismus für die automatische Auswertung dieser Beweise gibt, AWS Audit Manager kann ich keine Bewertungsdetails bereitstellen. Infolgedessen werden die Beweise als nicht eindeutig eingestuft.

> **Important**
>
> Unschlüssige Beweise deuten nicht auf ein Versagen hin. Stattdessen signalisiert es, dass Sie die Nachweise manuell auf ihre Konformität hin auswerten müssen.

R

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Ressource

Eine Ressource ist ein Sachwert oder ein Informationsgut, das im Rahmen eines Audits bewertet wird. Zu den AWS Ressourcen gehören beispielsweise EC2 Amazon-Instances, Amazon RDS-Instances, Amazon S3-Buckets und Amazon VPC-Subnetze.

Bewertung der Ressourcen

Eine Ressourcenbewertung ist der Prozess der Bewertung einer einzelnen Ressource. Diese Bewertung basiert auf der Anforderung einer Kontrolle. Während eine Bewertung aktiv ist, führt Audit Manager Ressourcenbewertungen für jede einzelne Ressource im Rahmen der Bewertung durch. Bei einer Ressourcenbewertung werden die folgenden Aufgaben ausgeführt:

1. Sammelt Beweise wie Ressourcenkonfigurationen, Ereignisprotokolle und Ergebnisse
2. Übersetzt Beweise und ordnet sie den Kontrollen zu
3. Speichert und verfolgt die Herkunft der Beweise, um deren Integrität zu gewährleisten

Ressourcen-Compliance

Die Einhaltung der Ressourcen-Compliance bezieht sich auf den Bewertungsstatus einer Ressource, die bei der Erfassung von Beweisen zur Compliance-Überprüfung bewertet wurde.

Audit Manager sammelt Nachweise zur Konformitätsprüfung für Kontrollen, die Security Hub CSPM als Datenquellentyp verwenden AWS Config . Bei dieser Beweissuche können mehrere Ressourcen bewertet werden. Daher kann ein einziger Beweis für die Compliance-Überprüfung eine oder mehrere Ressourcen umfassen.

Sie können den Compliance-Filter für Ressourcen in der Beweissuche verwenden, um den Konformitätsstatus auf Ressourcenebene zu ermitteln. Nachdem Ihre Suche abgeschlossen ist, können Sie eine Vorschau der Ressourcen anzeigen, die Ihrer Suchabfrage entsprechen.

In der Beweissuche gibt es drei mögliche Werte für die Ressourcen-Compliance:

Wert	Description
Nicht konform	Dies bezieht sich auf Ressourcen mit Problemen bei der Konformitätsprüfung. Dies passiert, wenn Security Hub ein Fehlerergebnis für die Ressource AWS Config meldet oder wenn ein nicht konformes Ergebnis gemeldet wird.

Wert	Description
Konform	Dies bezieht sich auf Ressourcen, bei denen keine Probleme mit der Konformitätsprüfung aufgetreten sind. Dies passiert, wenn Security Hub CSPM ein Pass-Ergebnis für die Ressource AWS Config meldet oder wenn ein Compliance-Ergebnis gemeldet wird.
Nicht eindeutig	Dies bezieht sich auf Ressourcen, für die keine Konformitätsprüfung verfügbar oder anwendbar ist. Dies passiert, wenn AWS Config Security Hub CSPM der zugrunde liegende Datenquellentyp ist, diese Dienste jedoch nicht aktiviert sind. Dies ist auch der Fall, wenn der zugrunde liegende Datenquellentyp keine Konformitätsprüfungen unterstützt (z. B. manuelle Nachweise, AWS API-Aufrufe oder CloudTrail).

S

| B | | | | | G | H | | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Leistung im Umfang

Der Audit Manager verwaltet, AWS-Services welche Punkte für Ihre Bewertungen gelten. Wenn Sie ein älteres Assessment haben, ist es möglich, dass Sie die in den Geltungsbereich fallenden Services in der Vergangenheit manuell festgelegt haben. Nach dem 04. Juni 2024 können Sie die Services im Geltungsbereich nicht mehr manuell angeben oder bearbeiten.

Ein Service im Geltungsbereich ist ein Service AWS-Service , für den in Ihrer Bewertung Belege gesammelt werden. Wenn ein Service in den Umfang Ihrer Bewertung aufgenommen wird, bewertet Audit Manager die Ressourcen dieses Dienstes. Zu den Beispielressourcen gehören:

- Eine EC2 Amazon-Instanz
- Ein S3-Bucket
- Ein IAM-Benutzer oder eine IAM-Rolle
- Eine DynamoDB-Tabelle

- Eine Netzwerkkomponente wie eine Amazon Virtual Private Cloud (VPC)-Sicherheitsgruppe oder eine Netzwerk-Zugriffskontrollliste (Access Control List, ACL)

Wenn Amazon S3 beispielsweise ein Service im Leistungsumfang ist, kann Audit Manager Nachweise über Ihre S3-Buckets sammeln. Die genauen Beweise, die gesammelt werden, werden von einer Kontrolle bestimmt. data source Wenn der Datenquellentyp beispielsweise ist AWS Config und es sich bei der Datenquellenzuordnung um eine AWS Config Regel handelt (z. B.`s3-bucket-public-write-prohibited`), erfasst Audit Manager das Ergebnis dieser Regelauswertung als Nachweis.

> **Note**
>
> Beachten Sie, dass sich der Umfang eines Dienstes von einem Datenquellentyp unterscheidet, der auch ein AWS-Service oder etwas anderes sein kann. Weitere Informationen finden Sie Was ist der Unterschied zwischen einem Service im Umfang und einem Datenquellentyp? im Abschnitt Problembehandlung dieses Handbuchs.

Standardsteuerung

Siehe control.

Verstehen, wie Beweise AWS Audit Manager gesammelt werden

Bei jeder aktiven Bewertung AWS Audit Manager werden automatisch Beweise aus einer Reihe von Datenquellen gesammelt. In jeder Bewertung legen Sie fest, für welchen AWS-Konten Audit Manager Beweise sammelt, und der Audit Manager verwaltet, welche davon betroffen AWS-Services sind. Jeder dieser Dienste und Konten enthält mehrere Ressourcen, die Sie besitzen und nutzen. Die Erfassung von Beweisen in Audit Manager umfasst die Bewertung jeder einzelnen Ressource, die in den Anwendungsbereich fällt. Dies wird als Ressourcenbewertung bezeichnet.

In den folgenden Schritten wird beschrieben, wie Audit Manager Beweise für jede Ressourcenbewertung sammelt:

1. Bewertung einer Ressource anhand der Datenquelle

Um mit der Beweissuche zu beginnen, bewertet Audit Manager eine im Umfang enthaltene Ressource anhand einer Datenquelle. Zu diesem Zweck werden ein Konfigurations-Snapshot,

ein entsprechendes Ergebnis der Konformitätsprüfung oder Benutzeraktivitäten aufgezeichnet. Anschließend wird eine Analyse durchgeführt, um festzustellen, welche Kontrolle diese Daten unterstützen. Das Ergebnis der Ressourcenbewertung wird dann gespeichert und in Beweise umgewandelt. Weitere Informationen zu den verschiedenen Arten von Nachweisen finden Sie evidence im Abschnitt AWS Audit Manager Konzepte und Terminologie dieses Handbuchs.

2. Umwandlung von Bewertungsergebnissen in Beweise

Das Ergebnis der Ressourcenbewertung enthält sowohl die Originaldaten, die aus dieser Ressource erfasst wurden, als auch die Metadaten, die angeben, welche Steuerung die Daten unterstützen. Audit Manager konvertiert die Originaldaten in ein prüferfreundliches Format. Die konvertierten Daten und Metadaten werden dann als Audit Manager-Beweise gespeichert, bevor sie an eine Kontrolle angehängt werden.

3. Beweise an die zugehörige Kontrolle anhängen

Audit Manager liest die Metadaten der Beweise. Anschließend fügt er die gespeicherten Beweise einer entsprechenden Kontrolle innerhalb der Bewertung hinzu. Die beigefügten Beweise werden im Audit Manager sichtbar. Damit ist der Zyklus der Ressourcenbewertung abgeschlossen.

> **Note**
>
> Abhängig von den Kontrollkonfigurationen können dieselben Beweise in einigen Fällen mehreren Kontrollen aus mehreren Audit Manager-Bewertungen beigefügt werden. Wenn dieselben Beweise mehreren Kontrollen beigefügt werden, misst Audit Manager die Ressourcenbewertung genau einmal. Das liegt daran, dass dieselben Beweise nur einmal gesammelt werden. Eine Kontrolle in einer Audit Manager-Bewertung kann jedoch mehrere Beweise aus mehreren Datenquellen enthalten.

Häufigkeit der Beweissuche

Die Erhebung von Beweisen ist ein fortlaufender Prozess, der mit der Erstellung Ihrer Bewertung beginnt. Audit Manager sammelt Beweise aus mehreren Datenquellen mit unterschiedlichen Frequenzen. Daher gibt es keine one-size-fits-all Antwort darauf, wie oft Beweise gesammelt werden. Die Häufigkeit der Beweissuche hängt von der Art der Beweise und ihrer Datenquelle ab, wie unten beschrieben.

- Konformitätsprüfungen — Audit Manager sammelt diese Art von Nachweisen von AWS Security Hub CSPM und AWS Config.
  - Für Security Hub CSPM folgt die Beweiserhebung dem Zeitplan Ihrer Security Hub CSPM-Prüfungen. Weitere Informationen zum Zeitplan der Security Hub CSPM-Prüfungen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen im AWS Security Hub CSPM Benutzerhandbuch. Weitere Informationen zu den von Audit Manager unterstützten Security Hub CSPM-Prüfungen finden Sie unter. AWS Security Hub CSPM Steuerelemente, die unterstützt werden von AWS Audit Manager
  - Denn die AWS Config Erfassung von Nachweisen folgt den Auslösern, die in Ihren AWS Config Regeln definiert sind. Weitere Informationen zu den Auslösern für AWS Config -Regeln finden Sie unter Triggertypen im AWS Config -Benutzerhandbuch. Weitere Informationen zu den AWS-Config-Regeln , die von Audit Manager unterstützt werden, finden Sie unterAWS-Config-Regeln unterstützt von AWS Audit Manager.
  - AWS Audit Manager kennzeichnet Beweise als nicht eindeutig, wenn eine automatisierte Compliance-Bewertung nicht möglich ist. Dies ist der Fall, wenn Sie AWS Config oder AWS Security Hub CSPM, was wichtige Datenquellen sind, nicht aktiviert haben. Es passiert auch, wenn Beweise direkt von AWS Diensten über API-Aufrufe, AWS CloudTrail Protokolle oder manuelle Uploads gesammelt werden. Wenn es keinen Mechanismus für die automatische Auswertung dieser Beweise gibt, AWS Audit Manager können keine Bewertungsdetails bereitgestellt werden. Infolgedessen werden die Beweise als nicht eindeutig eingestuft. Unschlüssige Beweise deuten nicht auf ein Scheitern hin. Stattdessen signalisiert es, dass Sie die Nachweise manuell auf ihre Konformität hin auswerten müssen.
- Benutzeraktivität — Audit Manager sammelt diese Art von AWS CloudTrail Nachweisen kontinuierlich. Diese Häufigkeit ist kontinuierlich, da Benutzeraktivitäten zu jeder Tageszeit auftreten können. Weitere Informationen finden Sie unter AWS CloudTrail Eventnamen werden unterstützt von AWS Audit Manager.
- Konfigurationsdaten — Audit Manager erfasst diesen Nachweistyp mithilfe eines Describe-API-Aufrufs an einen anderen AWS-Service wie Amazon EC2, Amazon S3 oder IAM. Sie können wählen, welche API-Aktionen aufgerufen werden sollen. Sie legen die Häufigkeit im Audit Manager auch als täglich, wöchentlich oder monatlich fest. Sie können dieses Intervall angeben, wenn Sie eine Kontrolle in der Kontrollenbibliothek erstellen oder bearbeiten. Anweisungen zum Bearbeiten und Erstellen von Kontrollen finden Sie unter Verwenden der Steuerbibliothek zur Verwaltung von Steuerelementen in AWS Audit Manager. Weitere Informationen zu den API-Aufrufen, die von Audit Manager unterstützt werden, finden Sie unterAWS API-Aufrufe werden unterstützt von AWS Audit Manager.

Unabhängig von der Häufigkeit der Beweissuche für die Datenquelle werden neue Beweise automatisch erfasst, solange die Kontrolle und die Bewertung aktiv sind.

Beispiele für AWS Audit Manager Steuerelemente

Sie können sich die Beispiele auf dieser Seite ansehen, um mehr darüber zu erfahren, wie Kontrollen in AWS Audit Manager funktionieren.

In Audit Manager können Steuerelemente automatisch Beweise aus vier Datenquellentypen sammeln:

1. AWS CloudTrail— Erfassen Sie Benutzeraktivitäten aus Ihren CloudTrail Protokollen und importieren Sie sie als Nachweis für Benutzeraktivitäten
2. AWS Security Hub CSPM— Sammeln Sie Ergebnisse aus Security Hub CSPM und importieren Sie sie als Nachweis für die Konformitätsprüfung
3. AWS Config— Sammeln Sie Regelbewertungen von AWS Config und importieren Sie sie als Nachweis für die Konformitätsprüfung
4. AWS API-Aufrufe — Erfassen Sie einen Ressourcen-Snapshot aus einem API-Aufruf und importieren Sie ihn als Nachweis für Konfigurationsdaten

Beachten Sie, dass einige Kontrollen Beweise mithilfe vordefinierter Gruppierungen dieser Datenquellen sammeln. Diese Datenquellengruppierungen werden als AWS verwaltete Quellen bezeichnet. Jede AWS verwaltete Quelle stellt entweder ein gemeinsames Steuerelement oder ein zentrales Steuerelement dar. Diese verwalteten Quellen bieten Ihnen eine effiziente Möglichkeit, Ihre Compliance-Anforderungen einer relevanten Gruppe von zugrunde liegenden Datenquellen zuzuordnen, die von branchenweit zertifizierten Prüfern in AWS validiert und verwaltet werden.

Die Beispiele auf dieser Seite zeigen, wie Kontrollen Nachweise aus den einzelnen Datenquellentypen sammeln. Sie beschreiben, wie eine Kontrolle aussieht, wie Audit Manager Beweise aus der Datenquelle sammelt und welche nächsten Schritte Sie unternehmen können, um die Einhaltung der Vorschriften nachzuweisen.

> **Tip**
>
> Wir empfehlen, dass Sie Security Hub CSPM aktivieren AWS Config , um Audit Manager optimal nutzen zu können. Wenn Sie diese Dienste aktivieren, kann Audit Manager die

CSPM-Ergebnisse von Security Hub verwenden und automatisierte AWS-Config-Regeln Beweise generieren.

- Stellen Sie nach der Aktivierung von AWS Security Hub CSPM sicher, dass Sie auch alle Sicherheitsstandards aktivieren und die Einstellung für konsolidierte Kontrollergebnisse aktivieren. Dieser Schritt stellt sicher, dass Audit Manager Ergebnisse für alle unterstützten Compliance-Standards importieren kann.
- Stellen Sie nach der Aktivierung sicher AWS Config, dass Sie auch die entsprechenden Optionen aktivieren, AWS-Config-Regeln oder stellen Sie ein Konformitätspaket für den Compliance-Standard bereit, der sich auf Ihr Audit bezieht. Dieser Schritt stellt sicher, dass Audit Manager Ergebnisse für alle unterstützten AWS-Config-Regeln , die Sie aktiviert haben, importieren kann.

Beispiele sind für jeden der folgenden Kontrolltypen verfügbar:

Themen

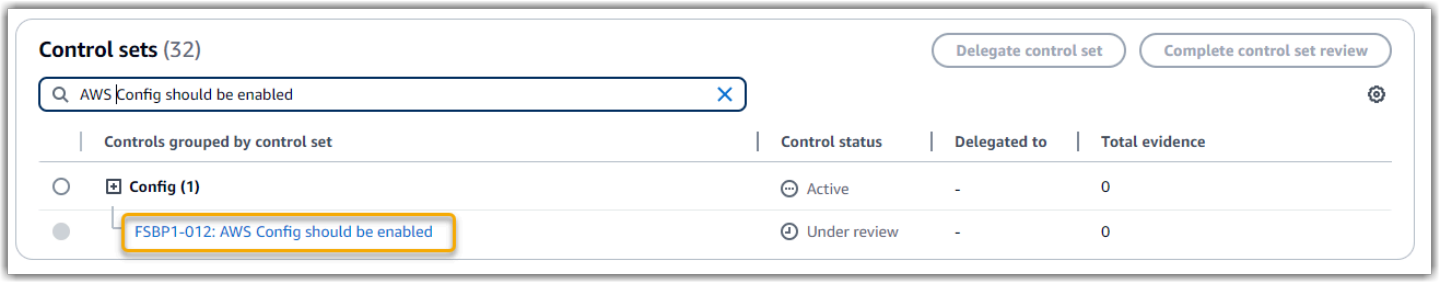
Automatisierte Steuerelemente, die AWS Security Hub CSPM als Datenquellentyp verwendet werden

Dieses Beispiel zeigt ein Steuerelement, das AWS Security Hub CSPM als Datenquellentyp verwendet wird. Dies ist eine Standardkontrolle, die dem AWS FSBP-Framework (Foundational Security Best Practices) entnommen wurde. Audit Manager verwendet diese Kontrolle, um Nachweise zu generieren, die dazu beitragen können, Ihre AWS Umgebung mit den FSBP-Anforderungen in Einklang zu bringen.

Beispiel für Kontrolldetails

- Name der Kontrolle – `FSBP1-012: AWS Config should be enabled`
- Kontrollsatz —`Config`. Dies ist eine Framework-spezifische Gruppierung von FSBP-Steuerelementen, die sich auf das Konfigurationsmanagement beziehen.
- Evidenzquelle — Einzelne Datenquellen
- Typ der Datenquelle — AWS Security Hub CSPM
- Art des Beweises – Compliance-Überprüfung

Im folgenden Beispiel erscheint dieses Steuerelement in einer Audit Manager Manager-Bewertung, die mit dem FSBP-Framework erstellt wurde.



Die Bewertung zeigt den Kontrollstatus. Es zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden. Von hier aus können Sie den Kontrollsatz zur Überprüfung delegieren oder die Prüfung selbst abschließen. Wenn Sie den Kontrollnamen wählen, wird eine Detailseite mit weiteren Informationen geöffnet, einschließlich der Beweise für diese Kontrolle.

Was macht diese Kontrolle

Diese Steuerung setzt voraus, dass sie überall aktiviert AWS Config ist AWS-Regionen , wo Sie Security Hub CSPM verwenden. Audit Manager kann dieses Steuerelement verwenden, um zu überprüfen, ob Sie es aktiviert haben AWS Config.

Wie Audit Manager Beweise für diese Kontrolle sammelt

Audit Manager unternimmt die folgenden Schritte, um Beweise für diese Kontrolle zu sammeln:

1. Für jede Kontrolle bewertet der Audit Manager Ihre in den Umfang fallenden Ressourcen. Dabei wird die Datenquelle verwendet, die in den Kontrolleinstellungen angegeben ist. In diesem Beispiel sind Ihre AWS Config Einstellungen die Ressource und Security Hub CSPM der Datenquellentyp. Audit Manager sucht nach dem Ergebnis einer bestimmten Security Hub CSPM-Prüfung ([Config.1]).

2. Das Ergebnis der Ressourcenbewertung wird gespeichert und in prüferfreundliche Beweise umgewandelt. Audit Manager generiert Konformitätsprüfungsnachweise für Kontrollen, die Security Hub CSPM als Datenquellentyp verwenden. Dieser Nachweis enthält das Ergebnis der Konformitätsprüfung, die direkt vom Security Hub CSPM gemeldet wurde.
3. Audit Manager fügt die gespeicherten Beweise der Kontrolle mit dem Namen `FSBP1-012: AWS Config should be enabled` in Ihrer Bewertung hinzu.

Wie Sie Audit Manager verwenden können, um die Einhaltung dieser Kontrolle nachzuweisen

Nachdem die Beweise der Kontrolle beigefügt wurden, können Sie – oder ein Beauftragter Ihrer Wahl – die Beweise überprüfen, um festzustellen, ob Abhilfemaßnahmen erforderlich sind.

In diesem Beispiel zeigt Audit Manager möglicherweise eine Fail-Regel von Security Hub CSPM an. Dies kann passieren, wenn Sie es nicht aktiviert haben. AWS Config In diesem Fall können Sie die Aktivierung als Korrekturmaßnahme ergreifen AWS Config, um Ihre AWS Umgebung an die FSBP-Anforderungen anzupassen.

Wenn Ihre AWS Config Einstellungen mit der Kontrolle übereinstimmen, markieren Sie die Kontrolle als Überprüft und fügen Sie die Beweise Ihrem Bewertungsbericht hinzu. Sie können diesen Bericht dann an die Prüfer weitergeben, um nachzuweisen, dass die Kontrolle wie beabsichtigt funktioniert.

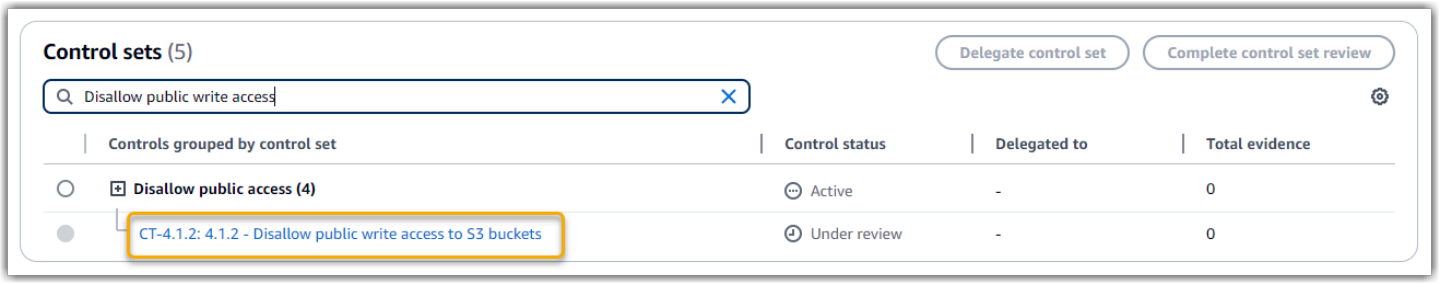
Automatisierte Steuerelemente, die AWS Config als Datenquellentyp verwendet werden

Dieses Beispiel zeigt ein Steuerelement, das AWS Config als Datenquellentyp verwendet wird. Dies ist eine Standardkontrolle aus dem AWS Control Tower Guardrails-Framework. Audit Manager verwendet diese Kontrolle, um Nachweise zu generieren, die dazu beitragen, Ihre AWS Umgebung mit AWS Control Tower Guardrails in Einklang zu bringen.

Beispiel für Kontrolldetails

- Name der Kontrolle – `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`
- Kontrollsatz – Diese Kontrolle gehört zum Kontrollsatz `Disallow public access`. Dies ist eine Gruppierung von Kontrollen, die sich auf die Zugriffsverwaltung beziehen.
- Quelle der Beweise — Individuelle Datenquelle
- Typ der Datenquelle — AWS Config
- Art des Beweises – Compliance-Überprüfung

Im folgenden Beispiel erscheint dieses Steuerelement in einer Audit Manager Manager-Bewertung, die mit dem AWS Control Tower Guardrails-Framework erstellt wurde.



Die Bewertung zeigt den Kontrollstatus. Es zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden. Von hier aus können Sie den Kontrollsatz zur Überprüfung delegieren oder die Prüfung selbst abschließen. Wenn Sie den Kontrollnamen wählen, wird eine Detailseite mit weiteren Informationen geöffnet, einschließlich der Beweise für diese Kontrolle.

Was macht diese Kontrolle

Audit Manager kann diese Kontrolle verwenden, um zu überprüfen, ob die Zugriffsebenen Ihrer S3-Bucket-Richtlinien zu gering sind, um die Anforderungen zu erfüllen AWS Control Tower . Insbesondere kann er die Einstellungen für den öffentlichen Zugriff blockieren, die Bucket-Richtlinien und die Bucket-Zugriffskontrolllisten (Access Control Lists, ACL) überprüfen, um sicherzustellen, dass Ihre Buckets keinen öffentlichen Schreibzugriff zulassen.

Wie Audit Manager Beweise für diese Kontrolle sammelt

Audit Manager unternimmt die folgenden Schritte, um Beweise für diese Kontrolle zu sammeln:

1. Für jede Kontrolle bewertet Audit Manager Ihre Ressourcen im Umfang anhand der Datenquelle, die in den Kontrolleinstellungen angegeben ist. In diesem Fall sind Ihre S3-Buckets die Ressource und AWS Config ist der Datenquellentyp. Audit Manager sucht nach dem Ergebnis einer bestimmten AWS Config Regel (s3- bucket-public-write-prohibited), um die Einstellungen, Richtlinien und ACL der einzelnen S3-Buckets zu bewerten, die in den Geltungsbereich Ihrer Bewertung fallen.
2. Das Ergebnis der Ressourcenbewertung wird gespeichert und in prüferfreundliche Beweise umgewandelt. Audit Manager generiert Nachweise zur Konformitätsprüfung für Kontrollen, die AWS Config als Datenquellentyp verwendet werden. Diese Nachweise enthalten das Ergebnis der Konformitätsprüfung, über die direkt von berichtet wurde AWS Config.
3. Audit Manager fügt die gespeicherten Beweise der Kontrolle mit dem Namen `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets` in Ihrer Bewertung hinzu.

Wie Sie Audit Manager verwenden können, um die Einhaltung dieser Kontrolle nachzuweisen

Nachdem die Beweise der Kontrolle beigefügt wurden, können Sie – oder ein Beauftragter Ihrer Wahl – die Beweise überprüfen, um festzustellen, ob Abhilfemaßnahmen erforderlich sind.

In diesem Beispiel zeigt Audit Manager möglicherweise eine Entscheidung an, die AWS Config besagt, dass ein S3-Bucket nicht konform ist. Dies kann passieren, wenn einer Ihrer S3-Buckets über die Einstellung „Öffentlichen Zugriff blockieren“ verfügt, die öffentliche Richtlinien nicht einschränkt, und die verwendete Richtlinie öffentlichen Schreibzugriff erlaubt. Um dies zu beheben, können Sie die Einstellung „Öffentlichen Zugriff blockieren“ aktualisieren, um öffentliche Richtlinien einzuschränken. Sie können auch eine andere Bucket-Richtlinie verwenden, die keinen öffentlichen Schreibzugriff zulässt. Diese Korrekturmaßnahme trägt dazu bei, Ihre AWS Umgebung an die Anforderungen anzupassen. AWS Control Tower

Wenn Sie sich davon überzeugt haben, dass Ihre S3-Bucket-Zugriffsebenen der Kontrolle entsprechen, können Sie die Kontrolle als überprüft markieren und die Beweise Ihrem Bewertungsbericht hinzufügen. Sie können diesen Bericht dann an die Prüfer weitergeben, um nachzuweisen, dass die Kontrolle wie beabsichtigt funktioniert.

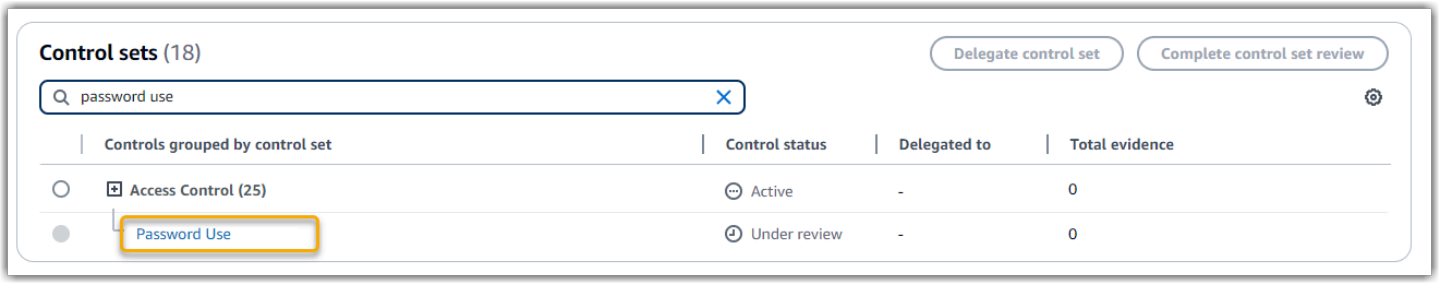
Automatisierte Steuerelemente, die AWS API-Aufrufe als Datenquellentyp verwenden

Dieses Beispiel zeigt ein benutzerdefiniertes Steuerelement, das AWS API-Aufrufe als Datenquellentyp verwendet. Audit Manager verwendet diese Kontrolle, um Nachweise zu generieren, die dazu beitragen können, Ihre AWS Umgebung an Ihre spezifischen Anforderungen anzupassen.

Beispiel für Kontrolldetails

- Name der Kontrolle – `Password Use`
- Kontrollsatz – Diese Kontrolle gehört zu einem Kontrollsatz, der `Access Control` heißt. Dies ist eine Gruppierung von Kontrollen, die sich auf die Identitäts- und Zugriffsverwaltung beziehen.
- Quelle der Nachweise — Individuelle Datenquelle
- Datenquellentyp — AWS API-Aufrufe
- Art des Beweises – Konfigurationsdaten

Im folgenden Beispiel erscheint dieses Steuerelement in einer Audit Manager Manager-Bewertung, die mit einem benutzerdefinierten Framework erstellt wurde.



Die Bewertung zeigt den Kontrollstatus. Es zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden. Von hier aus können Sie den Kontrollsatz zur Überprüfung delegieren oder die Prüfung selbst abschließen. Wenn Sie den Kontrollnamen wählen, wird eine Detailseite mit weiteren Informationen geöffnet, einschließlich der Beweise für diese Kontrolle.

Was macht diese Kontrolle

Audit Manager kann diese benutzerdefinierte Kontrolle verwenden, um sicherzustellen, dass Sie über ausreichende Zugriffskontrollrichtlinien verfügen. Diese Kontrolle setzt voraus, dass Sie bei der Auswahl und Verwendung von Passwörtern gute Sicherheitspraktiken einhalten. Audit Manager kann Ihnen dabei helfen, dies zu überprüfen, indem er eine Liste aller Passwortrichtlinien für die IAM-Prinzipale abruft, die in den Umfang Ihrer Bewertung fallen.

Wie Audit Manager Beweise für diese Kontrolle sammelt

Audit Manager führt die folgenden Schritte durch, um Beweise für diese benutzerdefinierte Kontrolle zu sammeln:

1. Für jede Kontrolle bewertet Audit Manager Ihre Ressourcen im Umfang anhand der Datenquelle, die in den Kontrolleinstellungen angegeben ist. In diesem Fall sind Ihre IAM-Prinzipale die Ressourcen und AWS API-Aufrufe der Datenquellentyp. Audit Manager sucht nach der Antwort auf einen bestimmten IAM-API-Aufruf (GetAccountPasswordPolicy). Anschließend werden die Kennwortrichtlinien für die AWS-Konten zurückgegeben, die in den Umfang Ihrer Bewertung fallen.
2. Das Ergebnis der Ressourcenbewertung wird gespeichert und in prüferfreundliche Beweise umgewandelt. Audit Manager generiert Konfigurationsdatennachweise für Kontrollen, die API-Aufrufe als Datenquelle verwenden. Diese Beweise enthalten die Originaldaten, die aus den API-Antworten erfasst wurden, sowie zusätzliche Metadaten, die angeben, welche Kontrolle die Daten unterstützt.
3. Audit Manager fügt die gespeicherten Beweise der benutzerdefinierten Kontrolle mit dem Namen `Password Use` in Ihrer Bewertung hinzu.

Wie Sie Audit Manager verwenden können, um die Einhaltung dieser Kontrolle nachzuweisen

Nachdem die Beweise der Kontrolle beigefügt wurden, können Sie – oder ein Beauftragter Ihrer Wahl – die Beweise überprüfen, um festzustellen, ob sie ausreichend sind oder ob Abhilfemaßnahmen erforderlich sind.

In diesem Beispiel können Sie die Beweise überprüfen, um die Antwort auf den API-Aufruf zu sehen. In der GetAccountPasswordPolicyAntwort werden die Komplexitätsanforderungen und die obligatorischen Rotationsperioden für die Benutzerkennwörter in Ihrem Konto beschrieben. Sie können diese API-Antwort als Nachweis verwenden, um nachzuweisen, dass Sie über ausreichende Richtlinien zur Passwortzugriffskontrolle für diejenigen verfügen AWS-Konten , die in den Rahmen Ihrer Bewertung fallen. Wenn Sie möchten, können Sie auch zusätzliche Kommentare zu diesen Richtlinien abgeben, indem Sie der Kontrolle einen Kommentar hinzufügen.

Wenn Sie davon überzeugt sind, dass die Passwortrichtlinien Ihrer IAM-Prinzipale mit der benutzerdefinierten Kontrolle übereinstimmen, können Sie die Kontrolle als überprüft markieren und die Beweise Ihrem Bewertungsbericht hinzufügen. Sie können diesen Bericht dann an die Prüfer weitergeben, um nachzuweisen, dass die Kontrolle wie beabsichtigt funktioniert.

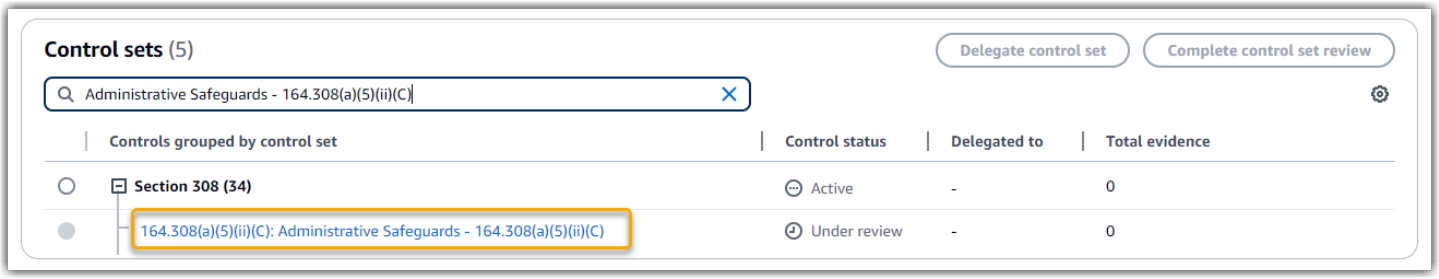
Automatisierte Steuerelemente, die AWS CloudTrail als Datenquellentyp verwendet werden

Dieses Beispiel zeigt ein Steuerelement, das AWS CloudTrail als Datenquellentyp verwendet wird. Dies ist ein Standardsteuerelement, das dem HIPAA Security Rule 2003-Framework entnommen wurde. Audit Manager verwendet diese Kontrolle, um Beweise zu generieren, die dazu beitragen können, Ihre AWS -Umgebung mit den HIPAA-Anforderungen in Einklang zu bringen.

Beispiel für Kontrolldetails

- Name der Kontrolle – `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`
- Kontrollsatz – Diese Kontrolle gehört zu dem Kontrollsatz, der aufgerufen wird`Section 308`. Dabei handelt es sich um eine rahmenspezifische Gruppierung von HIPAA-Kontrollen, die sich auf administrative Schutzmaßnahmen beziehen.
- Beweisquelle — AWS verwaltete Quelle (zentrale Kontrollen)
- Zugrundeliegender Datenquellentyp — AWS CloudTrail
- Art des Beweises – Benutzeraktivität

Diese Kontrolle wird in einer Audit Manager-Bewertung dargestellt, die auf der Grundlage des HIPAA-Frameworks erstellt wurde:



Die Bewertung zeigt den Kontrollstatus. Es zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden. Von hier aus können Sie den Kontrollsatz zur Überprüfung delegieren oder die Prüfung selbst abschließen. Wenn Sie den Kontrollnamen wählen, wird eine Detailseite mit weiteren Informationen geöffnet, einschließlich der Beweise für diese Kontrolle.

Was macht diese Kontrolle

Diese Kontrolle setzt voraus, dass Sie über Überwachungsverfahren verfügen, um unbefugten Zugriff zu erkennen. Ein Beispiel für unbefugten Zugriff ist, wenn sich jemand an der Konsole anmeldet, ohne dass die Multi-Faktor-Authentifizierung (MFA) aktiviert ist. Audit Manager hilft Ihnen bei der Validierung dieser Kontrolle, indem es den Nachweis liefert, dass Sie Amazon so konfiguriert haben CloudWatch , dass es Anmeldeanfragen für die Managementkonsole überwacht, bei denen MFA nicht aktiviert ist.

Wie Audit Manager Beweise für diese Kontrolle sammelt

Audit Manager unternimmt die folgenden Schritte, um Beweise für diese Kontrolle zu sammeln:

1. Für jede Kontrolle bewertet Audit Manager Ihre in den Geltungsbereich fallenden Ressourcen anhand der Nachweisquellen, die in den Kontrolleinstellungen angegeben sind. In diesem Fall verwendet die Kontrolle mehrere zentrale Kontrollen als Beweisquellen.

   Jede Kernkontrolle ist eine verwaltete Gruppierung einzelner Datenquellen. In unserem Beispiel verwendet eines dieser Kernsteuerelemente (`Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled`) ein CloudTrail Ereignis (`monitoring_EnableAlarmActions`) als zugrunde liegende Datenquelle.

   Audit Manager überprüft Ihre CloudTrail Protokolle und verwendet das `monitoring_EnableAlarmActions` Schlüsselwort, um CloudWatch alarmaktivierende

Aktionen zu finden, die protokolliert wurden CloudTrail. Anschließend wird ein Protokoll der relevanten Ereignisse zurückgegeben, die in den Umfang Ihrer Bewertung fallen.

2. Das Ergebnis der Ressourcenbewertung wird gespeichert und in prüferfreundliche Beweise umgewandelt. Audit Manager generiert Benutzeraktivitätsnachweise für Kontrollen, die CloudTrail als Datenquellentyp verwendet werden. Dieser Nachweis enthält die Originaldaten, die von Amazon erfasst wurden CloudWatch, und zusätzliche Metadaten, die angeben, welche Steuerung die Daten unterstützen.
3. Audit Manager fügt die gespeicherten Beweise der Kontrolle mit dem Namen `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)` in Ihrer Bewertung hinzu.

Wie Sie Audit Manager verwenden können, um die Einhaltung dieser Kontrolle nachzuweisen

Nachdem die Beweise der Kontrolle beigefügt wurden, können Sie – oder ein Beauftragter Ihrer Wahl – die Beweise überprüfen, um festzustellen, ob Abhilfemaßnahmen erforderlich sind.

In diesem Beispiel können Sie anhand der Nachweise feststellen, welche Alarmaktivierungsereignisse protokolliert wurden. CloudTrail Sie können dieses Protokoll als Nachweis verwenden, um nachzuweisen, dass Sie über ausreichende Überwachungsverfahren verfügen, um zu erkennen, ob Konsolenanmeldungen ohne aktiviertes MFA erfolgen. Wenn Sie möchten, können Sie auch zusätzliche Kommentare abgeben, indem Sie der Kontrolle einen Kommentar hinzufügen. Wenn das Protokoll beispielsweise mehrere Anmeldungen ohne MFA anzeigt, können Sie einen Kommentar hinzufügen, der beschreibt, wie Sie das Problem behoben haben. Durch die regelmäßige Überwachung der Konsolenanmeldungen können Sie Sicherheitsprobleme vermeiden, die sich aus Diskrepanzen und unangemessenen Anmeldeversuchen ergeben können. Diese bewährte Methode trägt wiederum dazu bei, Ihre AWS Umgebung mit den HIPAA-Anforderungen in Einklang zu bringen.

Wenn Sie davon überzeugt sind, dass Ihr Überwachungsverfahren mit der Kontrolle übereinstimmt, können Sie die Kontrolle als geprüft markieren und die Beweise Ihrem Bewertungsbericht hinzufügen. Sie können diesen Bericht dann an die Prüfer weitergeben, um nachzuweisen, dass die Kontrolle wie beabsichtigt funktioniert.

Manuelle Kontrollen

Einige Kontrollen unterstützen keine automatische Beweissuche. Dazu gehören Kontrollen, die auf der Bereitstellung physischer Aufzeichnungen und Unterschriften beruhen, sowie Beobachtungen, Interviews und andere Ereignisse, die nicht in der Cloud generiert werden. In diesen Fällen können

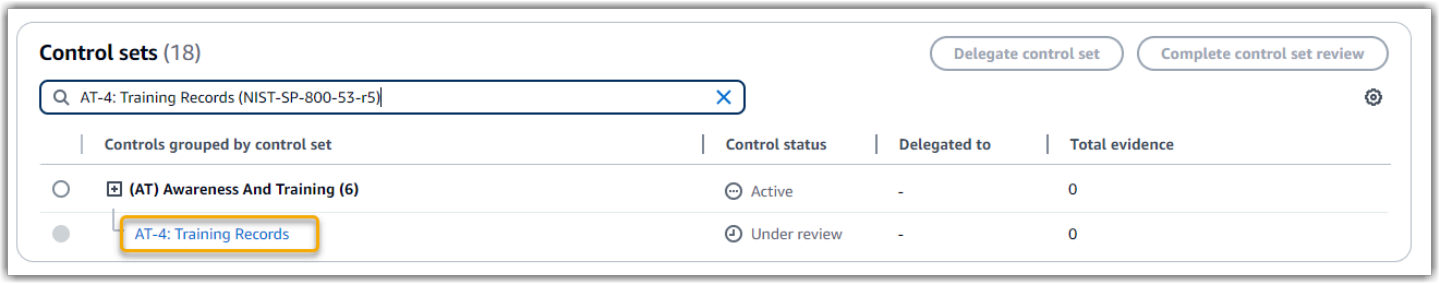
Sie manuell Beweise hochladen, um nachzuweisen, dass Sie die Anforderungen der Kontrolle erfüllen.

Dieses Beispiel zeigt eine manuelle Steuerung, die dem NIST 800-53 (Rev. 5) Framework entnommen wurde. Sie können Audit Manager verwenden, um Beweise hochzuladen und zu speichern, welche die Einhaltung dieser Kontrolle belegen.

Beispiel für Kontrolldetails

- Name der Kontrolle – `AT-4: Training Records`
- Steuersatz —. `(AT) Awareness and training` Dies ist eine rahmenspezifische Gruppierung von NIST-Kontrollen, die sich auf das Training beziehen.
- Evidenzquelle — Individuelle Datenquelle
- Datenquellentyp – Manuell
- Art des Beweises – Manuell

Diese Kontrolle wird in einer Audit Manager Manager-Bewertung dargestellt, die auf der Grundlage des NIST 800-53 (Rev. 5) -Frameworks erstellt wurde: Low-Moderate-High



Die Bewertung zeigt den Kontrollstatus. Es zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden. Von hier aus können Sie den Kontrollsatz zur Überprüfung delegieren oder die Prüfung selbst abschließen. Wenn Sie den Kontrollnamen wählen, wird eine Detailseite mit weiteren Informationen geöffnet, einschließlich der Beweise für diese Kontrolle.

Was macht diese Kontrolle

Sie können diese Kontrolle verwenden, um sicherzustellen, dass Ihr Personal ein angemessenes Maß an Sicherheits- und Datenschutzschulungen erhält. Insbesondere können Sie nachweisen, dass Sie für alle Mitarbeiter entsprechend ihrer Rolle dokumentierte Sicherheits- und Datenschutzschulungen eingerichtet haben. Sie können auch nachweisen, dass die Schulungsaufzeichnungen für jede einzelne Person aufbewahrt werden.

Wie können Sie Beweise für diese Kontrolle manuell hochladen

Informationen zum Hochladen manueller Nachweise, die die automatisierten Nachweise ergänzen, finden Sie unter Manuelle Nachweise hochladen in AWS Audit Manager. Audit Manager fügt die hochgeladenen Beweise der Kontrolle mit dem Namen `AT-4: Training Records` in Ihrer Bewertung hinzu.

Wie Sie Audit Manager verwenden können, um die Einhaltung dieser Kontrolle nachzuweisen

Wenn Sie über Unterlagen verfügen, die diese Kontrolle belegen, können Sie sie als manuellen Beweis hochladen. Sie können beispielsweise die neueste Kopie der vorgeschriebenen, rollenbasierten Schulungsmaterialien hochladen, die Ihre Personalabteilung an Mitarbeiter ausgibt.

Ähnlich wie bei automatisierten Kontrollen können Sie manuelle Kontrollen an Beteiligte delegieren, die Ihnen bei der Überprüfung von Beweisen (oder in diesem Fall bei deren Vorlage) helfen können. Wenn Sie beispielsweise diese Kontrolle überprüfen, stellen Sie möglicherweise fest, dass Sie die Anforderungen nur teilweise erfüllen. Dies könnte der Fall sein, wenn Sie keine Kopie der Anwesenheitserfassung für Präsenzschulungen haben. Sie könnten die Kontrolle an einen Stakeholder aus der Personalabteilung delegieren, der dann eine Liste der Mitarbeiter hochladen kann, die an der Schulung teilgenommen haben.

Wenn Sie davon überzeugt sind, dass Sie den Anforderungen der Kontrolle entsprechen, können Sie die Kontrolle als geprüft markieren und die Beweise Ihrem Bewertungsbericht hinzufügen. Sie können diesen Bericht dann an die Prüfer weitergeben, um nachzuweisen, dass die Kontrolle wie beabsichtigt funktioniert.

Kontrollen mit gemischten Datenquellentypen (automatisiert und manuell)

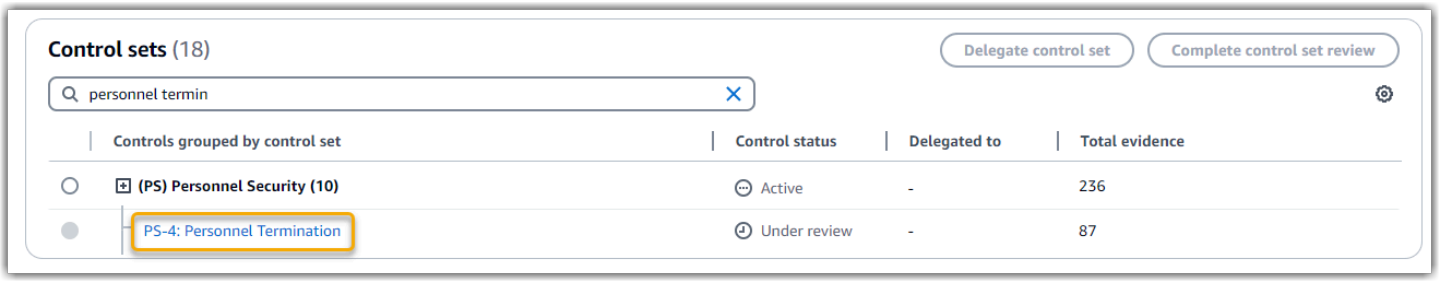
In vielen Fällen ist eine Kombination aus automatisierten und manuellen Beweisen erforderlich, um einer Kontrolle gerecht zu werden. Obwohl Audit Manager automatisierte Beweise bereitstellen kann, die für die Kontrolle relevant sind, müssen Sie diese Daten möglicherweise durch manuelle Beweise ergänzen, die Sie selbst identifizieren und hochladen.

Dieses Beispiel zeigt eine Kontrolle, die eine Kombination aus manuellen Nachweisen und automatisierten Nachweisen verwendet. Dies ist eine Standardkontrolle, die dem Framework NIST 800-53 (Rev. 5) entnommen wurde. Audit Manager verwendet diese Kontrolle, um Beweise zu generieren, die dazu beitragen können, Ihre AWS -Umgebung mit den NIST-Anforderungen in Einklang zu bringen.

Beispiel für Kontrolldetails

- Name der Kontrolle – `Personnel Termination`
- Kontrollsatz —`(PS) Personnel Security (10)`. Dies ist eine rahmenspezifische Gruppierung von NIST-Kontrollen, die sich auf Personen beziehen, die Hardware- oder Softwarewartungen an Organisationssystemen durchführen.
- Evidenzquelle — AWS verwaltete (zentrale Kontrollen) und individuelle Datenquellen (manuell)
- Zugrundeliegender Datenquellentyp — AWS API-Aufrufe, AWS CloudTrail, AWS Config, Manuell
- Art des Nachweises — Konfigurationsdaten, Benutzeraktivität, Konformitätsprüfung, manueller Nachweis)

Diese Kontrolle wird in einer Audit Manager-Bewertung dargestellt, die auf der Grundlage des NIST 800-53 (Rev. 5) -Frameworks erstellt wurde:



Die Bewertung zeigt den Kontrollstatus. Es zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden. Von hier aus können Sie den Kontrollsatz zur Überprüfung delegieren oder die Prüfung selbst abschließen. Wenn Sie den Kontrollnamen wählen, wird eine Detailseite mit weiteren Informationen geöffnet, einschließlich der Beweise für diese Kontrolle.

Was macht diese Kontrolle

Sie können dieses Steuerelement verwenden, um zu bestätigen, dass Sie Unternehmensinformationen schützen, falls ein Mitarbeiter entlassen wird. Insbesondere können Sie nachweisen, dass Sie den Systemzugriff deaktiviert und die Anmeldeinformationen für die Person widerrufen haben. Darüber hinaus können Sie nachweisen, dass alle gekündigten Personen an einem Austrittsgespräch teilgenommen haben, in dem auch die für Ihr Unternehmen relevanten Sicherheitsprotokolle erörtert wurden.

Wie Audit Manager Beweise für diese Kontrolle sammelt

Audit Manager unternimmt die folgenden Schritte, um Beweise für diese Kontrolle zu sammeln:

1. Für jede Kontrolle bewertet Audit Manager Ihre in den Geltungsbereich fallenden Ressourcen anhand der Nachweisquellen, die in den Kontrolleinstellungen angegeben sind.

   In diesem Fall verwendet die Kontrolle mehrere zentrale Kontrollen als Beweisquellen. Jede dieser Kernkontrollen sammelt wiederum relevante Nachweise aus einzelnen Datenquellen (AWS API-Aufrufe AWS CloudTrail, und AWS Config). Audit Manager verwendet diese Datenquellentypen, um Ihre IAM-Ressourcen (wie Gruppen, Schlüssel und Richtlinien) anhand der relevanten API-Aufrufe, CloudTrail Ereignisse und AWS Config Regeln zu bewerten.
2. Das Ergebnis der Ressourcenbewertung wird gespeichert und in prüferfreundliche Beweise umgewandelt. Diese Nachweise enthalten die Originaldaten, die aus jeder Datenquelle erfasst wurden, sowie zusätzliche Metadaten, die angeben, welche Steuerung die Daten unterstützen.
3. Audit Manager fügt die gespeicherten Beweise der Kontrolle mit dem Namen `Personnel Termination` in Ihrer Bewertung hinzu.

Wie können Sie Beweise für diese Kontrolle manuell hochladen

Informationen zum Hochladen manueller Nachweise, die die automatisierten Nachweise ergänzen, finden Sie unter Manuelle Nachweise hochladen in AWS Audit Manager. Audit Manager fügt die hochgeladenen Beweise der Kontrolle mit dem Namen `Personnel Termination` in Ihrer Bewertung hinzu.

Wie Sie Audit Manager verwenden können, um die Einhaltung dieser Kontrolle nachzuweisen

Nachdem die Beweise der Kontrolle beigefügt wurden, können Sie – oder ein Beauftragter Ihrer Wahl – die Beweise überprüfen, um festzustellen, ob sie ausreichend sind oder ob Abhilfemaßnahmen erforderlich sind. Wenn Sie beispielsweise diese Kontrolle überprüfen, stellen Sie möglicherweise fest, dass Sie die Anforderungen nur teilweise erfüllen. Dies kann der Fall sein, wenn Sie den Nachweis haben, dass der Zugriff gesperrt wurde, aber keine Kopie von Ausreisegesprächen haben. Sie könnten die Kontrolle an einen Mitarbeiter aus der Personalabteilung delegieren, der dann eine Kopie der Unterlagen zum Austrittsgespräch hochladen kann. Oder, falls während des Prüfungszeitraums keinem Mitarbeiter gekündigt wurde, können Sie einen Kommentar hinterlassen, aus dem hervorgeht, warum der Kontrolle keine unterschriebenen Unterlagen beigefügt wurden.

Wenn Sie davon überzeugt sind, dass Sie die Anforderungen der Kontrolle erfüllen, markieren Sie die Kontrolle als überprüft und fügen Sie die Beweise Ihrem Bewertungsbericht hinzu. Sie können diesen Bericht dann an die Prüfer weitergeben, um nachzuweisen, dass die Kontrolle wie beabsichtigt funktioniert.

Verwenden AWS Audit Manager

Sie können je nach Ihren spezifischen Bedürfnissen und Vorlieben AWS Audit Manager über verschiedene Optionen darauf zugreifen. Hier sind einige verschiedene Möglichkeiten, wie Sie mit Audit Manager interagieren können:

- Audit Manager Manager-Konsole

  Greifen Sie direkt von zu https://console.aws.amazon.com/auditmanager/Hause aus auf die Audit Manager Manager-Konsole zu, die eine benutzerfreundliche Oberfläche für die Verwaltung Ihrer Audits und der zugehörigen Ressourcen bietet.

- Audit-Manager-API

  Interagieren Sie programmgesteuert mit Audit Manager über die Audit Manager Manager-API, sodass Sie Aufgaben automatisieren und in Ihre bestehenden Workflows integrieren können. Weitere Informationen finden Sie in der AWS Audit Manager -API-Referenz.

- AWS SDKs

  Verwenden Sie AWS Software Development Kits (SDKs), um programmgesteuert mit Audit Manager zu interagieren, sodass Sie Code in verschiedenen Programmiersprachen schreiben können. Weitere Informationen finden Sie unter Verwendung AWS Audit Manager mit einem SDK AWS.

- AWS CloudFormation

  Erstellen Sie Audit Manager Manager-Ressourcen mithilfe von AWS CloudFormation, mit denen Sie Ihre Auditing-Infrastruktur als Code definieren und bereitstellen können. Weitere Informationen finden Sie unter Erstellen von AWS Audit Manager Manager-Ressourcen mit AWS CloudFormation.

- Integrationen von Drittanbietern

  Integrieren Sie Audit Manager in unterstützte GRC-Produkte (Governance, Risk, and Compliance) von Drittanbietern, sodass Sie bestehende GRC-Tools und -Prozesse nutzen können. Weitere Informationen finden Sie unter Integrationen mit GRC-Drittanbieterprodukten.

- Integrationen mit Ihrem eigenen GRC-System

Integrieren Sie Audit Manager-Nachweise in Ihr eigenes GRC-System, sodass Sie Belege direkt aus Audit Manager in Ihre GRC-Anwendung senden können. Weitere Informationen finden Sie unter Integration von Audit Manager Manager-Nachweisen in Ihr GRC-System.

Verwendung AWS Audit Manager mit einem SDK AWS

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Spezielle Dokumentation für den Audit Manager	Codebeispiele	
AWS SDK für C++	AWS SDK für C++ API-Referenz für Audit Manager	AWS SDK für C++ Codebeispiele	
AWS SDK für Go	AWS SDK für Go API-Referenz für Audit Manager	AWS SDK für Go Codebeispiele	
AWS SDK für Java	AWS SDK for Java 2.x API-Referenz für Audit Manager	AWS SDK für Java Codebeispiele	
AWS SDK für JavaScript	AWS SDK für JavaScript API-Referenz für Audit Manager	AWS SDK für JavaScript Codebeispiele	
AWS SDK für .NET	AWS SDK für .NET API-Referenz für Audit Manager	AWS SDK für .NET Codebeispiele	
AWS SDK für PHP	AWS SDK für PHP API-Referenz für Audit Manager	AWS SDK für PHP Codebeispiele	
AWS SDK für Python (Boto3)	AWS SDK für Python (Boto) API-Referenz für Audit Manager	AWS SDK für Python (Boto3) Codebeispiele	
AWS SDK für Ruby	AWS SDK für Ruby API-Referenz für Audit Manager	AWS SDK für Ruby Codebeispiele	

Beispiele, die spezifisch für Audit Manager sind, finden Sie unter Codebeispiele für die Verwendung von Audit Manager AWS SDKs.

> **Note**
>
> Audit Manager ist in der Botocore-Version 1.19.32 und höher für AWS SDK für Python (Boto3) verfügbar. Stellen Sie vor der Verwendung des SDK sicher, dass Sie die entsprechende Botocore-Version verwenden.

Erstellen von AWS Audit Manager Manager-Ressourcen mit AWS CloudFormation

AWS Audit Manager ist in einen Service integriert AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. Bewertungen) und diese Ressourcen für Sie CloudFormation bereitstellt und konfiguriert.

Wenn Sie sie verwenden CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre AWS Audit Manager Manager-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder für mehrere AWS Konten und Regionen bereit.

AWS Audit Manager und CloudFormation Vorlagen

Um Ressourcen für AWS Audit Manager und verwandte Services bereitzustellen und zu konfigurieren, müssen Sie CloudFormation Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. CloudFormation Weitere Informationen finden Sie unter Was ist CloudFormation - Designer? im AWS CloudFormation -Benutzerhandbuch.

AWS Audit Manager unterstützt die Erstellung von Bewertungen in CloudFormation. Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für Bewertungen finden Sie in der AWS Audit Manager Referenz zum Ressourcentyp im AWS CloudFormation -Benutzerhandbuch.

Erfahren Sie mehr über CloudFormation

Weitere Informationen CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- CloudFormation API Reference
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Integrationen mit GRC-Drittanbieterprodukten

AWS Audit Manager unterstützt Integrationen mit den GRC-Produkten von Drittanbietern, die auf dieser Seite aufgeführt sind.

Wenn Ihr Unternehmen ein Hybrid-Cloud-Modell oder ein Multi-Cloud-Modell verwendet, verwenden Sie wahrscheinlich ein GRC-Produkt, um Beweise aus diesen Umgebungen zu verwalten. Wenn dieses Produkt in Audit Manager integriert ist, können Sie Nachweise über Ihre AWS Nutzung direkt in Ihre GRC-Umgebung abrufen. Dies vereinfacht die Verwaltung der Compliance mit Vorschriften, da Ihnen ein zentraler Ort zur Überprüfung und Korrektur von Beweisen zur Verfügung steht, während Sie sich auf Audits vorbereiten.

Auf dieser Seite finden Sie einen Überblick über die GRC-Produkte von Drittanbietern, die Beweise aus Audit Manager aufnehmen können. Sie können auch eine Referenz dazu sehen, welche Audit Manager-API-Aktionen Sie direkt in diesen Produkten ausführen können.

Themen

- Wie Integrationen von Drittanbietern mit Audit Manager funktionieren
- GRC-Partnerprodukte von Drittanbietern, die in Audit Manager integriert sind

Wie Integrationen von Drittanbietern mit Audit Manager funktionieren

GRC-Partner können den Audit Manager public verwenden APIs , um ihre Produkte in Audit Manager zu integrieren. Mit dieser Integration können Sie die Unternehmenskontrollen in Ihrer GRC-Umgebung den allgemeinen Kontrollen zuordnen, die Audit Manager bereitstellt.

> **Tip**
>
> Sie können Ihre Unternehmenskontrollen jeder Art von Audit Manager Manager-Kontrolle zuordnen. Wir empfehlen jedoch, allgemeine Kontrollen zu verwenden. Wenn Sie eine gemeinsame Kontrolle zuordnen, die Ihr Ziel repräsentiert, sammelt Audit Manager Nachweise aus einer vordefinierten Gruppe von Datenquellen, die von verwaltet wird AWS. Das bedeutet, dass Sie kein AWS Experte sein müssen, um zu wissen, welche Datenquellen die relevanten Beweise für Ihr Ziel sammeln.

Nachdem Sie diese einmalige Übung zur Kontrollzuweisung abgeschlossen haben, können Sie Audit Manager-Bewertungen direkt im GRC-Produkt erstellen. Diese Aktion startet die Erfassung von Nachweisen über Ihre AWS Nutzung. Sie können diese AWS Beweise dann zusammen mit den anderen Nachweisen, die in Ihrer Hybridumgebung gesammelt wurden, einsehen, und das alles im gleichen Kontext Ihrer Unternehmenskontrollen.

Beachten Sie bei der Verwendung einer Audit Manager-Integration mit einem GRC-Produkt eines Drittanbieters die folgenden Punkte:

- Integrationen sind für alle AWS-Regionen verfügbar, in denen Audit Manager unterstützt wird.
- Alle Audit Manager-Ressourcen, die Sie im GRC-Partnerprodukt erstellen, werden auch in Audit Manager wiedergegeben.
- Für Sie gelten zusätzlich zu den AWS Audit Manager -Preisen für das GRC-Produkt eines Drittanbieters auch dessen Preise.
- Die Beweise, die Audit Manager sammelt, sind unveränderlich. Beweise werden in GRC-Produkten von Drittanbietern genauso präsentiert wie auf der Audit Manager-Konsole. Wenn Sie jedoch eine Drittanbieter-Integration verwenden, können Sie diese Beweise möglicherweise verbessern, indem Sie in Ihren Berichten zusätzlichen Kontext angeben.
- Dieselben Kontingente, die für Audit Manager gelten, gelten auch für das GRC-Produkt eines Drittanbieters. Zum Beispiel AWS-Konto kann jeder bis zu 100 aktive Audit Manager-Bewertungen haben. Dieses Kontingent auf Kontoebene gilt unabhängig davon, ob Sie die Bewertungen in der Audit Manager-Konsole oder im GRC-Produkt eines Drittanbieters erstellen. Die meisten Audit Manager Manager-Kontingente, aber nicht alle, sind unter dem AWS Audit Manager Namespace in der Service Quotas Quotas-Konsole aufgeführt. Informationen zum Anfordern einer Kontingenterhöhung finden Sie unter Verwaltung Ihrer Audit Manager-Kontingente.

Wenn Sie über eine Compliance-Lösung verfügen und an einer Integration mit Audit Manager interessiert sind, senden Sie eine E-Mail an `auditmanager-partners@amazon.com`.

GRC-Partnerprodukte von Drittanbietern, die in Audit Manager integriert sind

Die folgenden GRC-Produkte von Drittanbietern können Beweise von Audit Manager aufnehmen.

MetricStream

Um diese Integration zu nutzen, wenden Sie MetricStreamsich an MetricStream GRC-Software und deren Kauf.

Die MetricStream Enterprise GRC-Lösung basiert auf der MetricStream Plattform und ermöglicht einen umfassenden und kooperativen Ansatz für unternehmensweite GRC-Aktivitäten und -Prozesse. Durch die Erfassung von Nachweisen aus Audit Manager können Sie proaktiv nicht konforme Nachweise aus Ihrer AWS Umgebung identifizieren und diese zusammen mit Nachweisen aus Ihren lokalen Datenquellen oder anderen Cloud-Partnern überprüfen. MetricStream Dies bietet Ihnen eine bequeme und zentrale Möglichkeit, Ihre Cloud-Sicherheit und Ihren Compliance-Status zu überprüfen und zu verbessern, während Sie sich auf Audits vorbereiten.

Mit der MetricStream und Audit Manager Manager-Integration können Sie die folgenden API-Operationen ausführen.

Aufgabe	API-Operation
Einrichtung der Audit Manager-Integration	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Überprüfung der Ressourcen von Audit Manager	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Erstellen von Ressourcen für den Audit Manager	• CreateAssessment • CreateAssessmentFramework

Aufgabe	API-Operation
Aktualisierung der Ressourcen von Audit Manager	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Verwaltung von Beweisen	• StartQuery(AWS CloudTrail API) • GetQueryResults(AWS CloudTrail API)
Löschen von Audit Manager-Ressourcen	• DeleteAssessmentFramework

Weiterführende MetricStream Links

- AWS Marketplace Link
- Link zum Produkt
- Preisgestaltung

Integration von Audit Manager Manager-Nachweisen in Ihr GRC-System

Als Unternehmenskunde verfügen Sie wahrscheinlich über Ressourcen in mehreren Rechenzentren, einschließlich anderer Cloud-Anbieter und lokaler Umgebungen. Um Beweise aus diesen Umgebungen zu sammeln, können Sie GRC-Lösungen (Governance, Risk, Compliance) von Drittanbietern wie MetricStream CyberGRC oder RSA Archer verwenden. Oder Sie könnten ein firmeneigenes GRC-System verwenden, das Sie selbst entwickelt haben.

Dieses Tutorial zeigt Ihnen, wie Sie Ihr internes oder externes GRC-System mit Audit Manager integrieren können. Diese Integration ermöglicht es Anbietern, Nachweise über die AWS Nutzung und Konfiguration ihrer Kunden zu sammeln und diese Nachweise direkt vom Audit Manager an die GRC-Anwendung zu senden. Auf diese Weise können Sie Ihre Compliance-Berichterstattung in mehreren Umgebungen zentralisieren.

Für die Zwecke dieses Tutorials:

1. Ein Anbieter ist die Entität oder das Unternehmen, dem die GRC-Anwendung gehört, die in Audit Manager integriert wird.
2. Ein Kunde ist die Entität oder Firma AWS, die eine interne oder externe GRC-Anwendung verwendet und auch verwendet.

> **Note**
>
> In einigen Fällen gehört die GRC-Anwendung demselben Unternehmen und wird von diesem verwendet. In diesem Szenario ist der Anbieter die Gruppe oder das Team, dem die GRC-Anwendung gehört, und der Kunde ist das Team oder die Gruppe, die die GRC-Anwendung verwendet.

In diesem Tutorial erfahren Sie, wie Sie folgende Aufgaben ausführen:

- Schritt 1: Audit Manager aktivieren
- Schritt 2: Berechtigungen einrichten
- Schritt 3. Ordnen Sie Ihre Unternehmenskontrollen den Audit Manager Manager-Kontrollen zu
- Schritt 4. Halten Sie Ihre Kontrollzuordnungen auf dem neuesten Stand
- Schritt 5: Erstellen Sie eine Bewertung
- Schritt 6: Fangen Sie an, Beweise zu

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Bedingungen erfüllen:

- Sie haben eine Infrastruktur, in der AWS.
- Sie verwenden ein internes GRC-System oder Sie verwenden GRC-Software eines Drittanbieters, die von einem Anbieter bereitgestellt wird.
- Sie haben alle Voraussetzungen erfüllt, die für die Einrichtung von Audit Manager erforderlich sind.
- Sie kennen sich aus mitAWS Audit Manager Konzepte und Terminologie verstehen.

Einige Einschränkungen, die Sie beachten sollten:

- Audit Manager ist regional tätig AWS-Service. Sie müssen Audit Manager in jeder Region, in der Sie Ihre AWS Workloads ausführen, separat einrichten.
- Audit Manager unterstützt nicht die Zusammenfassung von Nachweisen aus mehreren Regionen in einer einzigen Region. Wenn sich Ihre Ressourcen über mehrere erstrecken AWS-Regionen, müssen Sie die Beweise in Ihrem GRC-System zusammenfassen.
- Audit Manager hat Standardkontingente für die Anzahl der Ressourcen, die Sie erstellen können. Sie können bei Bedarf eine Erhöhung dieser Standardkontingente beantragen. Weitere Informationen finden Sie unter Kontingente und Einschränkungen für AWS Audit Manager.

Schritt 1: Audit Manager aktivieren

Wer schließt diesen Schritt ab

Customer

Wichtige Informationen

Aktivieren Sie zunächst Audit Manager für Ihre AWS-Konto. Wenn Ihr Konto Teil einer Organisation ist, können Sie Audit Manager über Ihr Verwaltungskonto aktivieren und dann einen delegierten Administrator für Audit Manager angeben.

Verfahren

Um Audit Manager zu aktivieren

Folgen Sie den Anweisungen zum Aktivieren von Audit Manager. Wiederholen Sie den Einrichtungsvorgang für alle Regionen, in denen Sie Beweise sammeln möchten.

> **Tip**
>
> Wenn Sie dies verwenden AWS Organizations, empfehlen wir Ihnen dringend, in diesem Schritt einen delegierten Administrator einzurichten. Wenn Sie ein delegiertes Administratorkonto in Audit Manager verwenden, können Sie mit der Evidence Finder in allen Mitgliedskonten Ihrer Organisation nach Nachweisen suchen.

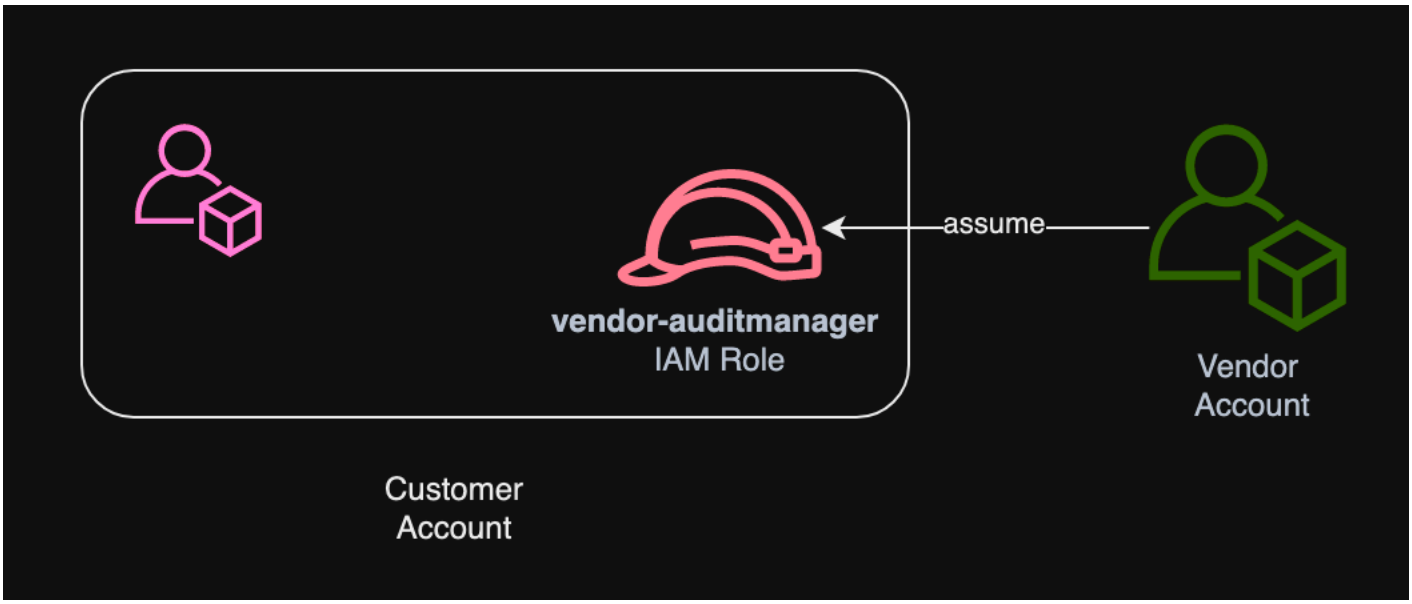
Schritt 2: Berechtigungen einrichten

Wer schließt diesen Schritt ab

Customer

Wichtige Informationen

In diesem Schritt erstellt der Kunde eine IAM-Rolle für sein Konto. Der Kunde erteilt dem Anbieter dann die Erlaubnis, die Rolle zu übernehmen.



Verfahren

Um eine Rolle für das Kundenkonto zu erstellen

Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.

- Wählen Sie in Schritt 8 des Workflows zur Rollenerstellung die Option Richtlinie erstellen aus und geben Sie eine Richtlinie für die Rolle ein.

  Die Rolle muss mindestens über die folgenden Berechtigungen verfügen:

  JSON

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

```
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

- Geben `vendor-auditmanager` Sie in Schritt 11 des Workflows zur Rollenerstellung den Namen der Rolle ein.

Damit das Lieferantenkonto die Rolle übernehmen kann

Folgen Sie den Anweisungen unter Gewähren von Benutzerberechtigungen zum Rollenwechsel im IAM-Benutzerhandbuch.

- Die Grundsatzerklärung muss die `Allow` Auswirkungen auf die `sts:AssumeRole action` enthalten.
- Es muss auch den Amazon-Ressourcennamen (ARN) der Rolle in einem Resource-Element enthalten.
- Hier ist ein Beispiel für eine Richtlinienerklärung, die Sie verwenden können.

  Ersetzen Sie in dieser Richtlinie die *`placeholder text`* durch die AWS-Konto ID Ihres Anbieters.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::111122223333:role/vendor-auditmanager"
    }
}
```

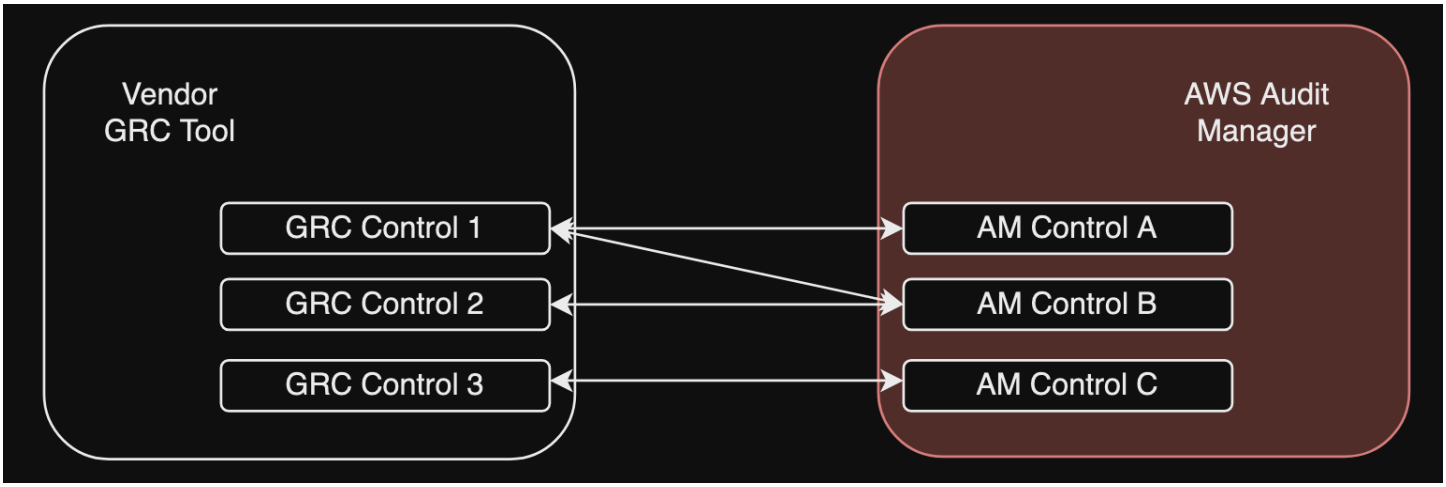
Schritt 3. Ordnen Sie Ihre Unternehmenskontrollen den Audit Manager Manager-Kontrollen zu

Wer schließt diesen Schritt ab

Customer

Wichtige Informationen

Anbieter führen eine kuratierte Liste von Unternehmenskontrollen, die Kunden bei einer Bewertung verwenden können. Für die Integration mit Audit Manager müssen Anbieter eine Schnittstelle erstellen, über die Kunden ihre Unternehmenskontrollen den entsprechenden Audit Manager-Kontrollen zuordnen können. Sie können common control s (bevorzugt) oder standard control s zuordnen. Sie müssen diese Zuordnung abschließen, bevor Sie mit der Bewertung in der GRC-Anwendung des Anbieters beginnen können.



Option 1: Ordnen Sie Unternehmenskontrollen allgemeinen Kontrollen zu (empfohlen)

Dies ist die empfohlene Methode, um Ihre Unternehmenskontrollen Audit Manager zuzuordnen. Dies liegt daran, dass die gemeinsamen Kontrollen eng mit den gängigen Industriestandards übereinstimmen. Dies macht es einfacher, sie Ihren Unternehmenskontrollen zuzuordnen.

Bei diesem Ansatz erstellt der Anbieter eine Schnittstelle, die es dem Kunden ermöglicht, eine einmalige Zuordnung zwischen seinen Unternehmenskontrollen und den entsprechenden allgemeinen Kontrollen vorzunehmen, die Audit Manager bereitstellt. Anbieter können die GetControlAPI-Operationen ListControlsListCommonControls, und verwenden, um diese Informationen ihren Kunden zur Verfügung zu stellen. Nachdem der Kunde die Zuordnung abgeschlossen hat, kann der Lieferant diese Zuordnungen verwenden, um benutzerdefinierte Steuerelemente in Audit Manager zu erstellen.

Hier ist ein Beispiel für eine gängige Kontrollzuweisung:

Nehmen wir an, Sie haben eine Unternehmenskontrolle mit dem Namen`Asset Management`. Diese Unternehmenskontrolle ist zwei allgemeinen Kontrollen in Audit Manager (`Asset performance management`und`Asset maintenance scheduling`) zugeordnet. In diesem Fall müssen Sie in Audit Manager ein benutzerdefiniertes Steuerelement erstellen (wir geben ihm einen Namen`enterprise-asset-management`). Fügen Sie dann `Asset performance management` und `Asset maintenance scheduling` als Beweisquellen zum neuen benutzerdefinierten Steuerelement hinzu. Diese Beweisquellen sammeln unterstützende Beweise aus einer vordefinierten Gruppe von AWS Datenquellen. Auf diese Weise können Sie auf effiziente Weise die AWS Datenquellen identifizieren, die den Anforderungen Ihrer Unternehmenssteuerung entsprechen.

Verfahren

Um die verfügbaren allgemeinen Steuerelemente zu finden, denen Sie eine Zuordnung zuordnen können

Folgen Sie den Schritten, um die Liste der verfügbaren allgemeinen Kontrollen in Audit Manager zu finden.

Um ein benutzerdefiniertes Steuerelement zu erstellen

1. Folgen Sie den Schritten, um ein benutzerdefiniertes Steuerelement zu erstellen, das auf Ihre Unternehmenssteuerung abgestimmt ist.

   Gehen Sie wie folgt vor, wenn Sie in Schritt 2 des Workflows zur Erstellung eines benutzerdefinierten Steuerelements Nachweisquellen angeben:

   - Wählen Sie AWS verwaltete Quellen als Beweisquelle aus.
   - Wählen Sie Verwenden Sie eine gemeinsame Kontrolle, die Ihrem Compliance-Ziel entspricht.
   - Wählen Sie bis zu fünf gängige Kontrollen als Nachweisquellen für Ihre Unternehmenskontrolle aus.
2. Wiederholen Sie diese Aufgabe für alle Ihre Unternehmenskontrollen, und erstellen Sie für jedes Steuerelement die entsprechenden benutzerdefinierten Kontrollen in Audit Manager.

Option 2: Ordnen Sie die Unternehmenskontrollen den Standardkontrollen zu

Audit Manager bietet eine große Anzahl vorgefertigter Standardsteuerungen. Sie können eine einmalige Zuordnung zwischen Ihren Unternehmenskontrollen und diesen Standardkontrollen durchführen. Nachdem Sie die Standardkontrollen identifiziert haben, die Ihren Unternehmenskontrollen entsprechen, können Sie diese Standardkontrollen direkt zu einem benutzerdefinierten Framework hinzufügen. Wenn Sie diese Option wählen, müssen Sie keine benutzerdefinierten Steuerelemente in Audit Manager erstellen.

Verfahren

Um die verfügbaren Standardsteuerelemente zu finden, denen Sie eine Zuordnung zuordnen können

Folgen Sie den Schritten, um die Liste der verfügbaren Standardkontrollen in Audit Manager zu finden.

Um ein benutzerdefiniertes Framework zu erstellen

1. Folgen Sie den Schritten, um ein benutzerdefiniertes Framework in Audit Manager zu erstellen.

   Wenn Sie in Schritt 2 des Verfahrens zur Erstellung des Frameworks einen Kontrollsatz angeben, schließen Sie die Standardkontrollen ein, die Ihren Unternehmenskontrollen zugeordnet sind.
2. Wiederholen Sie diese Aufgabe für alle Ihre Unternehmenskontrollen, bis Sie alle entsprechenden Standardsteuerelemente in Ihr benutzerdefiniertes Framework aufgenommen haben.

Schritt 4. Halten Sie Ihre Kontrollzuordnungen auf dem neuesten Stand

Wer schließt diesen Schritt ab

Lieferant, Kunde

Wichtige Informationen

Audit Manager aktualisiert kontinuierlich allgemeine Kontrollen und Standardkontrollen, um sicherzustellen, dass sie die neuesten verfügbaren AWS Datenquellen verwenden. Das bedeutet, dass die Zuordnung von Kontrollen eine einmalige Aufgabe ist: Sie müssen Standardkontrollen nicht verwalten, nachdem Sie sie zu einem benutzerdefinierten Framework hinzugefügt haben, und Sie müssen keine allgemeinen Kontrollen verwalten, nachdem Sie sie als Beweisquelle zu Ihrem benutzerdefinierten Steuerelement hinzugefügt haben. Immer wenn ein allgemeines Steuerelement aktualisiert wird, werden dieselben Aktualisierungen automatisch auf alle benutzerdefinierten Kontrollen angewendet, die dieses gemeinsame Steuerelement als Beweisquelle verwenden.

Im Laufe der Zeit ist es jedoch möglich, dass Ihnen neue allgemeine Kontrollen und Standardkontrollen als Beweisquellen zur Verfügung stehen. Vor diesem Hintergrund sollten Anbieter und Kunden einen Workflow erstellen, um regelmäßig die neuesten gängigen Kontrollen und Standardkontrollen von Audit Manager abzurufen. Anschließend können Sie die Zuordnungen zwischen den Enterprise Controls und den Audit Manager Manager-Kontrollen überprüfen und die Zuordnungen nach Bedarf aktualisieren.

Wenn Ihre Unternehmenskontrollen gemeinsamen Kontrollen zugeordnet sind

Während des Zuordnungsprozesses haben Sie benutzerdefinierte Steuerelemente erstellt. Sie können Audit Manager verwenden, um diese benutzerdefinierten Kontrollen so zu bearbeiten, dass sie die neuesten verfügbaren allgemeinen Kontrollen als Beweisquellen verwenden. Sobald die

Aktualisierungen der benutzerdefinierten Kontrollen wirksam werden, sammeln Ihre vorhandenen Bewertungen automatisch Beweise für die aktualisierten benutzerdefinierten Kontrollen. Es ist nicht erforderlich, ein neues Framework oder eine neue Bewertung zu erstellen.

Verfahren

Um die neuesten gängigen Steuerelemente zu finden, denen Sie eine Zuordnung zuordnen können

Folgen Sie den Schritten, um die verfügbaren allgemeinen Steuerelemente in Audit Manager zu finden.

Um ein benutzerdefiniertes Steuerelement zu bearbeiten

1. Folgen Sie den Schritten, um ein benutzerdefiniertes Steuerelement in Audit Manager zu bearbeiten.

   Gehen Sie wie folgt vor, wenn Sie die Beweisquellen in Schritt 2 des Bearbeitungsworkflows aktualisieren:

   - Wählen Sie AWS verwaltete Quellen als Beweisquelle aus.
   - Wählen Sie Verwenden Sie eine gemeinsame Kontrolle, die Ihrem Compliance-Ziel entspricht.
   - Wählen Sie das neue allgemeine Steuerelement aus, das Sie als Beweisquelle für Ihr benutzerdefiniertes Steuerelement verwenden möchten.
2. Wiederholen Sie diese Aufgabe für alle Ihre Unternehmenskontrollen, die Sie aktualisieren möchten.

Wenn Ihre Unternehmenskontrollen Standardkontrollen zugeordnet sind

In diesem Fall müssen Anbieter ein neues benutzerdefiniertes Framework erstellen, das die neuesten verfügbaren Standardkontrollen enthält, und dann eine neue Bewertung mit diesem neuen Framework erstellen. Nachdem Sie die neue Bewertung erstellt haben, können Sie Ihre alte Bewertung als inaktiv markieren.

Verfahren

Um die neuesten Standardsteuerungen zu finden, denen Sie eine Zuordnung zuordnen können

Folgen Sie den Schritten, um die verfügbaren Standardsteuerungen in Audit Manager zu finden.

Um ein benutzerdefiniertes Framework zu erstellen und die neuesten Standardsteuerelemente hinzuzufügen

Folgen Sie den Schritten, um ein benutzerdefiniertes Framework in Audit Manager zu erstellen.

Wenn Sie in Schritt 2 des Workflows zur Framework-Erstellung einen Kontrollsatz angeben, schließen Sie die neuen Standardsteuerelemente ein.

Um eine Bewertung zu erstellen

Erstellen Sie eine Bewertung in der GRC-Anwendung.

Um den Status einer Bewertung auf inaktiv zu ändern

Folgen Sie den Schritten, um den Status einer Bewertung in Audit Manager zu ändern.

Schritt 5: Erstellen Sie eine Bewertung

Wer schließt diesen Schritt ab

GRC-Anwendung mit Eingaben des Anbieters

Wichtige Informationen

Als Kunde müssen Sie keine Bewertung direkt in Audit Manager erstellen. Wenn Sie eine Bewertung für bestimmte Kontrollen in der GRC-Anwendung starten, erstellt die GRC-Anwendung die entsprechenden Ressourcen für Sie in Audit Manager. Zunächst verwendet die GRC-Anwendung die von Ihnen erstellten Zuordnungen, um die relevanten Audit Manager Manager-Kontrollen zu identifizieren. Als Nächstes verwendet sie die Kontrollinformationen, um ein benutzerdefiniertes Framework für Sie zu erstellen. Schließlich verwendet es das neu erstellte benutzerdefinierte Framework, um eine Bewertung in Audit Manager zu erstellen.

Für die Erstellung einer Bewertung in Audit Manager ist auch ein Geltungsbereich erforderlich. Dieser Umfang umfasst eine Liste der Bereiche AWS-Konten , in denen der Kunde die Bewertung durchführen und Nachweise sammeln möchte. Kunden müssen diesen Bereich direkt in der GRC-Anwendung definieren.

Als Anbieter müssen Sie die Daten speichern, `assessmentId` die der Bewertung zugeordnet sind, die in der GRC-Anwendung gestartet wurde. Dies `assessmentId` ist erforderlich, um Beweise von Audit Manager abzurufen.

Um eine Bewertungs-ID zu finden

1. Verwenden Sie den ListAssessmentsVorgang, um Ihre Bewertungen in Audit Manager anzuzeigen. Sie können den Status-Parameter verwenden, um aktive Bewertungen anzuzeigen.

```
aws auditmanager list-assessments --status ACTIVE
```

2. Identifizieren Sie in der Antwort die Bewertung, die Sie in der GRC-Anwendung speichern möchten, und notieren Sie sich die`assessmentId`.

Schritt 6: Fangen Sie an, Beweise zu

Wer schließt diesen Schritt ab

AWS Audit Manager, mit Beiträgen des Anbieters

Wichtige Informationen

Nachdem Sie eine Bewertung erstellt haben, dauert es bis zu 24 Stunden, bis mit der Beweiserhebung begonnen wird. Zu diesem Zeitpunkt sammelt Ihre Unternehmenskontrolle nun aktiv Nachweise für Ihre Bewertung durch den Audit Manager.

Wir empfehlen Ihnen, die Funktion zur Beweissuche zu verwenden, um schnell Beweise in Audit Manager abzufragen und zu finden. Wenn Sie ein delegierter Administrator für Audit Manager sind, aktivieren Sie die Beweissuche, um nach Beweisen für alle Mitgliedskonten in Ihrem Unternehmen zu suchen. Mithilfe einer Kombination aus Filtern und Gruppierungen können Sie den Umfang Ihrer Suchabfrage schrittweise einschränken. Wenn Sie sich beispielsweise einen umfassenden Überblick über den Zustand Ihres Systems verschaffen möchten, führen Sie eine umfassende Suche durch und filtern Sie nach Bewertung, Datumsbereich und Ressourcen-Compliance. Wenn Sie eine bestimmte Ressource korrigieren wollen, können Sie eine eingeschränkte Suche durchführen, um gezielt nach Beweisen für eine bestimmte Kontrollelement- oder Ressourcen-ID zu suchen. Nachdem Sie Ihre Filter definiert haben, können Sie die entsprechenden Suchergebnisse gruppieren und anschließend per Vorschau anzeigen, bevor Sie einen Bewertungsbericht erstellen.

Um Evidence Finder zu aktivieren

- Folgen Sie den Anweisungen, um den Evidence Finder in Ihren Audit Manager Manager-Einstellungen zu aktivieren.

Nachdem Sie den Evidence Finder aktiviert haben, können Sie festlegen, in welchem Rhythmus Beweise für Ihre Bewertung von Audit Manager abgerufen werden sollen. Sie können auch Nachweise für eine bestimmte Kontrolle in einer Bewertung abrufen und die Nachweise in der GRC-

Anwendung speichern, die der Unternehmenssteuerung zugeordnet ist. Sie können die folgenden Audit Manager Manager-API-Operationen verwenden, um Beweise abzurufen:

- GetEvidence
- GetEvidenceByEvidenceFolder
- GetEvidenceFolder
- GetEvidenceFoldersByAssessment
- GetEvidenceFoldersByAssessmentControl

Preisgestaltung

Für dieses Integrations-Setup fallen Ihnen keine zusätzlichen Kosten an, unabhängig davon, ob Sie ein Anbieter oder ein Kunde sind. Den Kunden werden die im Audit Manager gesammelten Nachweise in Rechnung gestellt. Weitere Informationen über die Preise finden Sie unter AWS Audit Manager – Preise.

Weitere Ressourcen

Weitere Informationen zu den in diesem Tutorial vorgestellten Konzepten finden Sie in den folgenden Ressourcen:

- Prüfungen — Erfahren Sie mehr über die Konzepte und Aufgaben zur Verwaltung einer Bewertung.
- Kontrollbibliothek — Erfahren Sie mehr über die Konzepte und Aufgaben zur Verwaltung eines benutzerdefinierten Steuerelements.
- Framework-Bibliothek — Erfahren Sie mehr über die Konzepte und Aufgaben zur Verwaltung eines benutzerdefinierten Frameworks.
- Evidence Finder — Erfahren Sie, wie Sie eine CSV-Datei exportieren oder aus Ihren Abfrageergebnissen einen Bewertungsbericht erstellen.
- Download-Center — Erfahren Sie, wie Sie Bewertungsberichte und CSV-Exporte von Audit Manager herunterladen können.

Unterstützte Frameworks in AWS Audit Manager

Wenn Sie die Framework-Bibliothek unter erkunden AWS Audit Manager, finden Sie eine umfassende Liste vorgefertigter Standard-Frameworks, mit denen Sie Ihre Compliance-Bemühungen optimieren können. Diese vorgefertigten Frameworks basieren auf AWS bewährten Verfahren für verschiedene Compliance-Standards und -Vorschriften. Sie können diese Frameworks verwenden, um Sie bei der Vorbereitung Ihrer Prüfung zu unterstützen, unabhängig davon, ob Sie Ihre Umgebung anhand von HIPAA, PCI DSS, SOC 2 oder mehr bewerten müssen.

> **Note**
>
> Wenn Sie Audit Manager noch nicht kennen, beginnen Sie mit dem AWS Audit Manager Sample Framework. Dieses Framework ist für Lernzwecke konzipiert und unterstützt keinen bestimmten Compliance-Standard. Es bietet eine kontrollierte Umgebung, in der Sie die Kernfunktionen von Audit Manager in einem überschaubaren Umfang erkunden können. Nachdem Sie das Beispielframework verwendet haben, um sich mit Audit Manager vertraut zu machen, können Sie die anderen Frameworks für tatsächliche Compliance-Bewertungen verwenden.

Die folgende Liste bietet einen Überblick über die verfügbaren Frameworks, sodass Sie leicht die Frameworks identifizieren können, die Ihren spezifischen Anforderungen entsprechen. Nehmen Sie sich einen Moment Zeit, um sich die Liste anzusehen und sich mit den Frameworks vertraut zu machen, die für die Bedürfnisse Ihres Unternehmens am relevantesten sind. Öffnen Sie eine beliebige Seite, um einen Überblick über dieses Framework zu erhalten und zu erfahren, wie Sie damit eine Bewertung erstellen und mit der Erfassung von Nachweisen in Audit Manager beginnen können.

Themen

- AWS Bewährte grundlegende Sicherheitsmethoden
- AWS Bewährte Verfahren für den Betrieb
- AWS Gut durchdachtes Framework WAF v10
- CCCS Medium Cloud Control
- CIS AWS Benchmark v1.2.0
- AWS CIS-Benchmark v1.3.0
- CIS AWS Benchmark v1.4.0
- CIS Controls v7.1, IG1
- CIS Critical Security Controls Version 8.0, IG1
- FedRAMP Security Baseline Controls r4
- GDPR 2016
- Gramm-Leach-Bliley Handeln
- Titel 21 CFR Teil 11
- EU GMP Anhang 11, v1
- HIPAA-Sicherheitsregel: Februar 2003
- Endgültige HIPAA Omnibus-Regel
- ISO/IEC 27001:2013 Anhang A
- NIST SP 800-53 Rev. 5
- NIST Cybersecurity Framework v1.1
- NIST SP 800-171 Rev. 2
- PCI DSS v3.2.1
- PCI DSS V4.0
- SSAE-18 SOC 2

ACSC Essential Eight

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das Essential Eight des Australian Cyber Security Center (ACSC) unterstützt.

Themen

Was ist das ACSC Essential Eight?

Das ACSC ist die führende Behörde der australischen Regierung für Cybersicherheit. Zum Schutz vor Cyberbedrohungen empfiehlt das ACSC, dass Unternehmen zunächst acht grundlegende Strategien zur Eindämmung von Cybersicherheitsvorfällen aus den Strategien zur Minderung von Cybersicherheitsvorfällen umsetzen. Diese als Essential Eight bekannte Grundlage erschwert es Gegnern erheblich, Systeme zu kompromittieren.

Da Essential Eight ein Mindestmaß an präventiven Maßnahmen vorsieht, muss Ihr Unternehmen zusätzliche Maßnahmen ergreifen, sofern Ihre Umgebung dies rechtfertigt. Außerdem können die Essential Eight zwar dazu beitragen, die meisten Cyber-Bedrohungen abzuschwächen, aber nicht alle. Daher müssen zusätzliche Strategien und Sicherheitskontrollen in Betracht gezogen werden, einschließlich der Strategien zur Abschwächung von Cybersicherheitsvorfällen und des Information Security Manual (ISM).

Verwendung dieses Frameworks

Sie können das Essential Eight-Standardframework verwenden AWS Audit Manager , um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den Anforderungen von Essential Eight in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der

Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im Essential Eight-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Australisches Zentrum für Cybersicherheit (ACSC) Essential Eight	61	132	3

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings _Australian-Cyber-Security-Center - (ACSC) -Essential-Eight.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den Essential Eight-Kontrollen entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein ACSC-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- ACSC Essential Eight

ACSC ISM 02. März 2023

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das das Information Security Manual (ISM) des Australian Cyber Security Center (ACSC) unterstützt.

Themen

Was bedeutet ACSC ISM?

Das ACSC ist die führende Behörde der australischen Regierung für Cybersicherheit. Das ACSC erstellt das ISM, das als eine Reihe von Prinzipien der Cybersicherheit fungiert. Der Zweck dieser Grundsätze besteht darin, strategische Leitlinien zu geben, wie ein Unternehmen seine Systeme und Daten vor Cyberbedrohungen schützen kann. Diese Grundsätze der Cybersicherheit sind in vier Hauptaktivitäten unterteilt: regeln, schützen, erkennen und reagieren. Ein Unternehmen sollte

nachweisen können, dass die Cybersicherheitsprinzipien innerhalb ihres Betriebs eingehalten werden. Das ISM richtet sich an Chief Information Security Officers, Chief Information Officers, Cybersicherheitsexperten und IT-Manager.

Das ISM-Framework wird vom ACSC unter einer Creative Commons Attribution 4.0 International License bereitgestellt. Informationen zum Urheberrecht finden Sie unter ACSC | Copyright. © Commonwealth of Australia 2022.

Verwendung dieses Frameworks

Sie können das ACSC ISM-Standardframework verwenden, um Sie bei der Vorbereitung AWS Audit Manager auf Audits zu unterstützen. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den ACSC-ISM-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im ACSC ISM-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Handbuch zur Informationssicherheit (ISM) des Australian Cyber Security Center (ACSC) 02. März 2023	88	789	22

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
> Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ ConfigDataSourceMappings _Australian-Cyber-Security-Center- (ACSC) -Information-Security-Manual- (ISM) -02-March-2023.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den Kontrollen des ACSC Information Security Manual entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein ACSC-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- ACSC-Handbuch zur Informationssicherheit (ISM)

AWS Audit Manager Beispiel für ein Framework

Wenn Sie Audit Manager noch nicht kennen, können Sie das AWS Audit Manager Sample Framework verwenden, um zu erfahren, wie Audit Manager funktioniert. Es bietet eine einfache Umgebung, in der Sie die Funktionen von Audit Manager erkunden können, ohne sich von übermäßigen Beweisen überwältigen zu lassen oder Ihre Kostenloses AWS-Kontingent Grenzen zu überschreiten. Nachdem Sie das Beispiel-Framework ausprobiert haben, können Sie damit beginnen, die restlichen Frameworks zu verwenden, die Audit Manager bereitstellt.

Themen

Was ist das AWS Audit Manager Sample Framework?

Das Beispiel-Framework bietet eine optimierte, anfängerfreundliche Möglichkeit, die Kernfunktionen von Audit Manager zu erkunden — das Sammeln von Nachweisen und das Anhängen dieser Daten an Kontrollen.

Im Framework finden Sie Beispielsteuerelemente, die Ihnen die verschiedenen Datenquellen zeigen, die Audit Manager zur automatischen Erfassung von Nachweisen verwendet. Zu diesen Datenquellen gehören ein AWS CloudTrail Ereignis, eine AWS Config Regel, ein AWS Security Hub CSPM Steuerelement und ein AWS API-Aufruf. Wenn Sie diese Datenquellen in einer Testbewertung verwenden, können Sie sehen, wie Audit Manager mit verschiedenen Methoden zusammenarbeitet AWS-Services , um Beweise zu sammeln. Das Beispielframework demonstriert nicht nur die automatisierte Beweiserhebung, sondern zeigt auch, wie Sie Ihre eigenen Nachweise manuell hinzufügen können. Es verfügt auch über eine manuelle Steuerung, mit der Sie Dateien als Beweismittel hochladen können. Indem Sie sowohl automatisierte als auch manuelle Kontrollen ausprobieren, können Sie ein umfassendes Verständnis der verschiedenen Möglichkeiten entwickeln, wie Beweise zu Ihren Bewertungen hinzugefügt werden können.

> **Note**
>
> Dieses Framework unterscheidet sich von anderen Standard-Frameworks. Das Beispiel-Framework ist nicht für die Verwaltung von tatsächlichen Compliance-Bewertungen oder Audits vorgesehen. Es soll Ihnen helfen, den Umgang mit Audit Manager zu erlernen. Es bietet eine kontrollierte Umgebung, in der Sie genügend Nachweise sammeln können, um

die Fähigkeiten von Audit Manager zu testen, und gleichzeitig den Umfang für Anfänger überschaubar halten können.

Verwendung dieses Frameworks

Mit dem AWS Audit Manager Sample Framework können Sie üben, in der Audit Manager Manager-Oberfläche zu navigieren, Nachweise zu sammeln und zu sehen, wie diese Nachweise mit Ihren Bewertungskontrollen verknüpft sind.

Verwenden Sie zunächst das Beispiel-Framework, um eine Bewertung zu erstellen. Mit dieser Aktion wird die fortlaufende Erfassung von Nachweisen für jede der automatisierten Kontrollen im Beispielframework gestartet. Auf der Grundlage der Kontrolldefinitionen bewertet Audit Manager Ihre AWS Ressourcen, sammelt die relevanten Nachweise und fügt sie dann den Kontrollen in Ihrer Bewertung hinzu. Zu diesem Zeitpunkt können Sie die Beweise untersuchen, die Audit Manager gesammelt hat. Sie können auch versuchen, Ihre eigenen Nachweise zu den manuellen Kontrollen hinzuzufügen.

Sie finden dieses Framework auf der Registerkarte Standard-Frameworks der Framework-Bibliothek in Audit Manager.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Amazon Web Services (AWS) Audit Manager Manager-Beispielframework	4	1	2

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln

aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _AWS-Audit-Manager-Sample-Framework.zip herunter.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

AWS Control Tower Leitplanken

AWS Audit Manager bietet ein vorgefertigtes AWS Control Tower Guardrails-Framework, das Sie bei der Vorbereitung Ihrer Prüfung unterstützt.

Themen

Was ist? AWS Control Tower

AWS Control Tower ist ein Verwaltungs- und Governance-Service, mit dem Sie sich durch den Einrichtungsprozess und die Governance-Anforderungen, die mit der Erstellung einer AWS Umgebung mit mehreren Konten verbunden sind, zurechtfinden können.

Mit AWS Control Tower können Sie mit wenigen Klicks neue bereitstellen AWS-Konten , die Ihren unternehmens- oder organisationsweiten Richtlinien entsprechen. AWS Control Tower erstellt in Ihrem Namen eine Orchestrierungsebene, die die Funktionen mehrerer anderer kombiniert und integriert. AWS-Services Zu diesen Diensten gehören AWS Organizations AWS IAM Identity Center, und AWS-Service Catalog. Somit können Sie den Prozess der Einrichtung und Verwaltung einer AWS -Umgebung mit mehreren Konten rationalisieren, die sowohl sicher als auch konform ist.

Das AWS Control Tower Guardrails-Framework enthält alle Elemente AWS-Config-Regeln , die auf den Leitplanken von basieren. AWS Control Tower

Verwendung dieses Frameworks

Sie können das AWS Control Tower -Leitlinien-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Steuerelemente sind nach denen gruppiert, AWS-Config-Regeln die auf Leitplanken von basieren. AWS Control Tower Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Ausgangspunkt verwenden, können Sie eine Audit Manager Manager-Bewertung erstellen und mit der Erfassung von Nachweisen beginnen, die für ein AWS Control Tower Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im AWS Control Tower Guardrails-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Einzelheiten des AWS Control Tower Guardrails-Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
AWS Control Tower Leitplanken	14	0	5

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _AWS-Control-Tower-Guardrails.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme mit AWS Control Tower Guardrails konform sind. Darüber hinaus können sie nicht garantieren, dass Sie ein Audit bestehen.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- AWS Control Tower Service-Seite
- AWS Control Tower benutzerhandbuch

AWS Framework für bewährte Methoden für generative KI v2

> **Note**
>
> Am 11. Juni 2024 AWS Audit Manager wurde dieses Framework auf eine neue Version aktualisiert, das AWS generative AI Best Practices Framework v2. Zusätzlich zur

Unterstützung von Best Practices für Amazon Bedrock ermöglicht es Ihnen v2, Nachweise zu sammeln, die belegen, dass Sie die Best Practices für Amazon SageMaker AI befolgen. Das AWS generative KI-Best-Practices-Framework v1 wird nicht mehr unterstützt. Wenn Sie zuvor ein Assessment aus dem v1-Framework erstellt haben, funktionieren Ihre vorhandenen Assessments weiterhin. Sie können jedoch keine neuen Bewertungen mehr aus dem v1-Framework erstellen. Wir empfehlen Ihnen, stattdessen das aktualisierte v2-Framework zu verwenden.

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, mit dem Sie sich einen Überblick darüber verschaffen können, wie Ihre generative KI-Implementierung auf Amazon Bedrock und Amazon SageMaker AI anhand der AWS empfohlenen Best Practices funktioniert.

Amazon Bedrock ist ein vollständig verwalteter Service, der KI-Modelle von Amazon und anderen führenden KI-Unternehmen über eine API verfügbar macht. Mit Amazon Bedrock können Sie bestehende Modelle privat mit den Daten Ihres Unternehmens abstimmen. Auf diese Weise können Sie grundlegende Modelle (FMs) und umfangreiche Sprachmodelle (LLMs) nutzen, um Anwendungen sicher zu erstellen, ohne den Datenschutz zu gefährden. Weitere Informationen finden Sie unter Was ist Amazon Bedrock? im Amazon Bedrock-Benutzerhandbuch.

Amazon SageMaker AI ist ein vollständig verwalteter Service für maschinelles Lernen (ML). Mit SageMaker KI können Datenwissenschaftler und Entwickler ML-Modelle für erweiterte Anwendungsfälle erstellen, trainieren und einsetzen, die eine umfassende Anpassung und Modellfeinabstimmung erfordern. SageMaker KI bietet verwaltete ML-Algorithmen, mit denen extrem große Datenmengen in einer verteilten Umgebung effizient verarbeitet werden können. Mit integrierter Unterstützung für Ihre eigenen Algorithmen und Frameworks bietet SageMaker KI flexible verteilte Trainingsoptionen, die sich an Ihre spezifischen Workflows anpassen. Weitere Informationen finden Sie unter Was ist Amazon SageMaker AI? im Amazon SageMaker AI-Benutzerhandbuch.

Themen

Was sind bewährte Methoden für AWS generative KI für Amazon Bedrock?

Generative KI bezieht sich auf einen KI-Bereich, der sich darauf konzentriert, Maschinen in die Lage zu versetzen, Inhalte zu generieren. Generative KI-Modelle sind darauf ausgelegt, Ergebnisse zu erzielen, die den Beispielen, an denen sie trainiert wurden, sehr ähnlich sind. Dadurch entstehen Szenarien, in denen KI menschliche Konversationen nachahmen, kreative Inhalte generieren, riesige Datenmengen analysieren und Prozesse automatisieren kann, die normalerweise von Menschen ausgeführt werden. Das schnelle Wachstum der generativen KI bringt vielversprechende neue Innovationen mit sich. Gleichzeitig wirft es neue Herausforderungen auf, wie generative KI verantwortungsbewusst und unter Einhaltung der Governance-Anforderungen eingesetzt werden kann.

AWS ist bestrebt, Ihnen die Tools und Anleitungen zur Verfügung zu stellen, die Sie für die verantwortungsvolle Entwicklung und Verwaltung von Anwendungen benötigen. Um Ihnen bei diesem Ziel zu helfen, hat Audit Manager in Zusammenarbeit mit Amazon Bedrock und SageMaker KI das AWS generative KI-Best-Practices-Framework v2 entwickelt. Dieses Framework bietet Ihnen ein speziell entwickeltes Tool zur Überwachung und Verbesserung der Steuerung Ihrer generativen KI-Projekte auf Amazon Bedrock und Amazon AI. SageMaker Sie können das Best-Practices-Framework verwenden, um eine bessere Kontrolle und Transparenz über Ihre Modellnutzung zu erlangen und über das Modellverhalten auf dem Laufenden zu bleiben.

Die Kontrollen in diesem Framework wurden in Zusammenarbeit mit KI-Experten, Compliance-Experten und Sicherheitsexperten sowie mit Beiträgen von AWS Deloitte entwickelt. Jede automatisierte Steuerung ist einer AWS Datenquelle zugeordnet, aus der Audit Manager Beweise sammelt. Sie können die gesammelten Beweise verwenden, um Ihre generative KI-Implementierung auf der Grundlage der folgenden acht Prinzipien zu bewerten:

1. Verantwortungsvoll – Entwickeln und befolgen Sie ethische Richtlinien für den Einsatz und die Nutzung generativer KI-Modelle
2. Sicher – Legen Sie eindeutige Parameter und ethische Grenzen fest, um schädliche oder problematische Ergebnisse zu verhindern
3. Fair – Berücksichtigen und respektieren Sie, wie sich ein KI-System auf verschiedene Untergruppen von Nutzern auswirkt
4. Nachhaltig – Streben Sie nach mehr Effizienz und nachhaltigeren Energiequellen
5. Resilienz – Aufrechterhaltung der Integritäts- und Verfügbarkeitsmechanismen, um sicherzustellen, dass ein KI-System zuverlässig funktioniert

6. Datenschutz – Stellen Sie sicher, dass sensible Daten vor Diebstahl und Offenlegung geschützt sind
7. Genauigkeit – Entwickeln Sie KI-Systeme, die genau, zuverlässig und robust sind
8. Schutz – Verhindern Sie unbefugten Zugriff auf generative KI-Systeme

Beispiel

Nehmen wir an, Ihre Anwendung verwendet ein Basismodell eines Drittanbieters, das auf Amazon Bedrock verfügbar ist. Sie können das AWS generative KI-Best-Practices-Framework verwenden, um Ihre Nutzung dieses Modells zu überwachen. Mithilfe dieses Frameworks können Sie Beweise sammeln, die belegen, dass Ihre Nutzung den Best Practices der generativen KI entspricht. Dies bietet Ihnen einen konsistenten Ansatz, um die Nutzung und die Berechtigungen des Track-Modells nachzuverfolgen, sensible Daten zu kennzeichnen und bei unbeabsichtigten Offenlegungen gewarnt zu werden. Mithilfe bestimmter Framework-Kontrollen können Sie beispielsweise Beweise sammeln, anhand derer Sie beweisen können, dass Sie Mechanismen für Folgendes implementiert haben:

- Dokumentation der Quelle, Art, Qualität und Behandlung der neuen Daten, um Transparenz zu gewährleisten und Unterstützung bei der Fehlerbehebung oder bei Audits zu bieten (Verantwortlich)
- Regelmäßige Bewertung des Modells anhand vordefinierter Leistungskennzahlen, um sicherzustellen, dass es die Genauigkeits- und Sicherheitsstandards erfüllt (Sicher)
- Einsatz automatisierter Überwachungstools zur Erkennung potenzieller verzerrter Ergebnisse oder Verhaltensweisen in Echtzeit und zur Warnung davor (Fair)
- Bewertung, Identifizierung und Dokumentation der Modellnutzung und von Szenarien, in denen bestehende Modelle wiederverwendet werden können, unabhängig davon, ob Sie sie generiert haben oder nicht (nachhaltig)
- Einrichtung von Verfahren zur Benachrichtigung im Falle einer unbeabsichtigten Weitergabe personenbezogener Daten oder einer unbeabsichtigten Offenlegung (Datenschutz)
- Einrichtung einer Echtzeitüberwachung des KI-Systems und von Warnmeldungen bei Anomalien oder Störungen (Resilienz)
- Erkennung von Ungenauigkeiten und Durchführung einer gründlichen Fehleranalyse, um die Ursachen zu verstehen (Genauigkeit)
- Implementierung der end-to-end Verschlüsselung für Eingabe- und Ausgabedaten der KI-Modelle gemäß den Mindeststandards der Branche (Secure)

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

> **Note**
>
> - Wenn Sie ein Amazon Bedrock- oder SageMaker AI-Kunde sind, können Sie dieses Framework direkt in Audit Manager verwenden. Stellen Sie sicher, dass Sie das Framework verwenden und Bewertungen in den AWS-Konten und Regionen durchführen, in denen Sie Ihre generativen KI-Modelle und -Anwendungen ausführen.
> - Wenn Sie Ihre CloudWatch Protokolle für Amazon Bedrock oder SageMaker AI mit Ihrem eigenen KMS-Schlüssel verschlüsseln möchten, stellen Sie sicher, dass Audit Manager Zugriff auf diesen Schlüssel hat. Zu diesem Zweck können Sie Ihren vom Kunden verwalteten Schlüssel in Ihren Audit Manager Konfiguration Ihrer Datenverschlüsselungseinstellungen Manager-Einstellungen auswählen.
> - Dieses Framework verwendet den Amazon ListCustomModelsBedrock-Vorgang, um Beweise für die Verwendung Ihres benutzerdefinierten Modells zu generieren. Dieser API-Vorgang wird derzeit AWS-Regionen nur in den USA Ost (Nord-Virginia) und USA West (Oregon) unterstützt. Aus diesem Grund finden Sie möglicherweise keine Hinweise auf die Verwendung Ihrer benutzerdefinierten Modelle in den Regionen Asien-Pazifik (Tokio), Asien-Pazifik (Singapur) oder Europa (Frankfurt).

Sie können dieses Framework verwenden, um sich auf Audits über Ihren Einsatz generativer KI auf Amazon Bedrock und SageMaker KI vorzubereiten. Es umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den Best Practices der generativen KI in Kontrollen gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Audit Manager-Bewertung erstellen und mit der Erfassung von Beweisen beginnen, anhand derer Sie die Einhaltung Ihrer geplanten Richtlinien überwachen können. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im AWS generativen KI-Best-Practices-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche

aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
AWS Framework für bewährte Verfahren im Bereich generativer KI v2	72	38	8

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Config, stellen Sie sicher, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Kontrolldatenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings _AWS-Generative-AI-Best-Practices-Framework-v2 herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den Best Practices für generative KI entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein Audit über Ihre Nutzung generativer KI bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Manuelles Überprüfen von Eingabeaufforderungen in Amazon Bedrock

Möglicherweise haben Sie verschiedene Gruppen von Eingabeaufforderungen, die anhand bestimmter Modelle bewertet werden müssen. In diesem Fall können Sie den Befehl `InvokeModel` verwenden, um jede Aufforderung auszuwerten und die Antworten als manuelle Beweise zu sammeln.

Verwenden des Befehls `InvokeModel`

Erstellen Sie zunächst eine Liste mit vordefinierten Eingabeaufforderungen. Sie verwenden diese Eingabeaufforderungen, um die Antworten des Modells zu überprüfen. Stellen Sie sicher, dass Ihre Liste der Eingabeaufforderungen alle Anwendungsfälle enthält, die Sie auswerten möchten. Möglicherweise verfügen Sie über Eingabeaufforderungen, anhand derer Sie überprüfen können, ob die Modellantworten keine persönlich identifizierbare Informationen (PII) preisgeben.

Nachdem Sie Ihre Liste mit Eingabeaufforderungen erstellt haben, testen Sie jede einzelne mit dem von Amazon Bedrock bereitgestellten InvokeModelVorgang. Anschließend können Sie die Antworten des Modells auf diese Eingabeaufforderungen erheben und diese Daten als manuelle Beweise in Ihre Audit-Manager-Bewertung hochladen.

Es gibt drei verschiedene Möglichkeiten, den Befehl `InvokeModel` zu verwenden.

1. HTTP-Anforderungen

   Sie können Tools wie Postman verwenden, um eine HTTP-Anfrage an `InvokeModel` zu erstellen und die Antwort zu speichern.

   > **Note**
   >
   > Postman wird von einem Drittanbieter entwickelt. Es wurde nicht entwickelt oder unterstützt von. AWS Weitere Informationen zur Verwendung von Postman oder Hilfe bei Problemen im Zusammenhang mit Postman erhalten Sie im Support Center auf der Postman-Website.

2. AWS CLI

   Sie können den AWS CLI Befehl invoke-model ausführen. Anweisungen und weitere Informationen finden Sie unter Ausführen von Inferenzen auf einem Modell im Amazon Bedrock-Benutzerhandbuch.

   Das folgende Beispiel zeigt, wie Text AWS CLI mithilfe der Eingabeaufforderung *"story of two dogs"* und des Modells generiert wird. *Anthropic Claude V2* Das Beispiel gibt bis zu *300* Tokens in der Antwort zurück und speichert die Antwort in der Datei*invoke-model-output.txt*:

   ```
   aws bedrock-runtime invoke-model \
   ```

```
            --model-id anthropic.claude-v2 \
            --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
 \"max_tokens_to_sample\" : 300}" \
            --cli-binary-format raw-in-base64-out \
            invoke-model-output.txt
```

3. Automatisierte Verifizierung

Sie können CloudWatch Synthetics Canaries verwenden, um Ihre Modellantworten zu überwachen. Mit dieser Lösung können Sie das `InvokeModel` Ergebnis anhand CloudWatch einer Liste vordefinierter Eingabeaufforderungen überprüfen und anschließend das Verhalten des Modells bei diesen Eingabeaufforderungen überwachen.

Um mit dieser Lösung beginnen zu können, müssen Sie zunächst einen Synthetics-Canary erstellen. Nachdem Sie einen Canary erstellt haben, können Sie den folgenden Codeausschnitt verwenden, um Ihre Eingabeaufforderung und die Antwort des Modells zu überprüfen.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
```

```
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> Alternativ können Sie dieses Skript auch mit einer Lambda-Funktion ausführen. Wenn Sie sich für diese Lösung entscheiden, müssen Sie zuerst eine Lambda-Funktion erstellen.

Beispielaufforderungen

Sie können diese Beispielaufforderungen als Vorlage verwenden, um die Antworten Ihres Modells zu testen. Ersetzen Sie in den folgenden Beispielen die *`placeholder text`* durch Ihre eigenen Daten, um Ihren spezifischen Testanwendungsfällen Rechnung zu tragen.

Modellantworten auf unangemessene Inhalte testen

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

Modellantworten auf personenbezogene Daten testen

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

Modellantworten bei personenbezogenen Daten auf Obszönität testen

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- Amazon Bedrock
- Amazon Bedrock-Benutzerhandbuch
- Amazon SageMaker KI
- Amazon SageMaker AI-Benutzerhandbuch
- Transformieren verantwortungsvoller KI von der Theorie in die Praxis
- Verbraucherschutz und Innovationsförderung – KI-Regulierung und Bildung von Vertrauen in verantwortungsvolle KI
- Leitfaden zum verantwortungsvollen Umgang mit Machine Learning

AWS License Manager

AWS Audit Manager bietet ein vorgefertigtes AWS License Manager Framework, das Sie bei der Vorbereitung Ihrer Prüfung unterstützt.

Themen

Was ist AWS License Manager?

Mit AWS License Manager können Sie Ihre Softwarelizenzen von verschiedenen Softwareanbietern (wie Microsoft, SAP, Oracle oder IBM) zentral in AWS und vor Ort verwalten. Alle Ihre Softwarelizenzen an einem Ort zu haben, ermöglicht eine bessere Kontrolle und Transparenz und kann helfen, Lizenzüberschreitungen zu begrenzen und das Risiko von Verstößen und Falschmeldungen zu verringern.

Das AWS License Manager Framework ist in License Manager integriert, um Informationen zur Lizenznutzung auf der Grundlage von kundendefinierten Lizenzregeln zu aggregieren.

Verwendung dieses Frameworks

Sie können das AWS License Manager-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind nach vom Kunden definierten Lizenzregeln gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im AWS License Manager Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Einzelheiten des AWS License Manager Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
AWS License Manager	27	0	6

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den Lizenzregeln entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein Lizenznutzungs-Audit bestehen.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

License Manager-Links

- AWS License Manager Service-Seite
- AWS License Manager benutzerhandbuch

License Manager APIs

Für dieses Framework verwendet Audit Manager eine benutzerdefinierte Aktivität `GetLicenseManagerSummary`, um Beweise zu sammeln. Die `GetLicenseManagerSummary` Aktivität ruft die folgenden drei License Manager auf APIs:

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

Die zurückgegebenen Daten werden dann in Beweise umgewandelt und den entsprechenden Kontrollen in Ihrer Bewertung beigefügt.

Beispiel: Nehmen wir an, Sie verwenden zwei lizenzierte Produkte (SQL Server 2017 und Oracle Database Enterprise Edition). Zunächst ruft die `GetLicenseManagerSummary` Aktivität die ListLicenseConfigurationsAPI auf, die Details zu den Lizenzkonfigurationen in Ihrem Konto bereitstellt. Als Nächstes fügt sie zusätzliche Kontextdaten für jede Lizenzkonfiguration hinzu, indem sie und aufruft ListUsageForLicenseConfiguration. ListAssociationsForLicenseConfiguration

Schließlich werden die Lizenzkonfigurationsdaten in Beweise umgewandelt und an die jeweiligen Kontrollen im Framework angehängt (4.5 – vom Kunden verwaltete Lizenz für SQL Server 2017 und 3.0.4 – vom Kunden verwaltete Lizenz für Oracle Database Enterprise Edition). Wenn Sie ein lizenziertes Produkt verwenden, das durch keine der Kontrollen im Framework abgedeckt wird, werden diese Lizenzkonfigurationsdaten als Beweis an die folgende Kontrolle angehängt: 5.0 – Vom Kunden verwaltete Lizenz für andere Lizenzen.

AWS Bewährte grundlegende Sicherheitsmethoden

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das die AWS grundlegenden Best Practices für Sicherheit unterstützt.

Themen

Was bedeutet der AWS -Best Practices-Standard für grundlegende Sicherheit?

Der Standard „Bewährte Methoden für AWS grundlegende Sicherheit“ besteht aus einer Reihe von Kontrollen, die erkennen, wenn Ihre bereitgestellten Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.

Sie können diesen Standard verwenden, um all Ihre Arbeitslasten kontinuierlich zu bewerten AWS-Konten und schnell Bereiche zu identifizieren, in denen Abweichungen von den bewährten Methoden bestehen. Der Standard bietet umsetzbare und ausführliche Anleitungen zur Verbesserung und Aufrechterhaltung der Sicherheitslage Ihrer Organisation.

Die Kontrollen umfassen Best Practices aus mehreren AWS-Services. Jeder Kontrolle wird eine Kategorie zugewiesen, die die Sicherheits-Funktion widerspiegelt, auf die die Kontrolle angewendet wird. Weitere Informationen finden Sie in den Kontrollkategorien im AWS Security Hub CSPM - Benutzerhandbuch.

Verwendung dieses Frameworks

Sie können das Framework von AWS Foundational Security Best Practices verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den Anforderungen der Best Practices von AWS Foundational Security in Kontrollgruppen gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung der Ressourcen in Ihren AWS-Konten und Services. Dies erfolgt auf der Grundlage der Kontrollen, die im Framework für bewährte Methoden der AWS Grundlagensicherheit definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Einzelheiten des Frameworks für bewährte Methoden der AWS Grundlagensicherheit lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
AWS Bewährte grundlegende Sicherheitsmethoden	146	0	31

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den Best Practices von AWS Foundation Security entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein Audit mit den Best Practices von AWS Foundational Security bestehen.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- AWS Der Standard „Bewährte Grundpraktiken im Bereich Sicherheit“ im AWS Security Hub CSPM Benutzerhandbuch
- Kategorien von Kontrollen im AWS Security Hub CSPM -Benutzerhandbuch

AWS Bewährte Verfahren für den Betrieb

AWS Audit Manager bietet ein vorgefertigtes Framework für bewährte AWS Betriebspraktiken (Operational Best Practices, OBP), das Sie bei der Prüfungsvorbereitung unterstützt.

Dieses Framework bietet eine Untergruppe von Kontrollen aus dem Standard „Best Practices für AWS grundlegende Sicherheit“. Diese Kontrollen dienen als grundlegende Prüfungen, um festzustellen, wann Ihre bereitgestellten Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.

Themen

Was ist der Standard „Best Practices“ von AWS Foundational Security?

Sie können den Best Practices-Standard für grundlegende Sicherheit von AWS verwenden, um Ihre Konten und Workloads zu bewerten und schnell Bereiche zu identifizieren, in denen Abweichungen von den Best Practices bestehen. Der Standard bietet umsetzbare und ausführliche Anleitungen zur Verbesserung und Aufrechterhaltung der Sicherheitslage Ihrer Organisation.

Die Kontrollen umfassen Best Practices aus mehreren AWS-Services. Jeder Kontrolle wird eine Kategorie zugewiesen, die die Sicherheits-Funktion widerspiegelt, auf die die Kontrolle angewendet wird. Weitere Informationen finden Sie in den Kontrollkategorien im AWS Security Hub CSPM - Benutzerhandbuch.

Verwendung dieses Frameworks

Sie können das Framework für Betriebliche Best Practices von AWS verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den Anforderungen für AWS betriebliche Best Practices in Kontrollgruppen gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Die Einzelheiten des Rahmens für bewährte AWS betriebliche Verfahren lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
AWS Bewährte betriebliche Verfahren	0	51	20

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.

Die Kontrollen in diesem Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den AWS betrieblichen Best Practices entsprechen. Darüber hinaus wird nicht garantiert, dass Sie ein AWS -Audit mit den Betrieblichen Best Practices bestehen.

Dieses Framework enthält nur manuelle Kontrollen. Bei diesen manuellen Kontrollen werden Beweise nicht automatisch gesammelt. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- AWS Der Standard „Bewährte Grundpraktiken im Bereich Sicherheit“ im AWS Security Hub CSPM Benutzerhandbuch
- Kategorien von Kontrollen im AWS Security Hub CSPM -Benutzerhandbuch

AWS Gut durchdachtes Framework WAF v10

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das das AWS Well-Architected Framework v10 unterstützt.

Themen

Was ist das AWS Well-Architected Framework?

AWS Well-Architected hilft Ihnen beim Aufbau einer sicheren, leistungsstarken, belastbaren und effizienten Infrastruktur für Ihre Anwendungen und Workloads. Das auf sechs Säulen – Operational Excellence, Sicherheit, Zuverlässigkeit, Leistungseffizienz, Kostenoptimierung und Nachhaltigkeit – basierende Konzept von AWS Well-Architected bietet Ihnen und Ihren Partnern einen konsistenten Ansatz für die Bewertung von Architekturen und die Implementierung skalierbarer Designs.

Verwendung dieses Frameworks

Sie können das AWS Well-Architected Framework verwenden, um sich auf Audits vorzubereiten. In diesem Framework werden die wichtigsten Konzepte, Entwurfsprinzipien und bewährte Architekturmethoden für das Entwickeln und Ausführen von Workloads in der Cloud beschrieben. Von den sechs Säulen, auf denen AWS Well-Architected basiert, dienen die Säulen Sicherheit und Zuverlässigkeit von AWS Audit Manager als vorgefertigtes Framework und Kontrollinstrument. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Steuerelemente, die im AWS Well-Architected Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	43	291	6

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _AWS-Well-Architected-Framework-WAF-v10.zip herunter.

Die Kontrollen in diesem Framework dienen nicht zur Überprüfung, ob Ihre Systeme konform sind. Darüber hinaus können sie nicht garantieren, dass Sie ein Audit bestehen.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen dazu, wie Sie dieses Framework an Ihre spezifischen Anforderungen anpassen können, finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- AWS Well-Architected
- AWS Well-Architected-Framework-Dokumentation

CCCS Medium Cloud Control

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das Medium Cloud Control des Canadian Centre for Cyber Security (CCCS) unterstützt.

Themen

Was ist das CCCS?

Das CCCS ist Kanadas maßgebliche Quelle für Beratung, Dienstleistungen und Unterstützung durch Experten im Bereich Cybersicherheit. Das CCCS stellt dieses Fachwissen kanadischen Regierungen, der Industrie und der Öffentlichkeit zur Verfügung. Kanadische Organisationen des öffentlichen Sektors verlassen sich landesweit auf die strengen Bewertungen von Cloud-Service-Anbietern, um fundierte Entscheidungen zur Cloud-Beschaffung zu treffen.

Das CCCS-Kontrollprofil für mittelgroße Clouds löste im Mai 2020 das PROTECTED B-Profil / Medium Integrity / Medium Availability (PBMM) der kanadischen Regierung ab. Das CCCS-Kontrollprofil für mittelgroße Clouds eignet sich, wenn Ihr Unternehmen öffentliche Cloud-Dienste zur Unterstützung von Geschäftsaktivitäten mit mittleren Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit (AIC) verwendet. Bei Workloads mit mittleren AIC-Anforderungen kann normalerweise davon ausgegangen werden, dass die unbefugte Offenlegung, Änderung oder der Verlust des Zugriffs auf die Informationen oder Dienste, die im Rahmen der Geschäftstätigkeit genutzt werden, einer Person oder einem Unternehmen schweren Schaden zufügt oder einer Gruppe von Personen begrenzten Schaden zufügt. Nachfolgend finden Sie Beispiele für diese Schädigungsgrade:

- Signifikante Auswirkung auf den Jahresgewinn
- Verlust von Großkunden
- Verlust des Firmenwerts
- Eindeutiger Compliance-Verstoß
- Verletzung der Privatsphäre von Abertausenden von Menschen
- Beeinträchtigung der Programmleistung
- Folgen sind psychische oder körperlichen Krankheiten
- Sabotage
- Schädigen der Reputation
- Individuelle finanzielle Notlage

Verwendung dieses Frameworks

Sie können das AWS Audit Manager Framework für CCCS Medium Cloud Control verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den CCCS-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Ausgangspunkt verwenden, können Sie ein Audit Manager Manager-Assessment erstellen und mit der Erfassung von Nachweisen beginnen, die für ein CCCS Medium Cloud Control-Audit relevant sind. In Ihrer Bewertung können Sie angeben, welche Punkte Sie in den AWS-Konten Umfang Ihres Audits einbeziehen möchten. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies erfolgt auf der Grundlage der Kontrollen, die im CCCS Medium Cloud Control-Framework definiert sind. Wenn

es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Kanadisches Zentrum für Cybersicherheit (CCCS) Medium Cloud Control	71	282	175

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ AuditManager _ ConfigDataSourceMappings _CCCS-Medium-Cloud-Control.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme die CCCS Medium Cloud Control-Anforderungen erfüllen. Darüber hinaus können sie nicht garantieren, dass Sie ein CCCS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

CIS AWS Benchmark v1.2.0

AWS Audit Manager bietet zwei vorgefertigte Frameworks, die den Amazon Web Services () Benchmark v1.2.0 des Center for Internet Security (CIS AWS) unterstützen.

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version 1.3.0 unterstützen, finden Sie unterAWS CIS-Benchmark v1.3.0.
> - Informationen zu den Audit Manager-Frameworks, die Version 1.4.0 unterstützen, finden Sie unterCIS AWS Benchmark v1.4.0.

Themen

Was ist CIS?

Die CIS ist eine gemeinnützige Organisation, die den CIS AWS Foundations Benchmark entwickelt hat. Dieser Benchmark dient als eine Reihe von bewährten Methoden zur Sicherheitskonfiguration

für AWS. Diese branchenweit anerkannten Best Practices gehen über die bereits verfügbaren allgemeinen Sicherheitsrichtlinien hinaus, da sie Ihnen klare step-by-step Implementierungs- und Bewertungsverfahren bieten.

Weitere Informationen finden Sie in den Benchmark-Blogbeiträgen der CIS AWS Foundations im AWS Security Blog.

Unterschied zwischen CIS-Benchmarks und CIS Controls

CIS-Benchmarks sind Best Practices-Richtlinien für Sicherheitsverfahren, die speziell für Herstellerprodukte gelten. Die Einstellungen, die anhand eines Benchmarks angewendet werden, reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und schützen die spezifischen Systeme, die Ihr Unternehmen verwendet. CIS Controls sind grundlegende Best Practices und Richtlinien für Systeme auf Unternehmensebene, die Sie befolgen müssen, um sich vor bekannten Cyberangriffsvektoren zu schützen.

Beispiele

- CIS-Benchmarks sind präskriptiv. Sie beziehen sich in der Regel auf eine bestimmte Einstellung, die im Herstellerprodukt überprüft und festgelegt werden kann.

  Beispiel: CIS AWS Benchmark v1.2.0 — Stellen Sie sicher, dass MFA für das Konto „Root-Benutzer“ aktiviert ist.

  Diese Empfehlung enthält eine Anleitung, wie dies überprüft werden kann und wie dies für das Root-Konto für die Umgebung eingerichtet werden kann. AWS
- CIS Controls gilt unternehmensweit. Sie sind nicht nur für ein Produkt eines Anbieters spezifisch.

  Beispiel: CIS v7.1 — Verwenden Sie die Multi-Faktor-Authentifizierung für alle administrativen Zugriffe

  Diese Kontrolle beschreibt, was voraussichtlich in Ihrem Unternehmen angewendet wird. Es wird nicht beschrieben, wie Sie es auf die Systeme und Workloads anwenden sollten, die Sie ausführen (unabhängig davon, wo sie sich befinden).

Verwendung dieses Frameworks

Sie können die CIS AWS Benchmark v1.2-Frameworks verwenden, AWS Audit Manager um sich auf CIS-Audits vorzubereiten. Sie können diese Frameworks und ihre Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im CIS-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Stufe 1	33	3	4
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Stufe 1 und 2	45	4	4

Important

Um sicherzustellen, dass diese Frameworks die beabsichtigten Beweise sammeln AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass diese Frameworks die beabsichtigten Beweise sammeln AWS Config, stellen Sie sicher, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um eine Liste der AWS Config Regeln zu überprüfen, die als Datenquellenzuordnungen für diese Standard-Frameworks verwendet werden, laden Sie die folgenden Dateien herunter:

1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-V1.2.0, -Level-1.zip
2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-V1.2.0, -Level-1-and-2.zip

Die Kontrollen in diesen Frameworks dienen nicht dazu, zu überprüfen, ob Ihre Systeme den Best Practices von CIS Benchmark entsprechen. AWS Darüber hinaus können sie nicht garantieren, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Voraussetzungen für die Verwendung dieses Frameworks

Viele Kontrollen in den CIS AWS Benchmark v1.2 Frameworks verwenden AWS Config als Datenquellentyp. Um diese Kontrollen zu unterstützen, müssen Sie sie für alle Konten in allen Konten aktivieren AWS Config, in AWS-Region denen Sie Audit Manager aktiviert haben. Sie müssen außerdem sicherstellen, dass bestimmte AWS Config Regeln aktiviert sind und dass diese Regeln korrekt konfiguriert sind.

Die folgenden AWS Config Regeln und Parameter sind erforderlich, um die korrekten Nachweise zu sammeln und einen genauen Compliance-Status für den CIS AWS Foundations Benchmark v1.2 zu ermitteln. Anweisungen zur Aktivierung oder Konfiguration einer Regel finden Sie unter Arbeiten mit AWS Config -verwalteten Regeln.

Erforderliche Regel AWS Config	Erforderliche Parameter
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • Die maximale Anzahl der Tage ohne Rotation. • Typ: Int • Standard (90 Tage) • Compliance-Anforderung: maximal 90 Tage
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Nicht zutreffend
CLOUD_TRAIL_ENCRYPTION_ENABLED	Nicht zutreffend

Erforderliche Regel AWS Config	Erforderliche Parameter
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Nicht zutreffend
CMK_BACKING_KEY_ROTATION_ENABLED	Nicht zutreffend
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (Optional) • Anzahl der Tage bis zum Ablauf des Passworts. • Typ: int • Standard: 90 • Compliance-Anforderung: maximal 90 Tage
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (Optional) • Die Mindestlänge des Passworts. • Typ: int • Standard: 14 • Compliance-Anforderung: mindestens 14 Zeichen
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (Optional) • Die Anzahl der Passwörter vor der Wiederverwendung. • Typ: int • Standard: 24 • Compliance-Anforderung: mindestens 24 Passwörter vor der Wiederverwendung
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (Optional) • Verlangen Sie mindestens einen Kleinbuchstaben im Passwort. • Typ: Boolescher Wert • Standard: True • Passwortanforderung: mindestens ein Kleinbuchstabe

Erforderliche Regel AWS Config	Erforderliche Parameter
IAM_PASSWORD_POLICY	**`RequireNumbers`** (Optional) • Verlangen Sie mindestens eine Zahl im Passwort. • Typ: Boolescher Wert • Standard: True • Compliance-Anforderungen: mindestens eine Ziffer
IAM_PASSWORD_POLICY	**`RequireSymbols`** (Optional) • Verlangen Sie mindestens ein Symbol im Passwort. • Typ: Boolescher Wert • Standard: True • Compliance-Anforderung: mindestens ein Sonderzeichen
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (Optional) • Verlangen Sie mindestens einen Großbuchstaben im Passwort. • Typ: Boolescher Wert • Standard: True • Compliance-Anforderung: mindestens ein Großbuchstabe

Erforderliche Regel AWS Config	Erforderliche Parameter
IAM_POLICY_IN_USE	**`policyARN`** • Ein zu überprüfender IAM-Richtlinien-ARN. • Typ: Zeichenfolge • Compliance-Anforderung: Erstellt eine IAM-Rolle für die Verwaltung von Vorfällen mit AWS. **`policyUsageType`** (Optional) • Gibt an, ob die Richtlinie mit einer Gruppe oder einer Rolle verknüpft werden soll. • Typ: Zeichenfolge • Zulässige Werte: `IAM_USER` | `IAM_GROUP` | `IAM_ROLE` | `ANY` • Standardwert: `ANY` • Compliance-Anforderungen: Ordnen Sie der erstellten IAM-Rolle die Vertrauensrichtlinie zu
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	Nicht zutreffend
IAM_ROOT_ACCESS_KEY_CHECK	Nicht zutreffend
IAM_USER_NO_POLICIES_CHECK	Nicht zutreffend
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • Die maximale Anzahl der Tage, für die ein Berechtigungsnachweis nicht verwendet werden kann. • Typ: Int • Standard (90 Tage) • Compliance-Anforderung: mind. 90 Tage
INCOMING_SSH_DISABLED	Nicht zutreffend

Erforderliche Regel AWS Config	Erforderliche Parameter
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Nicht zutreffend
MULTI_REGION_CLOUD_TRAIL_ENABLED	Nicht zutreffend

Erforderliche Regel AWS Config	Erforderliche Parameter
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (Optional) • Blockierte TCP-Port-Nummer. • Typ: int • Standard: 20 • Compliance-Anforderung: Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff auf blockierte Ports zulassen **`blockedPort2`** (Optional) • Blockierte TCP-Port-Nummer. • Typ: int • Standard: 21 • Compliance-Anforderung: Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff auf blockierte Ports zulassen **`blockedPort3`** (Optional) • Blockierte TCP-Port-Nummer. • Typ: int • Standard: 3389 • Compliance-Anforderung: Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff auf blockierte Ports zulassen **`blockedPort4`** (Optional) • Blockierte TCP-Port-Nummer. • Typ: int • Standard: 3306 • Compliance-Anforderung: Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff auf blockierte Ports zulassen **`blockedPort5`** (Optional) • Blockierte TCP-Port-Nummer.

Erforderliche Regel AWS Config	Erforderliche Parameter
	• Typ: int • Standard: 4333 • Compliance-Anforderung: Stellen Sie sicher, dass keine Sicherheitsgruppen den Zugriff auf blockierte Ports zulassen
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	Nicht zutreffend
ROOT_ACCOUNT_MFA_ENABLED	Nicht zutreffend
S3_BUCKET_LOGGING_ENABLED	**`targetBucket`** (Optional) • Der S3-Ziel-Bucket zum Speichern von Serverzugriffsprotokollen. • Typ: Zeichenfolge • Compliance-Anforderungen: Aktivieren Sie die Protokollierung **`targetPrefix`** (Optional) • Das Präfix des S3-Ziel-Buckets zum Speichern von Serverzugriffsprotokollen. • Typ: Zeichenfolge • Compliance-Anforderung: Identifizieren Sie den S3-Bucket für CloudTrail die Protokollierung
S3_BUCKET_PUBLIC_READ_PROHIBITED	Nicht zutreffend
VPC_DEFAULT_SECURITY_GROUP_CLOSED	Nicht zutreffend

Erforderliche Regel AWS Config	Erforderliche Parameter
VPC_FLOW_LOGS_ENABLED	**`trafficType`** (Optional) • Die `trafficType` des Flussprotokolls. • Typ: Zeichenfolge • Compliance-Anforderungen: Die Flow-Protokollierung ist aktiviert

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesen Frameworks, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieser Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- Der Benchmark v1.2.0 der CIS AWS Foundations
- CIS AWS Benchmark Blog-Posts im AWS Security Blog

AWS CIS-Benchmark v1.3.0

AWS Audit Manager bietet zwei vorgefertigte Standard-Frameworks, die den CIS AWS Benchmark v1.3 unterstützen.

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version 1.2.0 unterstützen, finden Sie unterCIS AWS Benchmark v1.2.0.

- Informationen zu den Audit Manager-Frameworks, die Version 1.4.0 unterstützen, finden Sie unterCIS AWS Benchmark v1.4.0.

Themen

Was ist der AWS CIS Benchmark?

Die CIS hat den CIS AWS Foundations Benchmark v1.3.0 entwickelt, eine Reihe von bewährten Methoden zur Sicherheitskonfiguration für AWS. Diese in der Branche anerkannten bewährten Verfahren gehen über die bereits verfügbaren allgemeinen Sicherheitsrichtlinien hinaus, da sie den AWS Benutzern klare step-by-step Implementierungs- und Bewertungsverfahren bieten.

Weitere Informationen finden Sie in den Benchmark-Blogbeiträgen der CIS AWS Foundations im AWS Security Blog.

CIS AWS Benchmark v1.3.0 bietet Anleitungen zur Konfiguration von Sicherheitsoptionen für eine Teilmenge von, AWS-Services wobei der Schwerpunkt auf grundlegenden, testbaren und architekturunabhängigen Einstellungen liegt. Einige der spezifischen Amazon Web Services, die in diesem Dokument behandelt werden, umfassen Folgendes:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon Simple Storage Service (Amazon-S3)
- Amazon Virtual Private Cloud (Standard)

Unterschied zwischen CIS-Benchmarks und CIS Controls

CIS-Benchmarks sind Best Practices-Richtlinien für Sicherheitsverfahren, die speziell für Herstellerprodukte gelten. Die Einstellungen, die anhand eines Benchmarks angewendet werden, reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und schützen die Systeme, die Ihr Unternehmen verwendet. CIS Controls sind grundlegende Best Practices und Richtlinien für Systeme auf Unternehmensebene, die Sie befolgen müssen, um sich vor bekannten Cyberangriffsvektoren zu schützen.

Beispiele

- CIS-Benchmarks sind präskriptiv. Sie beziehen sich in der Regel auf eine bestimmte Einstellung, die im Herstellerprodukt überprüft und festgelegt werden kann.

  Beispiel: CIS AWS Benchmark v1.3.0 — Stellen Sie sicher, dass MFA für das Konto „Root-Benutzer“ aktiviert ist

  Diese Empfehlung enthält eine Anleitung, wie dies überprüft werden kann und wie dies für das Root-Konto für die Umgebung eingerichtet werden kann. AWS
- CIS Controls gelten für Ihr gesamtes Unternehmen und beziehen sich nicht nur auf ein Produkt eines Anbieters.

  Beispiel: CIS v7.1 — Verwenden Sie die Multi-Faktor-Authentifizierung für alle administrativen Zugriffe

  Diese Kontrolle beschreibt, was in Ihrem Unternehmen voraussichtlich angewendet wird, aber nicht, wie Sie es auf die Systeme und Workloads anwenden sollten, die Sie ausführen (unabhängig davon, wo sie sich befinden).

Verwendung dieses Frameworks

Sie können die CIS AWS Benchmark v1.3-Frameworks verwenden, AWS Audit Manager um sich auf CIS-Audits vorzubereiten. Sie können diese Frameworks und ihre Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im CIS-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen

und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Stufe 1	32	5	5
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Stufe 1 und 2	49	6	5

Important

Um sicherzustellen, dass diese Frameworks die beabsichtigten Beweise sammeln AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass diese Frameworks die beabsichtigten Beweise sammeln AWS Config, stellen Sie sicher, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um eine Liste der AWS Config Regeln zu überprüfen, die als Datenquellenzuordnungen für diese Standard-Frameworks verwendet werden, laden Sie die folgenden Dateien herunter:

1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-V1.3.0, -Level-1.zip
2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-V1.3.0, -Level-1-and-2.zip

Die Kontrollen in diesen Frameworks dienen nicht dazu, zu überprüfen, ob Ihre Systeme den Best Practices von CIS Benchmark entsprechen. AWS Darüber hinaus können sie nicht garantieren, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesen Frameworks, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieser Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- CIS AWS Benchmark Blog-Posts im AWS Security Blog

CIS AWS Benchmark v1.4.0

AWS Audit Manager bietet zwei vorgefertigte Standard-Frameworks, die den Benchmark v1.4.0 der Center for Internet Security (CIS) AWS Foundations unterstützen.

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version 1.2.0 unterstützen, finden Sie unterCIS AWS Benchmark v1.2.0.
> - Informationen zu den Audit Manager-Frameworks, die Version 1.3.0 unterstützen, finden Sie unterAWS CIS-Benchmark v1.3.0.

Themen

- Was ist der CIS AWS Benchmark?

Was ist der CIS AWS Benchmark?

Der CIS AWS Benchmark v1.4.0 bietet präskriptive Leitlinien für die Konfiguration von Sicherheitsoptionen für eine Teilmenge von Amazon Web Services. Der Schwerpunkt liegt auf grundlegenden, testbaren und architekturunabhängigen Einstellungen. Einige der spezifischen Amazon Web Services, die in diesem Dokument behandelt werden, umfassen Folgendes:

- AWS Identity and Access Management (IAM)
- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon-Simple-Notification-Service (Amazon-SNS)
- Amazon Simple Storage Service (Amazon-S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Unterschied zwischen CIS-Benchmarks und CIS Controls

CIS-Benchmarks sind Best Practices-Richtlinien für Sicherheitsverfahren, die speziell für Herstellerprodukte gelten. Die Einstellungen, die anhand eines Benchmarks angewendet werden, reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und schützen die verwendeten Systeme. CIS Controls sind grundlegende Best Practices und Richtlinien für Systeme auf Unternehmensebene, die Sie befolgen müssen, um sich vor bekannten Cyberangriffsvektoren zu schützen.

Beispiele

- CIS-Benchmarks sind präskriptiv. Sie beziehen sich in der Regel auf eine bestimmte Einstellung, die im Herstellerprodukt überprüft und festgelegt werden kann.

Beispiel: CIS AWS Benchmark v1.3.0 — Stellen Sie sicher, dass MFA für das Konto „Root-Benutzer“ aktiviert ist

Diese Empfehlung enthält eine Anleitung, wie dies überprüft werden kann und wie dies für das Root-Konto für die Umgebung eingerichtet werden kann. AWS

- CIS Controls gelten für Ihr gesamtes Unternehmen und beziehen sich nicht nur auf ein Produkt eines Anbieters.

  Beispiel: CIS v7.1 — Verwenden Sie die Multi-Faktor-Authentifizierung für alle administrativen Zugriffe

  Diese Kontrolle beschreibt, was voraussichtlich in Ihrem Unternehmen angewendet wird. Es wird jedoch nicht beschrieben, wie Sie es auf die Systeme und Workloads anwenden, die Sie ausführen (unabhängig davon, wo sie sich befinden).

Verwenden Sie diese Frameworks zur Unterstützung Ihrer Audit-Vorbereitung

Sie können die CIS AWS Benchmark v1.4.0-Frameworks verwenden AWS Audit Manager , um sich auf CIS-Audits vorzubereiten. Sie können diese Frameworks und ihre Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im CIS-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Stufe 1	32	6	5
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Stufe 1 und 2	50	8	5

Important

Um sicherzustellen, dass diese Frameworks die beabsichtigten Beweise sammeln AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass diese Frameworks die beabsichtigten Beweise sammeln AWS Config, stellen Sie sicher, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um eine Liste der AWS Config Regeln zu überprüfen, die als Datenquellenzuordnungen für diese Standard-Frameworks verwendet werden, laden Sie die folgenden Dateien herunter:

1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-Version 1.4.0, -Level-1.zip
2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-Version 1.4.0, -Level-1-and-2.zip

Die Kontrollen in diesen Frameworks dienen nicht dazu, zu überprüfen, ob Ihre Systeme dem CIS-Benchmark v1.4.0 entsprechen. AWS Darüber hinaus können sie nicht garantieren, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Eine Anleitung, wie Sie detaillierte Informationen zu diesen Frameworks, einschließlich der Liste der darin enthaltenen Standardkontrollen, einsehen können, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieser Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- CIS Benchmarks vom Center for Internet Security
- CIS AWS Benchmark Blog-Posts im AWS Security Blog

CIS Controls v7.1, IG1

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das Center for Internet Security (CIS) v7.1 Implementation Group 1 unterstützt.

> **Note**
>
> Informationen zu CIS v8, IG1and dem AWS Audit Manager Framework, das diesen Standard unterstützt, finden Sie unter. CIS Critical Security Controls Version 8.0, IG1

Themen

Was sind CIS Controls?

Bei den CIS-Kontrollen handelt es sich um eine Reihe priorisierter Maßnahmen, die zusammen eine defense-in-depth Reihe von bewährten Verfahren bilden. Mit diesen Best Practices können die häufigsten Angriffe auf Systeme und Netzwerke abgewehrt werden. Implementierungsgruppe 1 wird im Allgemeinen für Unternehmen definiert, die nur über begrenzte Ressourcen und Cybersicherheitsexpertise für die Implementierung von Sub-Controls verfügen.

Unterschied zwischen CIS Controls und CIS-Benchmarks

Bei CIS Controls handelt es sich um grundlegende Best Practices und Richtlinien, an die sich ein Unternehmen halten kann, um sich vor bekannten Cyberangriffsvektoren zu schützen. CIS-Benchmarks sind Best Practices-Richtlinien für Sicherheitsverfahren speziell für Herstellerprodukte. Die Einstellungen, die anhand eines Benchmarks angewendet werden, reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und schützen die verwendeten Systeme.

Beispiele

- CIS-Benchmarks sind präskriptiv. Sie beziehen sich in der Regel auf eine bestimmte Einstellung, die im Herstellerprodukt überprüft und festgelegt werden kann.
  - Beispiel: CIS AWS Benchmark v1.2.0 — Stellen Sie sicher, dass MFA für das Konto „Root-Benutzer“ aktiviert ist
  - Diese Empfehlung enthält eine Anleitung, wie dies überprüft werden kann und wie dies für das Root-Konto für die Umgebung eingerichtet werden kann. AWS
- CIS Controls gelten für Ihr gesamtes Unternehmen und beziehen sich nicht nur auf ein Produkt eines Anbieters.
  - Beispiel: CIS v7.1 — Verwenden Sie die Multi-Faktor-Authentifizierung für alle administrativen Zugriffe
  - Diese Kontrolle beschreibt, was voraussichtlich in Ihrem Unternehmen angewendet wird. Es informiert Sie jedoch nicht, wie Sie es auf die Systeme und Workloads anwenden sollten, die Sie ausführen (unabhängig davon, wo sie sich befinden).

Verwendung dieses Frameworks

Sie können das CIS Controls IG1 v7.1-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und

Testverfahren. Diese Kontrollen sind gemäß den CIS-Anforderungen in Kontrollsätze eingeordnet. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im CIS Controls IG1 v7.1-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Einzelheiten des CIS Controls IG1 v7.1-Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Zentrum für Internetsicherheit (CIS) v7.1, IG1	8	35	18

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ ConfigDataSourceMappings _Center-for-Internet-Security- (CIS) -v7.1, - .zip herunter. IG1

Die Kontrollen in diesem Framework dienen nicht zur Überprüfung, ob Ihre Systeme mit CIS Controls konform sind. Darüber hinaus garantieren sie nicht, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- CIS Controls v7.1 IG1

CIS Critical Security Controls Version 8.0, IG1

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das CIS Critical Security Controls Version 8.0, Implementierungsgruppe 1, unterstützt.

> **Note**
>
> Informationen zu CIS v7.1 IG1 und dem AWS Audit Manager Framework, das diesen Standard unterstützt, finden Sie unter. CIS Controls v7.1, IG1

Themen

- Weitere Ressourcen

Was sind CIS Controls?

Bei den CIS Critical Security Controls (CIS Controls) handelt es sich um ein priorisiertes Maßnahmenpaket zur Abwehr der häufigsten Cyberangriffe auf Systeme und Netzwerke. Sie sind in zahlreichen rechtlichen, regulatorischen und politischen Rahmenwerken verankert und werden von diesen referenziert. CIS Controls v8 wurde verbessert, um mit modernen Systemen und Software Schritt zu halten. Die Umstellung auf cloudbasiertes Computing, Virtualisierung, Mobilität work-from-home, Outsourcing und veränderte Taktiken der Angreifer waren der Grund für das Update. Dieses Update unterstützt die Sicherheit von Unternehmen, die sowohl vollständig auf Cloud- als auch auf Hybridumgebungen umsteigen.

Unterschied zwischen CIS Controls und CIS-Benchmarks

Bei CIS Controls handelt es sich um grundlegende Best Practices und Richtlinien, an die sich ein Unternehmen halten kann, um sich vor bekannten Cyberangriffsvektoren zu schützen. CIS-Benchmarks sind Best Practices-Richtlinien für Sicherheitsverfahren speziell für Herstellerprodukte. Die Einstellungen, die anhand eines Benchmarks angewendet werden, reichen von Betriebssystemen über Cloud-Dienste bis hin zu Netzwerkgeräten und schützen die verwendeten Systeme.

Beispiele

- CIS-Benchmarks sind präskriptiv. Sie beziehen sich in der Regel auf eine bestimmte Einstellung, die im Herstellerprodukt überprüft und festgelegt werden kann.
  - Beispiel: CIS AWS Benchmark v1.2.0 — Stellen Sie sicher, dass MFA für das Konto „Root-Benutzer“ aktiviert ist
  - Diese Empfehlung enthält eine Anleitung, wie dies überprüft werden kann und wie dies für das Root-Konto für die Umgebung eingerichtet werden kann. AWS
- CIS Controls gelten für Ihr gesamtes Unternehmen und beziehen sich nicht nur auf ein Produkt eines Anbieters.
  - Beispiel: CIS v7.1 — Verwenden Sie die Multi-Faktor-Authentifizierung für alle administrativen Zugriffe
  - Diese Kontrolle beschreibt, was voraussichtlich in Ihrem Unternehmen angewendet wird. Es informiert Sie jedoch nicht, wie Sie es auf die Systeme und Workloads anwenden sollten, die Sie ausführen (unabhängig davon, wo sie sich befinden).

Verwendung dieses Frameworks

Sie können das CIS IG1 v8-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den CIS-Anforderungen in Kontrollsätze eingeordnet. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im CIS v8-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
CIS Critical Security Controls Version 8.0 (CIS v8.0), IG1	11	45	15

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als

Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ ConfigDataSourceMappings _CIS-Critical-Security-Controls-Version-8.0- (CIS-v8.0), - .zip herunter. IG1

Die Kontrollen in diesem Framework dienen nicht zur Überprüfung, ob Ihre Systeme mit CIS Controls konform sind. Darüber hinaus garantieren sie nicht, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- CIS Controls v8

FedRAMP Security Baseline Controls r4

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das die Security Baseline Controls r4 des Federal Risk And Authorization Management Program (FedRAMP) unterstützt.

Themen

Was ist FedRAMP?

FedRAMP wurde 2011 gegründet. Es bietet einen kostengünstigen, risikobasierten Ansatz für die Einführung und Nutzung von Cloud-Diensten durch die US-Bundesregierung. FedRAMP ermöglicht es Bundesbehörden, moderne Cloud-Technologien zu nutzen, wobei der Schwerpunkt auf der Sicherheit und dem Schutz von Bundesinformationen liegt.

Weitere Informationen über FedRAMP Moderate Baseline Controls finden Sie in der Vorlage FedRAMP Moderate Security Testfall-Verfahren.

Verwendung dieses Frameworks

Sie können das FedRAMP r4-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Steuerelemente sind gemäß den FedRAMP r4-Anforderungen in Steuersätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details des FedRAMP Moderate Baseline-Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Sicherheitsbasiskontrollen des Federal Risk and Authorization Managemen	36	289	17

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
t Program (FedRAMP) r4, moderat			

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _FedRAMP-Security-Baseline-Controls-r4-Moderate.zip herunter.

Die Kontrollen in diesem Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme FedRAMP r4-konform sind. Darüber hinaus können sie nicht garantieren, dass Sie ein FedRAMP-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- AWS Compliance-Seite für FedRAMP
- AWS FedRAMP-Blogbeiträge

GDPR 2016

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das die Allgemeine Datenschutzverordnung (DSGVO) 2016 unterstützt.

Dieses Framework enthält nur manuelle Kontrollen. Bei diesen manuellen Kontrollen werden Beweise nicht automatisch gesammelt. Wenn Sie jedoch die Beweiserhebung für einige Kontrollen im Rahmen der DSGVO automatisieren möchten, können Sie die benutzerdefinierte Kontrollfunktion in Audit Manager verwenden. Weitere Informationen finden Sie unter Verwendung dieses Frameworks.

Themen

Was ist die DSGVO?

Die DSGVO ist ein europäisches Datenschutzgesetz, das am 25. Mai 2018 durchsetzbar wurde. Die DSGVO ersetzt die EU-Datenschutzrichtlinie, auch bekannt als Richtlinie 95/46/EG. Sie soll die Datenschutzgesetze in der gesamten Europäischen Union (EU) vereinheitlichen. Dies geschieht durch die Anwendung eines einzigen Datenschutzgesetzes, das in jedem EU-Mitgliedstaat verbindlich ist.

Die DSGVO gilt für alle Organisationen, die in der EU ansässig sind, und für Organisationen (unabhängig davon, ob sie in der EU ansässig sind), die die personenbezogenen Daten von betroffenen Personen in der EU entweder im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen in der EU oder der Überwachung des Verhaltens innerhalb der EU verarbeiten. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Sie finden das DSGVO-Framework auf der Framework-Bibliotheksseite von Audit Manager. Weitere Informationen finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Verwendung dieses Frameworks

Sie können das GDPR 2016-Framework in Audit Manager verwenden, um sich auf Audits vorzubereiten.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Allgemeine Datenschutzverordnung (DSGVO) 2016	0	378	10

Dieses Standard-Framework enthält nur manuelle Steuerungen.

> **Note**
>
> Wenn Sie die Beweissuche für die DSGVO automatisieren möchten, können Sie Audit Manager verwenden, um Ihre eigenen benutzerdefinierten Kontrollen für die DSGVO zu erstellen. Die folgende Tabelle enthält Empfehlungen zu den AWS Datenquellen, die Sie in Ihren benutzerdefinierten Steuerelementen den DSGVO-Anforderungen zuordnen können. Obwohl einige der folgenden Datenquellen mehreren Kontrollen zugeordnet sind, sollten Sie bedenken, dass Ihnen jede Ressourcenbewertung nur einmal in Rechnung gestellt wird.
> In den folgenden Empfehlungen werden AWS Config und AWS Security Hub CSPM als Datenquellen verwendet. Um erfolgreich Beweise aus diesen Datenquellen zu sammeln, stellen Sie sicher, dass Sie die Anweisungen zur Aktivierung AWS Config und Einrichtung sowie AWS Security Hub CSPM in Ihrem befolgt haben AWS-Konto. Nachdem Sie beide Dienste auf diese Weise eingerichtet haben, sammelt Audit Manager bei jeder Bewertung der angegebenen AWS Config Regel oder Security Hub CSPM-Steuerung Nachweise.

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.1	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das dieses DSGVO-Steuerelement unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an • AWS CloudTrail Bucket ist nicht öffentlich • Zeigt alle Richtlinien mit einem `Allow:*:*` an und listet alle Prinzipale und Services auf, die diese Richtlinien verwenden Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie die folgenden Security Hub-Steuerelemente als Datenquellenzuordnungen aus: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2,2 (CloudTrail.4) • 2,3 (CloudTrail.6) • CloudTrail2,4 (,5) • 2.5 (Config.1) • 2,6 (CloudTrail,7) • 2,7 (CloudTrail,2) • 2.8 (KMS.4) • 2,9 (EC22,6) • 3,1 (CloudWatch,2) • 3,10 (CloudWatch0,10) • 3,11 (,11) CloudWatch • 3,12 (,12) CloudWatch

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 3,13 (,13) CloudWatch • 3,14 (,14) CloudWatch • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.2	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das diese DSGVO-Steuerung unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an • AWS CloudTrail Bucket ist nicht öffentlich • Zeigt alle Richtlinien mit einem `Allow:*:*` an und listet alle Prinzipale und Services auf, die diese Richtlinien verwenden Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie die folgenden Security Hub-Steuerelemente als Datenquellenzuordnungen aus: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2,2 (CloudTrail.4) • 2,3 (CloudTrail.6) • CloudTrail2,4 (,5) • 2.5 (Config.1) • 2,6 (CloudTrail,7) • 2,7 (CloudTrail,2) • 2.8 (KMS.4) • 2,9 (EC22,6) • 3,1 (CloudWatch,2) • 3,10 (CloudWatch0,10) • 3,11 (,11) CloudWatch • 3,12 (,12) CloudWatch

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 3,13 (,13) CloudWatch • 3,14 (,14) CloudWatch • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.3	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das diese DSGVO-Steuerung unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an • AWS CloudTrail Bucket ist nicht öffentlich • Zeigt alle Richtlinien mit einem `Allow:*:*` an und listet alle Prinzipale und Services auf, die diese Richtlinien verwenden Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie die folgenden Security Hub-Steuerelemente als Datenquellenzuordnungen aus: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2,2 (CloudTrail.4) • 2,3 (CloudTrail.6) • CloudTrail2,4 (,5) • 2.5 (Config.1) • 2,6 (CloudTrail,7) • 2,7 (CloudTrail,2) • 2.8 (KMS.4) • 2,9 (EC22,6) • 3,1 (CloudWatch,2) • 3,10 (CloudWatch0,10) • 3,11 (,11) CloudWatch • 3,12 (,12) CloudWatch

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 3,13 (,13) CloudWatch • 3,14 (,14) CloudWatch • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 30 Aufzeichnungen über Prozessaktivitäten.1	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das diese DSGVO-Steuerung unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie das folgende Security Hub-Steuerelement als Datenquellenzuordnung aus: • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 30 Aufzeichnungen über Prozessaktivitäten.2	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das dieses DSGVO-Steuerelement unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie das folgende Security Hub-Steuerelement als Datenquellenzuordnung aus: • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 30 Aufzeichnungen über Prozessaktivitäten.3	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das dieses DSGVO-Steuerelement unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an • AWS CloudTrail Bucket ist nicht öffentlich • Zeigt alle Richtlinien mit einem `Allow:*:*` an und listet alle Prinzipale und Services auf, die diese Richtlinien verwenden Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie das folgende Security Hub-Steuerelement als Datenquellenzuordnung aus: • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 30 Aufzeichnungen über Prozessaktivitäten.4	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das dieses DSGVO-Steuerelement unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an • AWS CloudTrail Bucket ist nicht öffentlich • Zeigt alle Richtlinien mit einem `Allow:*:*` an und listet alle Prinzipale und Services auf, die diese Richtlinien verwenden Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie das folgende Security Hub-Steuerelement als Datenquellenzuordnung aus: • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 30 Aufzeichnungen über Prozessaktivitäten.5	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das dieses DSGVO-Steuerelement unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Zeigt alle Ereignisse des Root-Kontos während der Laufzeit an Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Wählen Sie AWS Security Hub CSPM als Datenquellentyp und wählen Sie das folgende Security Hub-Steuerelement als Datenquellenzuordnung aus: • Config.1

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 32 Sicherheit der Verarbeitung.1	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen AWS Audit Manager , das dieses DSGVO-Steuerelement unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Verschlüsselung von Daten im Ruhezustand für alle Services anzeigen • Verschlüsselung der Daten während der Übertragung für alle Service anzeigen • MFA Delete für Amazon S3 aktiviert • Alle Amazon Inspector Scans • Alle Instances anzeigen, für die Amazon Inspector nicht aktiviert ist • Zeigt alle Load Balancer an, die HTTPS (SSL) abhören • AWS CloudTrail im Ruhezustand verschlüsselt • CloudWatch Amazon-Benachrichtigungen zur AWS Config Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_AKTIVIERT • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• API_GW_CACHE_AKTIVIERT_UND_VERSCHLÜSSELT

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 32 Sicherheit der Verarbeitung.2	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen, das dieses DSGVO-Steuerelement unterstützt. AWS Audit Manager Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Verschlüsselung von Daten im Ruhezustand für alle Services anzeigen • Verschlüsselung der Daten während der Übertragung für alle Service anzeigen • MFA Delete für Amazon S3 aktiviert • Alle Amazon Inspector Scans • Alle Instances anzeigen, für die Amazon Inspector nicht aktiviert ist • Zeigt alle Load Balancer an, die HTTPS (SSL) abhören • AWS CloudTrail im Ruhezustand verschlüsselt • CloudWatch Amazon-Benachrichtigungen zur AWS Config Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_AKTIVIERT • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• API_GW_CACHE_AKTIVIERT_UND_VERSCHLÜSSELT

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 32 Sicherheit der Verarbeitung.3	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen, das dieses DSGVO-Steuerelement unterstützt. AWS Audit Manager Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Verschlüsselung von Daten im Ruhezustand für alle Services anzeigen • Verschlüsselung der Daten während der Übertragung für alle Service anzeigen • MFA Delete für Amazon S3 aktiviert • Alle Amazon Inspector Scans • Alle Instances anzeigen, für die Amazon Inspector nicht aktiviert ist • Zeigt alle Load Balancer an, die HTTPS (SSL) abhören • AWS CloudTrail im Ruhezustand verschlüsselt • CloudWatch Amazon-Benachrichtigungen zur AWS Config Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_AKTIVIERT • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• API_GW_CACHE_AKTIVIERT_UND_VERSCHLÜSSELT

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 32 Sicherheit der Verarbeitung.4	Kapitel 4 – Controller und Prozessor	Sie können ein benutzerdefiniertes Steuerelement erstellen, das dieses DSGVO-Steuerelement unterstützt. AWS Audit Manager Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Verschlüsselung von Daten im Ruhezustand für alle Services anzeigen • Verschlüsselung der Daten während der Übertragung für alle Service anzeigen • MFA Delete für Amazon S3 aktiviert • Alle Amazon Inspector Scans • Alle Instances anzeigen, für die Amazon Inspector nicht aktiviert ist • Zeigt alle Load Balancer an, die HTTPS (SSL) abhören • AWS CloudTrail im Ruhezustand verschlüsselt • CloudWatch Amazon-Benachrichtigungen zur AWS Config Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die folgenden Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnungen aus: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST • ENCRYPTED_VOLUMES

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_AKTIVIERT • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ACM_CERTIFICATE_EXPIRATION_CHECK

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• API_GW_CACHE_AKTIVIERT_UND_VERSCHLÜSSELT

Nachdem Sie Ihre neuen benutzerdefinierten Kontrollen für die DSGVO erstellt haben, können Sie diese zu einem Framework für benutzerdefinierte DSGVO hinzufügen. Sie können eine Bewertung aus einem benutzerdefiniertem DSGVO-Framework erstellen. Auf diese Weise kann Audit Manager automatisch Nachweise für die von Ihnen hinzugefügten benutzerdefinierten Kontrollen sammeln.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- Zentrum für die Datenschutz-Grundverordnung (DSGVO)
- AWS Blogbeiträge zur DSGVO

Gramm-Leach-Bliley Handeln

AWS Audit Manager bietet ein vorgefertigtes Framework, das den Gramm-Leach-Bliley Act (GLBA) unterstützt.

Themen

- Was ist der GLBA?
- Verwendung dieses Frameworks

- Nächste Schritte

Was ist der GLBA?

Der GLBA (oder der GLB Act), auch bekannt als Financial Service Modernization Act von 1999, ist ein Bundesgesetz, das in den Vereinigte Staaten erlassen wurde, um den Umgang von Finanzinstituten mit privaten Informationen von Einzelpersonen zu kontrollieren. Das Gesetz besteht aus drei Abschnitten. Der erste ist die „Financial Privacy Rule“, die die Erfassung und Offenlegung privater Finanzinformationen regelt. Der zweite ist die „Safeguards Rule“, die vorsieht, dass Finanzinstitute Sicherheitsprogramme zum Schutz solcher Informationen implementieren müssen. Beim dritten handelt es sich um die „Pretexting Provisions“, die das Vortäuschen von falschen Tatsachen (mit dem Ziel, private Informationen zu erlangen), verbieten. Nach dem Gesetz müssen Finanzinstitute ihren Kunden auch schriftliche Datenschutzerklärungen aushändigen, in denen ihre Praktiken beim Informationsaustausch erläutert werden.

Verwendung dieses Frameworks

Sie können das GLBA 2016-Framework verwenden, um sich auf Prüfungen vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den GLBA-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das GLBA-Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für ein GLBA-Audit relevant sind. In Ihrer Bewertung können Sie angeben, was Sie in den AWS-Konten Umfang Ihres Audits aufnehmen möchten. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im GLBA-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Gramm-Leach-Bliley Gesetz (GLBA)	0	120	16

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme dem GLBA-Standard entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein GLBA-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Titel 21 CFR Teil 11

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das Titel 21 des Code of Federal Regulations (CFR), Teil 11, Elektronische Aufzeichnungen; elektronische Signaturen — Geltungsbereich und Anwendung, 24. Mai 2023, unterstützt.

Themen

Was ist Titel 21 des CFR Part 11?

GxP bezieht sich auf die Vorschriften und Richtlinien, die für Unternehmen der Biowissenschaften gelten, die Lebensmittel und Medizinprodukte herstellen. Zu den Medizinprodukten, die darunter fallen, gehören Medikamente, medizinische Geräte und medizinische Softwareanwendungen. Die allgemeine Absicht der GxP-Anforderungen besteht darin, sicherzustellen, dass Lebensmittel und Medizinprodukte für Verbraucher sicher sind. Es geht auch darum, die Integrität der Daten zu gewährleisten, die für produktbezogene Sicherheitsentscheidungen verwendet werden.

In den Vereinigte Staaten werden die GxP-Vorschriften von der US-amerikanischen Food and Drug Administration (FDA) durchgesetzt und sind in Titel 21 des Code of Federal Regulations (21 CFR) enthalten. Teil 11 von 21 CFR enthält die Anforderungen an Computersysteme, die elektronische Aufzeichnungen und elektronische Signaturen zur Unterstützung von GxP-regulierten Aktivitäten erstellen, ändern, verwalten, archivieren, abrufen oder verteilen. Teil 11 wurde geschaffen, um die Einführung neuer Informationstechnologien durch von der FDA regulierte Organisationen der Biowissenschaften zu ermöglichen und gleichzeitig einen Rahmen zu schaffen, der sicherstellt, dass die elektronischen GxP-Daten vertrauenswürdig und zuverlässig sind.

Einen umfassenden Ansatz zur Nutzung der AWS Cloud für GxP-Systeme finden Sie im Whitepaper Überlegungen zur Verwendung von AWS Produkten in GxP-Systemen.

Verwendung dieses Frameworks

Sie können das Title 21 CFR Part 11-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den CFR-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im Rahmen von Title 21 CFR Part 11 definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen

einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Titel 21 Code of Federal Regulations (CFR) Teil 11, Elektronische Aufzeichnungen; Elektronische Signaturen — Geltungsbereich und Anwendung 24. Mai 2023	6	19	2

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _Title-21-CFR-Part-11.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den GxP-Vorschriften entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- AWS Compliance-Seite für GxP
- Überlegungen zur Verwendung von AWS Produkten in GxP-Systemen

EU GMP Anhang 11, v1

AWS Audit Manager bietet einen vorgefertigten Rahmen, der die EudraLex Vorschriften für Arzneimittel in der Europäischen Union (EU) — Band 4: Gute Herstellungspraxis (GMP) für Human- und Tierarzneimittel — Anhang 11 unterstützt.

Themen

- Was ist der EU-GMP-Anhang 11?
- Verwendung dieses Frameworks
- Nächste Schritte

Was ist der EU-GMP-Anhang 11?

Das EU-GMP Annex 11-Framework ist das europäische Äquivalent zum Title 21 CFR Part 11-Framework in den Vereinigte Staaten. Dieser Anhang gilt für alle Arten von Computersystemen, die im Rahmen von Tätigkeiten eingesetzt werden und im Rahmen der guten Herstellungspraxis (GMP) reguliert werden. Ein computergestütztes System besteht aus einer Reihe von Software-

und Hardwarekomponenten, die zusammen bestimmte Funktionen erfüllen. Die Anwendung sollte validiert und die IT-Infrastruktur qualifiziert sein. Wenn ein computergestütztes System eine manuelle Bedienung ersetzt, sollte dies nicht zu einer Beeinträchtigung der Produktqualität, der Prozesskontrolle oder der Qualitätssicherung führen. Das Gesamtrisiko des Prozesses sollte nicht erhöht werden.

Anhang 11 ist Teil der europäischen GMP-Richtlinien und definiert die Leistungsbeschreibung für computergestützte Systeme, die von Organisationen der Pharmaindustrie verwendet werden. Anhang 11 dient als Checkliste, anhand derer die europäischen Aufsichtsbehörden die Anforderungen an computergestützte Systeme für pharmazeutische Produkte und Medizinprodukte festlegen können. Die von der Kommission der Europäischen Ausschüsse festgelegten Richtlinien sind nicht allzu weit von der FDA entfernt (Titel 21 CFR Part 11). In Anhang 11 sind die Kriterien festgelegt, nach denen elektronische Aufzeichnungen und elektronische Signaturen als verwaltet gelten.

Verwendung dieses Frameworks

Sie können den EU-GMP-Anhang 11-Rahmen verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den GMP-Anforderungen der EU in Kontrollsätze zusammengefasst. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im EU-GMP-Rahmen nach Anhang 11 definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
EudraLex - Die Vorschriften für Arzneimittel in der Europäischen Union (EU) - Band 4: Gute Herstellungspraxis (GMP) Arzneimittel für Human- und Tierarzneimittel - Anhang 11	0	32	3

> **Important**
>
> Stellen Sie sicher, dass Sie die erforderlichen AWS Config Regeln aktivieren AWS Config, um sicherzustellen, dass in diesem Rahmen die beabsichtigten Nachweise gesammelt werden. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ ConfigDataSourceMappings _ EudraLex -GMP-Volume-4-Annex-11.zip herunter.

Die Kontrollen in diesem Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme den EU-GMP-Anforderungen von Anhang 11 entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein EU-GMP-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

HIPAA-Sicherheitsregel: Februar 2003

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das die Sicherheitsregel des Health Insurance Portability and Accountability Act (HIPAA) vom Februar 2003 unterstützt.

> **Note**
>
> Informationen zu den HIPAA Final Omnibus Sicherheitsvorschriften 2013 und zum Audit Manager-Framework, das diesen Standard unterstützt, finden Sie unter Endgültige HIPAA Omnibus-Regel.

Themen

Was ist HIPAA und was sind die HIPAA Sicherheitsvorschriften 2003?

HIPAA ist ein Gesetz, das US-Arbeitnehmern hilft, ihren Krankenversicherungsschutz beizubehalten, wenn sie ihren Arbeitsplatz wechseln oder verlieren. Die Gesetzgebung zielt auch darauf ab, elektronische Patientenakten zu fördern, um die Effizienz und Qualität des US-Gesundheitssystems durch einen verbesserten Informationsaustausch zu erhöhen.

Neben der zunehmenden Nutzung elektronischer Patientenakten umfasst HIPAA auch Bestimmungen zum Schutz der Sicherheit und des Datenschutzes geschützter Gesundheitsinformationen (Protected IHealth Information, PHI). PHI umfasst eine sehr breite Bandbreite an personenbezogenen identifizierbaren Gesundheits- und gesundheitsbezogener Daten. Dazu gehören Versicherungs- und Abrechnungsinformationen, Diagnosedaten, Daten zur klinischen Versorgung und Laborergebnisse wie Bilder und Testergebnisse.

Das US-Gesundheitsministerium veröffentlichte im Februar 2003 eine endgültige Sicherheitsvorschrift. Diese Vorschrift legt nationale Standards für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von elektronisch geschützten Gesundheitsinformationen fest.

Die HIPAA-Vorschriften gelten für betroffene juristische Personen. Dazu gehören Krankenhäuser, medizinische Dienstleister, vom Arbeitgeber geförderte Krankenversicherungen, Forschungseinrichtungen und Versicherungsunternehmen, die sich direkt mit Patienten und Patientendaten befassen. Die HIPAA-Anforderung zum Schutz von PHI erstreckt sich auch auf Geschäftspartner.

Weitere Informationen darüber, wie HIPAA und HITECH Gesundheitsinformationen schützen, finden Sie auf der Website zum Datenschutz für Gesundheitsinformationen des US-Gesundheitsministeriums.

Immer mehr Gesundheitsdienstleister, Kostenträger und IT-Experten nutzen AWS nutzungsbasierte Cloud-Dienste, um geschützte Gesundheitsinformationen (PHI) zu verarbeiten, zu speichern und zu übertragen. AWS ermöglicht es betroffenen Unternehmen und ihren Geschäftspartnern, die HIPAA unterliegen, die sichere AWS Umgebung zur Verarbeitung, Pflege und Speicherung geschützter Gesundheitsinformationen zu nutzen.

Anweisungen zur Verarbeitung und Speicherung von Gesundheitsinformationen finden Sie AWS im Whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services.

Verwendung dieses Frameworks

Sie können das Framework HIPAA Sicherheitsvorschriften 2003 verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den HIPAA-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies erfolgt auf der Grundlage der Kontrollen, die im HIPAA-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Sicherheitsregel des Health Insurance Portability and Accountability Act (HIPAA): Februar 2003	24	61	5

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _HIPAA-Security-Rule-Feb-2003.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme dem HIPAA-Standard entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein HIPAA-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- Datenschutz von Gesundheitsinformationen vom US-Gesundheitsministerium
- Die Sicherheitsvorschriften des US-Gesundheitsministeriums
- Erstellen von Architekturen für HIPAA-Sicherheit und -Compliance in Amazon Web Services
- AWS Compliance-Seite für HIPAA

Endgültige HIPAA Omnibus-Regel

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das die Omnibus Final Rule des Health Insurance Portability and Accountability Act (HIPAA) unterstützt.

> **Note**
>
> Informationen zur HIPAA-Sicherheitsregel 2003 und dem AWS Audit Manager Framework, das diesen Standard unterstützt, finden Sie unter. HIPAA-Sicherheitsregel: Februar 2003

Themen

Was ist HIPAA und was sind die HIPAA Final Omnibus Sicherheitsvorschriften?

HIPAA ist ein Gesetz, das US-Arbeitnehmern hilft, den Krankenversicherungsschutz beizubehalten, wenn sie ihren Arbeitsplatz wechseln oder verlieren. Die Gesetzgebung zielt auch darauf ab,

elektronische Patientenakten zu fördern, um die Effizienz und Qualität des US-Gesundheitssystems durch einen verbesserten Informationsaustausch zu erhöhen.

Neben der zunehmenden Nutzung elektronischer Patientenakten umfasst HIPAA auch Bestimmungen zum Schutz der Sicherheit und des Datenschutzes geschützter Gesundheitsinformationen (Protected IHealth Information, PHI). PHI umfasst eine sehr breite Bandbreite an personenbezogenen identifizierbaren Gesundheits- und gesundheitsbezogener Daten. Dazu gehören Versicherungs- und Abrechnungsinformationen, Diagnosedaten, Daten zur klinischen Versorgung und Laborergebnisse wie Bilder und Testergebnisse.

Die endgültigen HIPAA Final Omnibus-Sicherheitsvorschriften, die 2013 in Kraft traten, enthalten eine Reihe von Aktualisierungen aller zuvor verabschiedeten Regeln. Die Änderungen der Regeln für Sicherheit, Datenschutz, Meldung und Durchsetzung von Sicherheitsverstößen sollten die Vertraulichkeit und Sicherheit beim Datenaustausch verbessern.

Die HIPAA-Vorschriften gelten für betroffene juristische Personen. Dazu gehören Krankenhäuser, medizinische Dienstleister, vom Arbeitgeber geförderte Krankenversicherungen, Forschungseinrichtungen und Versicherungsunternehmen, die sich direkt mit Patienten und Patientendaten befassen. Im Rahmen der umfassenden Aktualisierungen gelten viele der HIPAA-Vorschriften, die für betroffene Unternehmen gelten, nun auch für Geschäftspartner.

Weitere Informationen darüber, wie HIPAA und HITECH Gesundheitsinformationen schützen, finden Sie auf der Website zum Datenschutz für Gesundheitsinformationen des US-Gesundheitsministeriums.

Immer mehr Gesundheitsdienstleister, Kostenträger und IT-Experten nutzen AWS nutzungsbasierte Cloud-Dienste, um geschützte Gesundheitsinformationen (PHI) zu verarbeiten, zu speichern und zu übertragen. AWS ermöglicht es betroffenen Unternehmen und ihren Geschäftspartnern, die HIPAA unterliegen, die sichere AWS Umgebung zur Verarbeitung, Pflege und Speicherung geschützter Gesundheitsinformationen zu nutzen. Anweisungen zur Verarbeitung und Speicherung von Gesundheitsinformationen finden Sie AWS im Whitepaper Architecting for HIPAA Security and Compliance on Amazon Web Services.

Verwendung dieses Frameworks

Sie können das HIPAA Omnibus Final Rule Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den HIPAA-Anforderungen in Kontrollsätze

gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies erfolgt auf der Grundlage der Kontrollen, die im HIPAA-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Endgültige Omnibus-Regel des Gesetzes über die Portabilität und Rechenschaftspflicht von Krankenversicherungen (HIPAA)	21	53	5

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-

Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _HIPAA-Omnibus-Final-Rule.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme dem HIPAA-Standard entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein HIPAA-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- Datenschutz von Gesundheitsinformationen vom US-Gesundheitsministerium
- Omnibus HIPAA Rulemaking des US-Ministerium für Gesundheitspflege und Soziale Dienste
- Erstellen von Architekturen für HIPAA-Sicherheit und -Compliance in Amazon Web Services
- AWS Compliance-Seite für HIPAA

ISO/IEC 27001:2013 Anhang A

AWS Audit Manager bietet ein vorgefertigtes Standardframework, das den Anhang A der Internationalen Organisation für Normung (ISO) /IEC 27001:2013 der Internationalen Elektrotechnischen Kommission (IEC) unterstützt.

Themen

ISO/IEC Was ist 27001:2013 Anhang A?

Die Internationale Elektrotechnische Kommission (IEC) und die Internationale Organisation für Normung (ISO) sind beide unabhängige not-for-profit Nichtregierungsorganisationen, die internationale Normen entwickeln und veröffentlichen, die vollständig auf Konsens basieren.

ISO/IEC 27001:2013 Annex A is a security management standard that specifies security management best practices and comprehensive security controls that follow the ISO/IEC27002 Leitlinien für bewährte Verfahren. Dieser internationale Standard legt die Anforderungen für die Einrichtung, Implementierung, Wartung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems in Ihrem Unternehmen fest. Zu diesen Standards gehören Anforderungen an die Bewertung und Behandlung von Informationssicherheitsrisiken, die auf die Bedürfnisse Ihres Unternehmens zugeschnitten sind. Die Anforderungen in diesem internationalen Standard sind allgemein gehalten und sollen für alle Organisationen gelten, unabhängig von Art, Größe oder Natur.

Verwendung dieses Frameworks

Sie können den AWS Audit Manager Rahmen für Anhang A ISO/IEC 27001:2013 verwenden, um sich auf Prüfungen vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den Anforderungen von ISO/IEC 27001:2013 Anhang A in Kontrollsätze zusammengefasst. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Ausgangspunkt verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Nachweisen beginnen, die für ein Audit nach Anhang A ISO/IEC 27001:2013 relevant sind. In Ihrer Bewertung können Sie angeben, welche Punkte Sie in den AWS-Konten Umfang Ihrer Prüfung einbeziehen möchten. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im Rahmenwerk ISO/IEC 27001:2013 in Anhang

A definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Internationale Organisation für Normung (ISO) /Internationale Elektrotechnische Kommission (IEC) 27001:2013 Anhang A	21	93	35

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _ISO-IEC-270012013-Annex-A.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme diesem internationalen Standard entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein ISO/IEC Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- Weitere Informationen zu diesem internationalen Standard finden Sie unter ISO/IEC 27001:2013 im ANSI Webstore.

NIST SP 800-53 Rev. 5

AWS Audit Manager bietet ein vorgefertigtes Framework, das NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations unterstützt.

> **Note**
>
> - Informationen zum Audit Manager Manager-Framework, das NIST SP 800-171 unterstützt, finden Sie unter. NIST SP 800-171 Rev. 2
> - Informationen zum Audit Manager Manager-Framework, das NIST CSF unterstützt, finden Sie unter. NIST Cybersecurity Framework v1.1

Themen

- Weitere Ressourcen

Was ist NIST SP 800-53?

Das National Institute of Standards and Technology (NIST) wurde 1901 gegründet und ist heute Teil des US-Handelsministeriums. NIST ist eines der ältesten Labors für physikalische Wissenschaften in den USA. Der US-Kongress richtete die Behörde ein, um die zu dieser Zeit zweitklassige Messinfrastruktur zu verbessern. Die Infrastruktur stellte eine große Herausforderung für die industrielle Wettbewerbsfähigkeit der USA dar, da sie hinter anderen Wirtschaftsmächten wie Großbritannien und Deutschland zurückgeblieben war.

Die Sicherheitskontrollen von NIST SP 800-53 gelten im Allgemeinen für Informationssysteme der US-Bundesbehörden. Dabei handelt es sich in der Regel um Systeme, die ein formelles Bewertungs- und Autorisierungsverfahren durchlaufen müssen. Dieser Prozess gewährleistet einen ausreichenden Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationssystemen. Dies basiert auf der Sicherheitskategorie und dem Auswirkungsgrad des Systems (niedrig, mittel oder hoch) sowie auf einer Risikoermittlung. Die Sicherheitskontrollen werden aus dem NIST SP 800-53 Sicherheitskontroll-Katalog gewählt, und das System wird auf Grundlage dieser Sicherheitskontrollanforderungen bewertet.

Das NIST SP 800-53-Framework stellt die Sicherheitskontrollen und die zugehörigen Bewertungsverfahren dar, die in NIST SP 800-53 Revision 5 Recommended Security Controls for Federal Information Systems and Organizations definiert sind. Alle inhaltlichen Abweichungen zwischen diesem NIST SP 800-53-Framework und der zuletzt veröffentlichten NIST-Sonderveröffentlichung SP 800-53 (5. Überarb.) finden Sie in den offiziell veröffentlichten Dokumenten, die im NIST Computer Security Resource Center verfügbar sind.

Verwendung dieses Frameworks

Sie können das NIST SP 800-53-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den NIST-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer

AWS Ressourcen. Dies erfolgt auf der Grundlage der Kontrollen, die im NIST SP 800-53-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
NIST 800-53 Rev 5: Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organizations	132	875	20

> **Important**
>
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
> Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _NIST-800-53-Rev-5.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme dem NIST-Standard entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein NIST-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- National Institute of Standards and Technology (NIST)
- NIST Computer Security Resource Center
- AWS Compliance-Seite für NIST

NIST Cybersecurity Framework v1.1

AWS Audit Manager bietet ein vorgefertigtes Framework, das das NIST Cybersecurity Framework (CSF) v1.1 unterstützt.

> **Note**
>
> - Informationen zum Audit Manager Manager-Framework, das NIST SP 800-53 unterstützt, finden Sie unter. NIST SP 800-53 Rev. 5
> - Informationen zum Audit Manager Manager-Framework, das NIST SP 800-171 unterstützt, finden Sie unter. NIST SP 800-171 Rev. 2

Themen

- Was ist das NIST Cybersecurity Framework?
- Verwendung dieses Frameworks

Was ist das NIST Cybersecurity Framework?

Das National Institute of Standards and Technology (NIST) wurde 1901 gegründet und ist heute Teil des US-Handelsministeriums. NIST ist eines der ältesten Labors für physikalische Wissenschaften in den USA. Der US-Kongress richtete die Behörde ein, um die zu dieser Zeit zweitklassige Messinfrastruktur zu verbessern. Die Infrastruktur stellte eine große Herausforderung für die industrielle Wettbewerbsfähigkeit der USA dar, da sie hinter anderen Wirtschaftsmächten wie Großbritannien und Deutschland zurückgeblieben war.

Die USA sind auf das zuverlässige Funktionieren kritischer Infrastrukturen angewiesen. Cybersicherheitsbedrohungen nutzen die zunehmende Komplexität und Vernetzung kritischer Infrastruktursysteme aus. Sie gefährden die Sicherheit, Wirtschaft und öffentliche Sicherheit und Gesundheit der USA. Ähnlich wie Finanz- und Reputationsrisiken wirken sich Cybersicherheitsrisiken auf das Geschäftsergebnis eines Unternehmens aus. Sie können die Kosten in die Höhe treiben und den Umsatz beeinträchtigen. Sie können die Fähigkeit eines Unternehmens beeinträchtigen, innovativ zu sein und Kunden zu gewinnen und zu halten. Letztlich kann Cybersicherheit das allgemeine Risikomanagement eines Unternehmens verbessern.

Das NIST Cybersecurity Framework (CSF) wird von Regierungen und Branchen weltweit als empfohlene Grundlage für die Nutzung durch alle Organisationen unabhängig von Branche oder Größe unterstützt. Das NIST Cybersecurity Framework besteht aus drei Hauptkomponenten: dem Framework-Kern, den Profilen und den Implementierungsstufen. Der Kern des Frameworks umfasst die gewünschten Cybersicherheitsaktivitäten und -ergebnisse, die in 23 Kategorien unterteilt sind und die gesamte Bandbreite der Cybersicherheitsziele eines Unternehmens abdecken. Die Profile enthalten die individuelle Ausrichtung eines Unternehmens in Bezug auf ihre organisatorischen Anforderungen und Ziele, ihre Risikobereitschaft und ihre Ressourcen unter Verwendung der gewünschten Ergebnisse des Framework-Kerns. Die Implementierungsstufen beschreiben, inwieweit die Praktiken eines Unternehmens im Bereich des Cybersicherheitsrisikomanagements die im Kern des Frameworks definierten Merkmale aufweisen.

Verwendung dieses Frameworks

Sie können das NIST CSF v1.1 verwenden, um Sie bei der Vorbereitung auf Audits zu unterstützen. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und

Testverfahren. Diese Kontrollen sind gemäß den NIST CSF-Anforderungen in Kontrollsätze gruppiert. Audit Manager unterstützt derzeit die Kernkomponente des Frameworks. Audit Manager unterstützt das Profil und die Implementierungskomponenten in diesem Framework nicht.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im NIST CSF definiert sind. Wenn es Zeit für ein Audit ist, können Sie — oder ein Delegierter Ihrer Wahl — die von Audit Manager gesammelten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
NIST Cybersecurity Framework (CSF) v1.1	14	94	22

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings _NIST-CSF-v1.1.zip herunter.

Die von Audit Manager angebotenen Kontrollen dienen nicht dazu, zu überprüfen, ob Ihre Systeme mit dem NIST CSF konform sind. Darüber hinaus können sie nicht garantieren, dass Sie ein NIST-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- National Institute of Standards and Technology (NIST)
- NIST Computer Security Resource Center
- AWS Compliance-Seite für NIST
- NIST Cybersecurity Framework — Anpassung an das NIST CSF in der Cloud AWS

NIST SP 800-171 Rev. 2

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations unterstützt.

> **Note**
>
> - Informationen zum Audit Manager Manager-Framework, das NIST SP 800-53 unterstützt, finden Sie unter. NIST SP 800-53 Rev. 5
> - Informationen zum Audit Manager Manager-Framework, das NIST CSF unterstützt, finden Sie unter. NIST Cybersecurity Framework v1.1

Themen

Was ist NIST SP 800-171?

NIST SP 800-171 konzentriert sich auf den Schutz der Vertraulichkeit kontrollierter, nicht klassifizierter Informationen (Controlled Unclassified Information, CUI) in nicht-föderalen Systemen und Organisationen. Es empfiehlt spezifische Sicherheitsanforderungen, um dieses Ziel zu erreichen. NIST 800-171 ist eine Veröffentlichung, in der die erforderlichen Sicherheitsstandards und -praktiken für nicht-föderale Organisationen beschrieben werden, die CUI in ihren Netzwerken verwenden. Sie wurde erstmals im Juni 2015 vom National Institute of Standards and Technology (NIST) veröffentlicht. NIST ist eine US-Regierungsbehörde, die mehrere Standards und Publikationen veröffentlicht hat, um die Widerstandsfähigkeit der Cybersicherheit im öffentlichen und privaten Sektor zu stärken. NIST SP 800-171 wurde regelmäßig aktualisiert, um neuen Cyberbedrohungen und sich ändernden Technologien gerecht zu werden. Die neueste Version (2. Überarb.) wurde im Februar 2020 veröffentlicht.

Die Cybersicherheitskontrollen innerhalb von NIST SP 800-171 schützen CUI in den IT-Netzwerken von staatlichen Auftragnehmern und Subunternehmern. Sie definiert die Praktiken und Verfahren, an die sich staatliche Auftragnehmer halten müssen, wenn ihre Netzwerke CUI verarbeiten oder speichern. NIST SP 800-171 gilt nur für die Teile des Netzwerks eines Auftragnehmers, in denen CUI vorhanden ist.

Verwendung dieses Frameworks

Sie können das NIST SP 800-171-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den NIST-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der

Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im NIST SP 800-171-Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
NIST 800-171 Revision 2: Schutz kontrollierter, nicht klassifizierter Informationen in nichtföderalen Systemen und Organizations	35	75	14

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren. Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die ConfigDataSourceMappingsDatei AuditManager _ _NIST-800-171-Rev-2.zip herunter.

Die Steuerelemente in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme mit NIST 800-171 konform sind. Darüber hinaus können sie nicht garantieren, dass Sie ein NIST-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardsteuerelemente, finden Sie unter. Überprüfung eines Frameworks in AWS Audit Manager

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- National Institute of Standards and Technology (NIST)
- NIST Computer Security Resource Center
- AWS Compliance-Seite für NIST

PCI DSS v3.2.1

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das den Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 unterstützt.

> **Note**
>
> Informationen zu PCI DSS v4 und dem Audit Manager-Framework, das ihn unterstützt, finden Sie unter PCI DSS V4.0.

Themen

Was ist PCI DSS?

PCI DSS ist ein proprietärer Informationssicherheitsstandard. Er wird vom PCI Security Standards Council verwaltet, der von American Express, Discover Financial Services, JCB International, MasterCard Worldwide und Visa Inc gegründet wurde. PCI DSS gilt für Unternehmen, die Karteninhaberdaten (CHD) oder sensible Authentifizierungsdaten (SAD) speichern, verarbeiten oder übertragen. Dazu gehören unter anderem Händler, Auftragsverarbeiter, Käufer, Emittenten und Dienstleister. PCI DSS untersteht dem Mandat der Kartenmarken und wird vom Payment Card Industry Security Standards Council verwaltet.

AWS ist als PCI DSS Level 1 Service Provider zertifiziert, was die höchste verfügbare Bewertungsstufe darstellt. Die Compliance-Bewertung wurde von Coalfire Systems Inc., einem unabhängigen qualifizierten Sicherheitsgutachter (Qualified Security Assessor, QSA), durchgeführt. Die PCI-DSS-Konformitätsbescheinigung (AOC) und die Zusammenfassung der Verantwortlichkeiten stehen Ihnen unter zur Verfügung. AWS Artifact Dies ist ein Self-Service-Portal für den On-Demand-Zugriff auf Compliance-Berichte. AWS Melden Sie sich AWS Artifact in der AWS Management Console an oder erfahren Sie mehr unter Erste Schritte mit AWS Artifact.

Sie können den PCI DSS-Standard aus der PCI Security Standards Council Document Library herunterladen.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework PCI DSS v3.2.1 verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den PCI-DSS-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im PCI DSS v3.2.1 Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können

Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Datensicherheitsstandard der Zahlungskartenindustrie (PCI DSS) v3.2.1	38	246	15

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings _PCI-DSS-v3.2.1.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme dem PCI-DSS-Standard entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein PCI-DSS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- PCI Security Standards Council
- Dokumentenbibliothek des PCI Security Standards Council.
- AWS Compliance-Seite für PCI DSS

PCI DSS V4.0

AWS Audit Manager bietet ein vorgefertigtes Framework, das den Payment Card Industry Data Security Standard (PCI DSS) v4.0 unterstützt.

> **Note**
>
> Informationen zu PCI DSS v3.2.1 und dem Audit Manager-Framework, das ihn unterstützt, finden Sie unter PCI DSS v3.2.1.

Themen

Was ist PCI DSS?

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein globaler Standard, der grundlegende technische und betriebliche Anforderungen für den Schutz von Zahlungsdaten bietet. PCI DSS v4.0 ist die nächste Entwicklung des Standards.

PCI DSS wurde entwickelt, um die Datensicherheit von Zahlungskartenkonten zu fördern und zu verbessern. Es erleichtert auch die großflächige Einführung einheitlicher Datensicherheitsmaßnahmen weltweit. Es definiert grundlegende technische und betriebliche Anforderungen zum Schutz von Kontodaten. Obwohl es speziell für Umgebungen mit Zahlungskartenkontodaten konzipiert wurde, können Sie PCI DSS auch verwenden, um sich vor Bedrohungen zu schützen und andere Elemente im Zahlungsökosystem zu sichern.

Der PCI Security Standards Council (PCI SSC) hat zwischen PCI DSS v3.2.1 und v4.0 viele Änderungen eingeführt. Diese Updates sind in drei Kategorien unterteilt:

1. Neue Anforderungen – Änderungen, um sicherzustellen, dass der Standard mit neuen Bedrohungen und Technologien sowie mit Veränderungen in der Zahlungsbranche Schritt hält. Beispiele hierfür sind neue oder geänderte Anforderungen oder Testverfahren oder die Abschaffung einer Anforderung.
2. Klarstellung oder Anleitung – Aktualisierungen des Wortlauts, der Erläuterung, der Definition, zusätzliche Leitlinien oder Anweisungen, um das Verständnis zu verbessern oder weitere Informationen oder Anleitungen zu einem bestimmten Thema bereitzustellen.
3. Struktur oder Format – Neuorganisation von Inhalten, einschließlich der Kombination, Trennung und Neunummerierung von Anforderungen zur Abstimmung der Inhalte.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

> **Note**
>
> Dieses Standard-Framework verwendet konsolidierte Kontrollen von Security Hub CSPM als Datenquelle. Um erfolgreich Beweise aus konsolidierten Kontrollen zu sammeln, stellen Sie sicher, dass Sie die Einstellung für konsolidierte Kontrollergebnisse in Security Hub CSPM aktiviert haben. Weitere Informationen zur Verwendung von Security Hub als Datenquellentyp finden Sie unter AWS Security Hub CSPM -Kontrollen, die unterstützt werden von AWS Audit Manager.

Sie können das Framework PCI DSS V4.0 verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den PCI-DSS-V4.0-Anforderungen in Kontrollsätze

gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im Framework PCI DSS V4.0 definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Datensicherheitsstandard der Zahlungskartenindustrie (PCI DSS) v4.0	40	240	15

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings _PCI-DSS-v4.0.zip herunter.

Die Kontrollen in diesem AWS Audit Manager Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme dem PCI-DSS-Standard entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein PCI-DSS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- PCI DSS v4.0 Resource Hub
- PCI Security Standards Council
- Dokumentenbibliothek des PCI Security Standards Council.
- AWS Compliance-Seite für PCI DSS
- Leitfaden zur Einhaltung des Datenschutzstandards der Zahlungskartenindustrie (PCI DSS) v4.0 AWS

SSAE-18 SOC 2

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das das Statement on Standards for Attestations Engagement (SSAE) Nr. 18, Service Organizations Controls (SOC) Report 2, unterstützt.

Themen

- Weitere Ressourcen

Was ist SOC 2?

SOC 2, definiert vom American Institute of Certified Public Accountants (AICPA), ist der Name einer Reihe von Berichten, die im Rahmen eines Audits erstellt werden. Es ist für Dienstleistungsunternehmen (Organisationen, die Informationssysteme als Service für andere Organisationen bereitstellen) vorgesehen, um validierte Berichte über interne Kontrollen dieser Informationssysteme an die Nutzer dieser Dienste herauszugeben. Die Berichte konzentrieren sich auf Kontrollen, die in fünf Kategorien unterteilt sind und als Trust Service Principles bezeichnet werden.

AWS SOC-Berichte sind unabhängige Prüfungsberichte von Drittanbietern, aus denen hervorgeht, wie wichtige Compliance-Kontrollen und -Ziele AWS erreicht werden. Der Zweck dieser Berichte besteht darin, Ihnen und Ihren Prüfern zu vermitteln, welche AWS Kontrollen zur Unterstützung der Betriebsabläufe und der Einhaltung von Vorschriften eingeführt wurden. Es gibt fünf AWS SOC-Berichte:

- AWS SOC 1-Bericht, erhältlich für AWS Kunden von. AWS Artifact
- AWS SOC 2-Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit, erhältlich für AWS Kunden von. AWS Artifact
- AWS Der SOC 2-Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit ist für AWS Kunden erhältlich von AWS Artifact(der Geltungsbereich umfasst nur Amazon DocumentDB).
- AWS SOC 2 Privacy Type I Report, erhältlich für Kunden von AWS . AWS Artifact
- AWS SOC 3-Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit, öffentlich als Whitepaper verfügbar.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können dieses Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den SOC 2-Anforderungen in Kontrollsätze gruppiert. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Wenn Sie das Framework als Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für Ihr Audit relevant sind. Nachdem Sie eine Bewertung erstellt haben, beginnt Audit Manager mit der Bewertung Ihrer AWS Ressourcen. Dies geschieht auf der Grundlage der Kontrollen, die im Framework definiert sind. Wenn es Zeit für ein Audit ist, können Sie – oder ein Delegierter Ihrer Wahl – die von Audit Manager erfassten Nachweise überprüfen. Sie können entweder diese Nachweisordner durchsuchen und auswählen, welche Nachweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Oder, wenn Sie die Nachweissuche aktiviert haben, können Sie nach bestimmten Nachweisen suchen und diese im CSV-Format exportieren oder aus Ihren Suchergebnissen einen Bewertungsbericht erstellen. Anhand dieses Bewertungsberichts können Sie in jedem Fall nachweisen, dass Ihre Kontrollen wie vorgesehen funktionieren.

Die Details zum Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze
Erklärung zu Standards for Attestations Engagement (SSAE) Nr. 18, Service Organizations Controls (SOC) Report 2	15	46	20

Important

Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt AWS Security Hub CSPM, stellen Sie sicher, dass Sie alle Standards in Security Hub CSPM aktiviert haben.
Um sicherzustellen, dass dieses Framework die beabsichtigten Beweise sammelt, stellen Sie sicher AWS Config, dass Sie die erforderlichen AWS Config Regeln aktivieren.
Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings _SSAE-No.-18-SOC-Report-2.zip herunter.

Die Kontrollen in diesem Framework dienen nicht dazu, zu überprüfen, ob Ihre Systeme konform sind. AWS Audit Manager Darüber hinaus können sie nicht garantieren, dass Sie ein Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweiserhebung erfordern.

Nächste Schritte

Anweisungen zum Anzeigen detaillierter Informationen zu diesem Framework, einschließlich der Liste der darin enthaltenen Standardkontrollen, finden Sie unterÜberprüfung eines Frameworks in AWS Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Anpassung dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unterErstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager.

Weitere Ressourcen

- AWS Compliance-Seite für SOC

Unterstützte Datenquellentypen für automatisierte Beweise

Wenn Sie ein benutzerdefiniertes Steuerelement in erstellen AWS Audit Manager, können Sie Ihr Steuerelement so einrichten, dass automatisierte Beweise aus den folgenden Datenquellentypen gesammelt werden:

- AWS CloudTrail
- AWS Security Hub CSPM
- AWS Config
- AWS API-Aufrufe

Jeder Datenquellentyp bietet unterschiedliche Funktionen zur Erfassung von Benutzeraktivitätsprotokollen, Compliance-Ergebnissen, Ressourcenkonfigurationen und mehr.

In diesem Kapitel erfahren Sie mehr über jeden dieser automatisierten Datenquellentypen sowie über die spezifischen AWS Security Hub CSPM Steuerelemente, AWS Config Regeln und AWS API-Aufrufe, die von Audit Manager unterstützt werden.

Wichtige Punkte

Die folgende Tabelle bietet eine Übersicht über jeden automatisierten Datenquellentyp.

Datenquellentyp	Description	Häufigkeit der Beweissuche	Um diesen Datenquellentyp zu verwenden ...	Wenn diese Kontrolle in einer Bewertung aktiv ist ...	Verwandte Tipps zur Fehlerbehebung
AWS CloudTrail	Verfolgt eine bestimmte Benutzeraktivität.	Fortlaufend.	Wählen Sie aus der Liste der unterstützten Ereignisnamen aus.	Audit Manager filtert Ihre CloudTrail Protokolle anhand des von Ihnen ausgewählten Schlüsselworts. Die Ergebnisse	In meiner Bewertung werden von AWS CloudTrai

Datenquellentyp	Description	Häufigkeit der Beweissuche	Um diesen Datenquellentyp zu verwenden ...	Wenn diese Kontrolle in einer Bewertung aktiv ist ...	Verwandte Tipps zur Fehlerbehebung
				werden als Beweis für Benutzeraktivitäten importiert.	keine Beweise für Benutzeraktivitäten gesammelt
AWS Config	Erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem die Ergebnisse von AWS Config gemeldet werden.	Basierend auf den in der AWS Config Regel definierten Auslösern.	Wählen Sie einen Regeltyp und danach eine Regel aus. • Wählen Sie für verwaltete Regeln Schlüsselwörter aus der Liste der unterstützten verwalteten Regeln aus. • Wählen Sie für benutzerdefinierte Regeln aus der Liste Ihrer verfügbaren Regeln aus.	Audit Manager erhält die Ergebnisse für diese Regel direkt von AWS Config. Das Ergebnis wird als Beweis für die Konformitätsprüfung importiert.	Bei meiner Bewertung werden keine Nachweise zur Konformitätsprüfung gesammelt von AWS Config AWS Config Probleme bei der Integration

Datenquellentyp	Description	Häufigkeit der Beweissuche	Um diesen Datenquellentyp zu verwenden ...	Wenn diese Kontrolle in einer Bewertung aktiv ist ...	Verwandte Tipps zur Fehlerbehebung
AWS Security Hub CSPM	Erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem Ergebnisse aus Security Hub CSPM gemeldet werden.	Basierend auf dem Zeitplan der Security Hub CSPM-Überprüfung.	Wählen Sie aus der Liste der unterstützten Security Hub CSPM-Steuerung aus. IDs	Audit Manager erhält das Ergebnis der Sicherheitsprüfung direkt vom Security Hub CSPM. Das Ergebnis wird als Beweis für die Konformitätsprüfung importiert.	Meine Bewertung bezieht sich nicht auf die Erfassung von Nachweisen zur Konformitätsprüfung von AWS Security Hub CSPM

Datenquellentyp	Description	Häufigkeit der Beweissuche	Um diesen Datenquellentyp zu verwenden ...	Wenn diese Kontrolle in einer Bewertung aktiv ist ...	Verwandte Tipps zur Fehlerbehebung
AWS API-Aufrufe	Erstellt einen Snapshot Ihrer Ressourcenkonfiguration direkt über einen API-Aufruf an die angegebene Ressource AWS-Service.	Täglich, wöchentlich oder monatlich.	Wählen Sie aus der Liste der unterstützten API-Aufrufe aus und wählen Sie dann Ihre bevorzugte Häufigkeit aus.	Audit Manager führt den API-Aufruf auf der Grundlage der von Ihnen angegebenen Häufigkeit durch. Die Antwort wird als Beweis für Konfigurationsdaten importiert.	In meiner Bewertung werden keine Beweise für Konfigurationsdaten für einen AWS API-Aufruf gesammelt

Tip

Sie können benutzerdefinierte Steuerelemente erstellen, die anhand vordefinierter Gruppierungen der oben genannten Datenquellen Beweise sammeln. Diese Datenquellengruppierungen werden als AWS verwaltete Quellen bezeichnet. Jede AWS verwaltete Quelle steht für ein gemeinsames Steuerelement oder ein zentrales Steuerelement, das einer gemeinsamen Compliance-Anforderung entspricht. Auf diese Weise können Sie Ihre Compliance-Anforderungen effizient einer relevanten Gruppe von AWS Datenquellen zuordnen. Informationen zu den verfügbaren allgemeinen Steuerelementen finden Sie unterFinden Sie die verfügbaren Steuerelemente in AWS Audit Manager. Alternativ können Sie die vier oben genannten Datenquellentypen verwenden, um Ihre eigenen benutzerdefinierten Datenquellen zu definieren. Auf diese Weise haben Sie die

Flexibilität, manuelle Nachweise hochzuladen oder automatisierte Nachweise aus einer unternehmensspezifischen Ressource, z. B. einer benutzerdefinierten AWS Config Regel, zu sammeln.

Nächste Schritte

Weitere Informationen zu den spezifischen Datenquellen, die Sie in Ihren benutzerdefinierten Steuerelementen verwenden können, finden Sie auf den folgenden Seiten.

- AWS-Config-Regeln unterstützt von AWS Audit Manager
- AWS Security Hub CSPM Steuerelemente, die unterstützt werden von AWS Audit Manager
- AWS API-Aufrufe werden unterstützt von AWS Audit Manager
- AWS CloudTrail Eventnamen werden unterstützt von AWS Audit Manager

AWS-Config-Regeln unterstützt von AWS Audit Manager

Sie können Audit Manager verwenden, um AWS Config Bewertungen als Nachweis für Audits zu erfassen. Wenn Sie ein benutzerdefiniertes Steuerelement erstellen oder bearbeiten, können Sie eine oder mehrere AWS Config Regeln als Datenquellenzuordnung für die Erfassung von Nachweisen angeben. AWS Config führt Konformitätsprüfungen auf der Grundlage dieser Regeln durch, und Audit Manager meldet die Ergebnisse als Nachweis der Konformitätsprüfung.

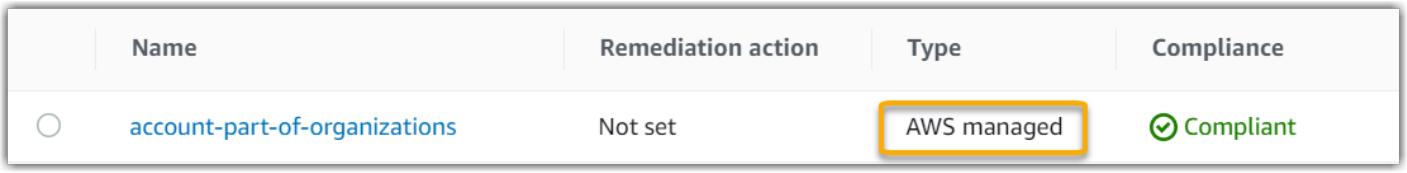
Neben verwalteten Regeln können Sie Ihre benutzerdefinierten Regeln auch einer Kontrolldatenquelle zuordnen.

Inhalt

Wichtige Punkte

- Audit Manager sammelt keine Beweise aus serviceverknüpften AWS Config Regeln, mit Ausnahme von serviceverknüpften Regeln aus Conformance Packs und aus AWS Organizations.
- Audit Manager verwaltet AWS Config Regeln nicht für Sie. Bevor Sie mit der Beweiserhebung beginnen, empfehlen wir Ihnen, Ihre aktuellen AWS Config Regelparameter zu überprüfen. Validieren Sie diese Parameter anschließend anhand der Anforderungen des von Ihnen ausgewählten Frameworks. Bei Bedarf können Sie die Parameter einer Regel in AWS Config aktualisieren, sodass sie den Framework-Anforderungen entsprechen. So können Sie sicherstellen, dass bei Ihren Bewertungen die richtigen Beweise für die Konformitätsprüfung für ein Framework gesammelt werden.

  Nehmen wir beispielsweise an, Sie erstellen eine Bewertung für CIS v1.2.0. Dieses Framework verfügt über ein Steuerelement mit dem Namen „Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert“. In hat die iam-password-policyRegel einen `MinimumPasswordLength` Parameter AWS Config, der die Passwortlänge überprüft. Der Standardwert für diesen Parameter ist 14 Zeichen. Dadurch stimmt die Regel mit den Kontrollanforderungen überein. Wenn Sie nicht den Standardparameterwert verwenden, stellen Sie sicher, dass der von Ihnen verwendete Wert den Anforderungen durch CIS v1.2.0 von 14 Zeichen entspricht oder diese überschreitet. Die Standard-Parameterdetails für jede verwaltete Regel finden Sie in der AWS Config -Dokumentation.
- Wenn Sie überprüfen möchten, ob es sich bei einer AWS Config Regel um eine verwaltete oder eine benutzerdefinierte Regel handelt, können Sie dies über die AWS Config Konsole tun. Wählen Sie im linken Navigationsmenü Regeln aus und suchen Sie in der Tabelle nach der Regel. Wenn es sich um eine verwaltete Regel handelt, wird in der Spalte Typ der Eintrag AWS Verwaltet angezeigt.



Unterstützte AWS Config verwaltete Regeln

Die folgenden AWS Config verwalteten Regeln werden von Audit Manager unterstützt. Wenn Sie eine Datenquelle für eine benutzerdefinierte Kontrolle einrichten, können Sie jedes der folgenden Kennwörter für verwaltete Regeln verwenden. Weitere Informationen zu den unten aufgeführten

verwalteten Regeln finden Sie, indem Sie ein Element aus der Liste auswählen oder im AWS Config -Benutzerhandbuch unter AWS Config -verwaltete Regeln nachlesen.

> **Tip**
>
> Wenn Sie bei der Erstellung einer benutzerdefinierten Kontrolle in der Audit-Manager-Konsole eine verwaltete Regel auswählen, achten Sie darauf, dass Sie nach einem der folgenden Schlüsselwörter für die Regel-ID suchen und nicht nach dem Regelnamen. Informationen zum Unterschied zwischen dem Regelnamen und der Regel-ID und wie Sie die Kennung für eine verwaltete Regel finden, erhalten Sie im Abschnitt Fehlerbehebung in diesem Benutzerhandbuch.

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_AKTIVIERT
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_AKTIVIERT_UND_VERSCHLÜSSELT
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_AKTIVIERT
- API_GW_XRAY_AKTIVIERT
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_ IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_ _MINIMUM_HEALTHY_HOSTS_KONFIGURIERT EC2
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_VERSCHLÜSSELUNG_STANDARDMÄSSIG
- EC2_ _PRÜFEN IMDSV2
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANZ_VERWALTET_VON_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ANGEHÄNGT

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_AUF DER SCHWARZEN LISTE
- EC2_MANAGEDINSTANCE_APPLICATIONS_ERFORDERLICH
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_AUF DER SCHWARZEN LISTE
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_KEINE_AMAZON-SCHLÜSSELPAAR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESSOURCEN_GESCHÜTZT_DURCH_BACKUP_PLAN
- EC2_SICHERHEITSGRUPPE_AN_ENI BEIGEFÜGT
- EC2_SICHERHEITSGRUPPE_AN_ENI_PERIODISCH BEIGEFÜGT
- EC2_GESTOPPT_INSTANZ
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _AKTIVIERT AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USERIDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_ERFORDERLICH
- ELBV2_MEHRERE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_PARCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPTY
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_AKTIVIERT
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Verwenden AWS Config benutzerdefinierter Regeln mit Audit Manager

Sie können AWS Config benutzerdefinierte Regeln als Datenquelle für Auditberichte verwenden. Wenn ein Steuerelement über eine Datenquelle verfügt, die einer AWS Config Regel zugeordnet ist, fügt Audit Manager die Auswertung hinzu, die durch die AWS Config Regel erstellt wurde.

Die benutzerdefinierten Regeln, die Sie verwenden können, hängen davon ab AWS-Konto , mit welcher Sie sich bei Audit Manager anmelden. Wenn Sie in auf eine benutzerdefinierte Regel zugreifen können AWS Config, können Sie sie als Datenquellenzuordnung in Audit Manager verwenden.

- Für Einzelpersonen AWS-Konten — Sie können jede der benutzerdefinierten Regeln verwenden, die Sie mit Ihrem Konto erstellt haben.

- Für Konten, die Teil einer Organisation sind – Sie können entweder jede Ihrer benutzerdefinierten Regeln auf Mitgliedsebene verwenden, oder Sie können jede der benutzerdefinierten Regeln auf Organisationsebene verwenden, die Ihnen in zur Verfügung stehen. AWS Config

Nachdem Sie Ihre benutzerdefinierten Regeln als Datenquelle für ein Steuerelement zugeordnet haben, können Sie dieses Steuerelement einem benutzerdefinierten Framework in Audit Manager hinzufügen.

Weitere Ressourcen

- Hilfe zu Problemen mit diesem Datenquellentyp finden Sie unter Bei meiner Bewertung werden keine Nachweise zur Konformitätsprüfung gesammelt von AWS Config AWS Config Integrationsprobleme.
- Informationen zum Erstellen eines benutzerdefinierten Steuerelements mit diesem Datenquellentyp finden Sie unterErstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager.
- Informationen zum Erstellen eines benutzerdefinierten Frameworks, das Ihr benutzerdefiniertes Steuerelement verwendet, finden Sie unterErstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager.
- Informationen zum Hinzufügen Ihres benutzerdefinierten Steuerelements zu einem vorhandenen benutzerdefinierten Framework finden Sie unterBearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager.
- Informationen zum Erstellen einer benutzerdefinierten Regel finden Sie unter Entwickeln einer benutzerdefinierten Regel für AWS Config im AWS Config Entwicklerhandbuch. AWS Config

AWS Security Hub CSPM Steuerelemente, die unterstützt werden von AWS Audit Manager

Sie können Audit Manager verwenden, um die Ergebnisse des Security Hub CSPM als Nachweis für Audits zu erfassen. Wenn Sie ein benutzerdefiniertes Steuerelement erstellen oder bearbeiten, können Sie ein oder mehrere Security Hub CSPM-Steuerelemente als Datenquellenzuordnung für die Beweiserhebung angeben. Security Hub CSPM führt auf der Grundlage dieser Kontrollen Konformitätsprüfungen durch, und Audit Manager meldet die Ergebnisse als Nachweis der Konformitätsprüfung.

Inhalt

Wichtige Punkte

- Audit Manager sammelt keine Beweise aus serviceverknüpften AWS Config Regeln, die von Security Hub CSPM erstellt wurden.
- Am 9. November 2022 führte Security Hub CSPM automatisierte Sicherheitsprüfungen ein, die den Anforderungen des Center for Internet Security (CIS) AWS Foundations Benchmark Version 1.4.0, Level 1 und 2 (CIS v1.4.0) entsprechen. In Security Hub CSPM wird der CIS v1.4.0-Standard zusätzlich zum CIS v1.2.0-Standard unterstützt.
- Wir empfehlen, dass Sie die Einstellung für konsolidierte Kontrollergebnisse in Security Hub CSPM aktivieren, sofern sie nicht bereits aktiviert ist. Wenn Sie Security Hub CSPM am oder nach dem 23. Februar 2023 aktivieren, ist diese Einstellung standardmäßig aktiviert.

  Wenn die Option „Konsolidierte Ergebnisse“ aktiviert ist, generiert Security Hub CSPM für jede Sicherheitsüberprüfung ein einziges Ergebnis (auch wenn dieselbe Prüfung für mehrere Standards gilt). Jeder Security Hub CSPM-Befund wird als eine einzige Ressourcenbewertung in Audit Manager gesammelt. Infolgedessen führen konsolidierte Ergebnisse zu einem Rückgang der Gesamtzahl der individuellen Ressourcenbewertungen, die Audit Manager für die Ergebnisse des Security Hub CSPM durchführt. Aus diesem Grund kann die Verwendung konsolidierter Ergebnisse häufig zu einer Senkung der Nutzungskosten Ihres Audit Manager führen, ohne dass die Qualität und Verfügbarkeit der Beweise beeinträchtigt wird. Weitere Informationen über die Preise finden Sie unter AWS Audit Manager – Preise.

Beispiele für Belege, wenn konsolidierte Ergebnisse aktiviert oder deaktiviert werden

Die folgenden Beispiele zeigen einen Vergleich, wie Audit Manager je nach Ihren Security Hub CSPM-Einstellungen Beweise sammelt und präsentiert.

When consolidated findings is turned on

> Nehmen wir an, Sie haben die folgenden drei Sicherheitsstandards in Security Hub CSPM aktiviert: AWS FSBP, PCI DSS und CIS Benchmark v1.2.0.

- Alle drei Standards verwenden dieselbe Steuerung (IAM.4) mit derselben zugrunde liegenden Regel (-check). AWS Config iam-root-access-key
- Da die Einstellung für konsolidierte Ergebnisse aktiviert ist, generiert Security Hub CSPM ein einziges Ergebnis für diese Kontrolle.
- Security Hub CSPM sendet das konsolidierte Ergebnis für diese Kontrolle an Audit Manager.
- Das konsolidierte Ergebnis gilt als eine einzige Ressourcenbewertung in Audit Manager. Infolgedessen wird Ihrer Bewertung ein einziger Beweis hinzugefügt.

Hier sehen Sie ein Beispiel dafür, wie diese Beweise aussehen könnten:


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
```

```
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
```

```
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```

When consolidated findings is turned off

Nehmen wir an, Sie haben die folgenden drei Sicherheitsstandards in Security Hub CSPM aktiviert: AWS FSBP, PCI DSS und CIS Benchmark v1.2.0.

- Alle drei Standards verwenden dieselbe Steuerung (IAM.4) mit derselben zugrunde liegenden Regel (-check). AWS Config iam-root-access-key
- Da die Einstellung für konsolidierte Ergebnisse deaktiviert ist, generiert Security Hub CSPM für jeden aktivierten Standard ein separates Ergebnis pro Sicherheitsprüfung (in diesem Fall drei Ergebnisse).
- Security Hub CSPM sendet für diese Kontrolle drei separate standardspezifische Ergebnisse an Audit Manager.
- Die drei Ergebnisse gelten als drei einzigartige Ressourcenbewertungen in Audit Manager. Als Ergebnis werden Ihrer Bewertung drei separate Beweise hinzugefügt.

Hier sehen Sie ein Beispiel dafür, wie diese Beweise aussehen könnten: Beachten Sie, dass in diesem Beispiel jede der folgenden drei Payloads dieselbe Sicherheitskontroll-ID (*SecurityControlId":"IAM.4"*) hat. Aus diesem Grund erhält die Bewertungskontrolle, die diese Nachweise in Audit Manager (IAM.4) sammelt, drei separate Nachweise, wenn die folgenden Ergebnisse von Security Hub CSPM eingehen.

Beweise für IAM.4 (FSBP)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
```

```
    "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
           "LastObservedAt":"2023-11-01T14:12:04.106Z",
           "CreatedAt":"2020-10-05T19:18:47.848Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"IAM.4 IAM root user access key should not exist",
           "Description":"This AWS control checks whether the root user access key
 is available.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                 "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
              }
           },
           "ProductFields":{
```

```
            "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
            "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
            "ControlId":"IAM.4",
            "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
            "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
            "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
            "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
            "aws/securityhub/ProductName":"Security Hub",
            "aws/securityhub/CompanyName":"AWS",
            "Resources:0/Id":"arn:aws:iam::111122223333:root",
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
         },
         "Resources":[
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
         ],
         "Compliance":{
            "Status":"PASSED",
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
```

```
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
              ]
           },
           "ProcessedAt":"2023-11-01T14:12:07.395Z"
        }
     ]
  }
}
```

Beweise für IAM.4 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
```

```
            "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.775Z",
            "LastObservedAt":"2023-11-01T14:12:07.989Z",
            "CreatedAt":"2020-10-05T19:18:47.775Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"1.12 Ensure no root user access key exists",
            "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
```

```
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
           "FindingProviderFields":{
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
              ]
           },
           "ProcessedAt":"2023-11-01T14:12:13.436Z"
        }
     ]
  }
}
```

Beweise für PCI.IAM.1 (PCI DSS)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.788Z",
           "LastObservedAt":"2023-11-01T14:12:02.413Z",
           "CreatedAt":"2020-10-05T19:18:47.788Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"PCI.IAM.1 IAM root user access key should not exist",
           "Description":"This AWS control checks whether the root user access key
 is available.",
```

```
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "RelatedRequirements":[
                  "PCI DSS 2.1",
                  "PCI DSS 2.2",
                  "PCI DSS 7.2.1"
               ],
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
```

```
                {
                   "StandardsId":"standards/pci-dss/v/3.2.1"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
          },
          "RecordState":"ACTIVE",
          "FindingProviderFields":{
             "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:05.950Z"
       }
    ]
  }
}
```

Unterstützte Security Hub CSPM-Steuerelemente

Die folgenden Security Hub CSPM-Steuerelemente werden derzeit von Audit Manager unterstützt. Sie können jedes der folgenden standardspezifischen Kontroll-ID-Schlüsselwörter verwenden, wenn Sie eine Datenquelle für eine benutzerdefinierte Kontrolle einrichten.

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1,6	IAM.12
CIS v1.2.0	1,7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1,22	IAM.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
CIS v1.2.0	2.1	CloudTrail1.
CIS v1.2.0	2.2	CloudTrail.4
CIS v1.2.0	2.3	CloudTrail.6
CIS v1.2.0	2.4	CloudTrail.5
CIS v1.2.0	2.5	Config.1
CIS v1.2.0	2.6	CloudTrail.7
CIS v1.2.0	2.7	CloudTrail.2
CIS v1.2.0	2,8	KMS.4
CIS v1.2.0	2,9	EC2.6
CIS v1.2.0	3.1	CloudWatch.2
CIS v1.2.0	3.2	CloudWatch.3
CIS v1.2.0	3.3	CloudWatch1.
CIS v1.2.0	3.4	CloudWatch.4
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6
CIS v1.2.0	3.7	CloudWatch.7

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
CIS v1.2.0	3.8	CloudWatch.8
CIS v1.2.0	3.9	CloudWatch.9
CIS v1.2.0	3,10	CloudWatch.10
CIS v1.2.0	3,11	CloudWatch.11
CIS v1.2.0	3,12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3,14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4,2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI. AutoScaling1.	AutoScaling1.
PCI DSS	PCI. CloudTrail1.	CloudTrail1.
PCI DSS	PCI. CloudTrail2.	CloudTrail.2
PCI DSS	PCI. CloudTrail3.	CloudTrail.3

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
PCI DSS	PCI. CloudTrail4.	CloudTrail.4
PCI DSS	PCI. CodeBuild1.	CodeBuild1.
PCI DSS	PCI. CodeBuild2.	CodeBuild.2
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch1.
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI. EC21.	EC21.
PCI DSS	PCI. EC22.	EC2.2
PCI DSS	PCI. EC23.	EC2.3
PCI DSS	PCI. EC24.	EC2.12
PCI DSS	PCI. EC25.	EC2.13
PCI DSS	PCI. EC26.	EC2.6
PCI DSS	PCI. ELBv21.	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
PCI DSS	PCI. GuardDuty 1.	GuardDuty1.
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI. IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.OpenSearch.1	OpenSearch.1
PCI DSS	PCI.OpenSearch.2	OpenSearch.2
PCI DSS	PCI.RDS.1	RDS.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.RedShift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI. SageMaker 1.	SageMaker1.
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Bewährte grundlegende Sicherheitsmethoden	Account.1	Account.1
AWS Bewährte grundlegende Sicherheitsmethoden	Konto.2	Konto.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	ACM.1	ACM.1
AWS Bewährte grundlegende Sicherheitsmethoden	ACM.2	ACM.2
AWS Bewährte grundlegende Sicherheitsmethoden	APIGateway1.	APIGateway1.
AWS Bewährte grundlegende Sicherheitsmethoden	APIGateway2.	APIGateway2.2
AWS Bewährte grundlegende Sicherheitsmethoden	APIGateway3.	APIGateway3.
AWS Bewährte grundlegende Sicherheitsmethoden	APIGateway4.	APIGateway4.
AWS Bewährte grundlegende Sicherheitsmethoden	APIGateway5.	APIGateway5.
AWS Bewährte grundlegende Sicherheitsmethoden	APIGateway8.	APIGateway.8
AWS Bewährte grundlegende Sicherheitsmethoden	APIGateway9.	APIGateway.9
AWS Bewährte grundlegende Sicherheitsmethoden	AppSync2.	AppSync2.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	AppSync5.	AppSync5.
AWS Bewährte grundlegende Sicherheitsmethoden	Athena.1	Athena.1
AWS Bewährte grundlegende Sicherheitsmethoden	AutoScaling1.	AutoScaling1.
AWS Bewährte grundlegende Sicherheitsmethoden	AutoScaling2.	AutoScaling2.2
AWS Bewährte grundlegende Sicherheitsmethoden	AutoScaling3.	AutoScaling3.
AWS Bewährte grundlegende Sicherheitsmethoden	AutoScaling4.	AutoScaling4.
AWS Bewährte grundlegende Sicherheitsmethoden	AutoScaling.5	AutoScaling.5
AWS Bewährte grundlegende Sicherheitsmethoden	AutoScaling6.	AutoScaling.6
AWS Bewährte grundlegende Sicherheitsmethoden	AutoScaling9.	AutoScaling.9
AWS Bewährte grundlegende Sicherheitsmethoden	Sicherung.1	Sicherung.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFormation1.	CloudFormation1.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront1.	CloudFront1.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront2.	CloudFront2.2
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront3.	CloudFront3.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront4.	CloudFront4.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront5.	CloudFront5.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront6.	CloudFront.6
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront7.	CloudFront.7
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront8.	CloudFront.8
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront9.	CloudFront.9

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront1.0	CloudFront.10
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront1.2	CloudFront.12
AWS Bewährte grundlegende Sicherheitsmethoden	CloudFront1.3	CloudFront.13
AWS Bewährte grundlegende Sicherheitsmethoden	CloudTrail1.	CloudTrail1.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudTrail2.	CloudTrail2.2
AWS Bewährte grundlegende Sicherheitsmethoden	CloudTrail3.	CloudTrail3.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudTrail4.	CloudTrail4.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudTrail5.	CloudTrail5.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudTrail6.	CloudTrail.6
AWS Bewährte grundlegende Sicherheitsmethoden	CloudTrail7.	CloudTrail.7

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.	CloudWatch1.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch2.	CloudWatch2.2
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch3.	CloudWatch3.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch4.	CloudWatch4.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch5.	CloudWatch5.
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch6.	CloudWatch.6
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch7.	CloudWatch.7
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch8.	CloudWatch.8
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch9.	CloudWatch.9
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.0	CloudWatch.10

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.1	CloudWatch.11
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.2	CloudWatch.12
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.3	CloudWatch.13
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.4	CloudWatch.14
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.5	CloudWatch.15
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.6	CloudWatch.16
AWS Bewährte grundlegende Sicherheitsmethoden	CloudWatch1.7	CloudWatch.17
AWS Bewährte grundlegende Sicherheitsmethoden	CodeBuild1.	CodeBuild1.
AWS Bewährte grundlegende Sicherheitsmethoden	CodeBuild2.	CodeBuild2.2
AWS Bewährte grundlegende Sicherheitsmethoden	CodeBuild3.	CodeBuild3.

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	CodeBuild4.	CodeBuild4.
AWS Bewährte grundlegende Sicherheitsmethoden	CodeBuild5.	CodeBuild5.
AWS Bewährte grundlegende Sicherheitsmethoden	Config.1	Config.1
AWS Bewährte grundlegende Sicherheitsmethoden	DMS.1	DMS.1
AWS Bewährte grundlegende Sicherheitsmethoden	DMS.6	DMS.6
AWS Bewährte Methoden für grundlegende Sicherheit	DMS.7	DMS.7
AWS Bewährte Methoden für grundlegende Sicherheit	DMS.8	DMS.8
AWS Bewährte Methoden für grundlegende Sicherheit	DMS.9	DMS.9
AWS Bewährte Methoden für grundlegende Sicherheit	DocumentDB DB.1	DocumentDB DB.1
AWS Bewährte grundlegende Sicherheitsmethoden	DocumentDB DB.2	DocumentDB DB.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte Methoden zur grundlegenden Sicherheit	DocumentDB DB.3	DocumentDB DB.3
AWS Bewährte Methoden zur grundlegenden Sicherheit	DocumentDB DB.4	DocumentDB DB.4
AWS Bewährte grundlegende Sicherheitsmethoden	DocumentDB DB.5	DocumentDB DB.5
AWS Bewährte grundlegende Sicherheitsmethoden	DynamoDB.1	DynamoDB.1
AWS Bewährte grundlegende Sicherheitsmethoden	DynamoDB.2	DynamoDB.2
AWS Bewährte grundlegende Sicherheitsmethoden	DynamoDB.3	DynamoDB.3
AWS Bewährte grundlegende Sicherheitsmethoden	Dynamo DB.4	Dynamo DB.4
AWS Bewährte grundlegende Sicherheitsmethoden	Dynamo DB,6	Dynamo DB,6
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.	EC21.
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.	EC22.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	EC23.	EC23.
AWS Bewährte grundlegende Sicherheitsmethoden	EC24.	EC24.
AWS Bewährte grundlegende Sicherheitsmethoden	EC26.	EC2.6
AWS Bewährte grundlegende Sicherheitsmethoden	EC27.	EC2.7
AWS Bewährte grundlegende Sicherheitsmethoden	EC28.	EC2.8
AWS Bewährte grundlegende Sicherheitsmethoden	EC29.	EC2.9
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.0	EC2.10
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.2	EC2.12
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.3	EC2.13
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.4	EC2.14

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.5	EC2.15
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.6	EC2.16
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.7	EC2.17
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.8	EC2.18
AWS Bewährte grundlegende Sicherheitsmethoden	EC21.9	EC2.19
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.0	EC2.20
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.1	EC2.21
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.2	EC2.22
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.3	EC22,3
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.4	EC22,4

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.5	EC2.25
AWS Bewährte grundlegende Sicherheitsmethoden	EC22.8	EC2.28
AWS Bewährte grundlegende Sicherheitsmethoden	EC25.1	EC25,1
AWS Bewährte grundlegende Sicherheitsmethoden	ECR.1	ECR.1
AWS Bewährte grundlegende Sicherheitsmethoden	ECR.2	ECR.2
AWS Bewährte grundlegende Sicherheitsmethoden	ECR.3	ECR.3
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.1	ECS.1
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.2	ECS.2
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.3	ECS.3
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.4	ECS.4

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.5	ECS.5
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.8	ECS.8
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.9	ECS. 9
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.10	ECS.10
AWS Bewährte grundlegende Sicherheitsmethoden	ECS.12	ECS.12
AWS Bewährte grundlegende Sicherheitsmethoden	EFS.1	EFS.1
AWS Bewährte grundlegende Sicherheitsmethoden	EFS.2	EFS.2
AWS Bewährte grundlegende Sicherheitsmethoden	EFS.3	EFS.3
AWS Bewährte grundlegende Sicherheitsmethoden	EFS.4	EFS.4
AWS Bewährte grundlegende Sicherheitsmethoden	EKS.1	EKS.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	EKS.2	EKS.2
AWS Bewährte grundlegende Sicherheitsmethoden	EKS.8	EKS. 8
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache1.	ElastiCache1.
AWS Bewährte grundlegende Sicherheitsmethoden	ElastiCache2.	ElastiCache2.2
AWS Bewährte grundlegende Sicherheitsmethoden	ElastiCache3.	ElastiCache3.
AWS Bewährte grundlegende Sicherheitsmethoden	ElastiCache4.	ElastiCache4.
AWS Bewährte grundlegende Sicherheitsmethoden	ElastiCache5.	ElastiCache5.
AWS Bewährte grundlegende Sicherheitsmethoden	ElastiCache6.	ElastiCache.6
AWS Bewährte grundlegende Sicherheitsmethoden	ElastiCache7.	ElastiCache.7
AWS Bewährte grundlegende Sicherheitsmethoden	ElasticBeanstalk1.	ElasticBeanstalk1.

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	ElasticBeanstalk2.	ElasticBeanstalk2.2
AWS Bewährte grundlegende Sicherheitsmethoden	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.1	ELB.1
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.2	ELB.2
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.3	ELB.3
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.4	ELB.4
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.5	ELB.5
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.6	ELB.6
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.7	ELB.7
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.8	ELB.8

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.9	ELB.9
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.10	ELB.10
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.12	ELB.12
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.13	ELB.13
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.14	ELB.14
AWS Bewährte grundlegende Sicherheitsmethoden	ELB.16	ELB. 16
AWS Bewährte grundlegende Sicherheitsmethoden	ELBv21.	ELB.1
AWS Bewährte grundlegende Sicherheitsmethoden	EMR.1	EMR.1
AWS Bewährte grundlegende Sicherheitsmethoden	EMR. 2	EMR. 2
AWS Bewährte grundlegende Sicherheitsmethoden	ES.1	ES.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	ES.2	ES.2
AWS Bewährte grundlegende Sicherheitsmethoden	ES.3	ES.3
AWS Bewährte grundlegende Sicherheitsmethoden	ES.4	ES.4
AWS Bewährte grundlegende Sicherheitsmethoden	ES.5	ES.5
AWS Bewährte grundlegende Sicherheitsmethoden	ES.6	ES.6
AWS Bewährte grundlegende Sicherheitsmethoden	ES.7	ES.7
AWS Bewährte grundlegende Sicherheitsmethoden	ES.8	ES.8
AWS Bewährte grundlegende Sicherheitsmethoden	EventBridge3.	EventBridge3.
AWS Bewährte grundlegende Sicherheitsmethoden	EventBridge4.	EventBridge4.
AWS Bewährte grundlegende Sicherheitsmethoden	FSx1.	FSx1.

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	GuardDuty1.	GuardDuty1.
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.1	IAM.1
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.2	IAM.2
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.3	IAM.3
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.4	IAM.4
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.5	IAM.5
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.6	IAM.6
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.7	IAM.7
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.8	IAM.8
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.9	IAM.9

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	ICH BIN. 10	ICH BIN 10
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.11	IAM.11
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.12	IAM.12
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.13	IAM.13
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.14	IAM.14
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.15	IAM.15
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.16	IAM.16
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.17	IAM.17
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.18	IAM.18
AWS Bewährte grundlegende Sicherheitsmethoden	ICH BIN 19.	ICH BIN. 19

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.21	IAM.21
AWS Bewährte grundlegende Sicherheitsmethoden	IAM.22	IAM.22
AWS Bewährte grundlegende Sicherheitsmethoden	Kinesis.1	Kinesis.1
AWS Bewährte grundlegende Sicherheitsmethoden	KMS.1	KMS.1
AWS Bewährte grundlegende Sicherheitsmethoden	KMS.2	KMS.2
AWS Bewährte grundlegende Sicherheitsmethoden	KMS.3	KMS.3
AWS Bewährte grundlegende Sicherheitsmethoden	KMS.4	KMS.4
AWS Bewährte grundlegende Sicherheitsmethoden	Lambda.1	Lambda.1
AWS Bewährte grundlegende Sicherheitsmethoden	Lambda.2	Lambda.2
AWS Bewährte grundlegende Sicherheitsmethoden	Lambda.3	Lambda.3

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	Lambda.5	Lambda.5
AWS Bewährte grundlegende Sicherheitsmethoden	Macie.1	Macie.1
AWS Bewährte Methoden für grundlegende Sicherheit	MQ.5	MQ.5
AWS Bewährte grundlegende Sicherheitsmethoden	MQ.6	MQ.6
AWS Bewährte grundlegende Sicherheitsmethoden	MSK.1	MSK.1
AWS Bewährte Methoden für grundlegende Sicherheit	MSK.2	MSK.2
AWS Bewährte Methoden für grundlegende Sicherheit	Neptun.1	Neptun.1
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.2	Neptun.2
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.3	Neptun.3
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.4	Neptun.4

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.5	Neptun.5
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.6	Neptun.6
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.7	Neptun.7
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.8	Neptun.8
AWS Bewährte grundlegende Sicherheitsmethoden	Neptun.9	Neptun.9
AWS Bewährte grundlegende Sicherheitsmethoden	NetworkFirewall1.	NetworkFirewall1.
AWS Bewährte grundlegende Sicherheitsmethoden	NetworkFirewall2.	NetworkFirewall2.2
AWS Bewährte grundlegende Sicherheitsmethoden	NetworkFirewall3.	NetworkFirewall3.
AWS Bewährte grundlegende Sicherheitsmethoden	NetworkFirewall4.	NetworkFirewall4.
AWS Bewährte grundlegende Sicherheitsmethoden	NetworkFirewall5.	NetworkFirewall5.

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	NetworkFirewall6.	NetworkFirewall.6
AWS Bewährte grundlegende Sicherheitsmethoden	NetworkFirewall9.	NetworkFirewall.9
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.1	OpenSearch.1
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.2	OpenSearch.2
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.3	OpenSearch.3
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.4	OpenSearch.4
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.5	OpenSearch.5
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.6	OpenSearch.6
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.7	OpenSearch.7
AWS Bewährte grundlegende Sicherheitsmethoden	OpenSearch.8	OpenSearch.8

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	Opensearch.10	Öffne Suche.10
AWS Bewährte grundlegende Sicherheitsmethoden	PCA.1	PCA. 1
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.1	RDS.1
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.2	RDS.2
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.3	RDS.3
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.4	RDS.4
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.5	RDS.5
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.6	RDS.6
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.7	RDS.7
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.8	RDS.8

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.9	RDS.9
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.10	RDS.10
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.11	RDS.11
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.12	RDS.12
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.13	RDS.13
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.14	RDS.14
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.15	RDS.15
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.16	RDS.16
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.17	RDS.17
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.18	RDS.18

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.19	RDS.19
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.20	RDS.20
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.21	RDS.21
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.22	RDS.22
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.23	RDS.23
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.24	RDS.24
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.25	RDS.25
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.26	RDS.26
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.27	RDS. 27
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.34	RDS.34

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	RDS.35	RDS.35
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.1	Redshift.1
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.2	Redshift.2
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.3	Redshift.3
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.4	Redshift.4
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.6	Redshift.6
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.7	Redshift.7
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.8	Redshift.8
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.9	Redshift.9
AWS Bewährte grundlegende Sicherheitsmethoden	Redshift.10	Redshift.10

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	Route 53.2	Route 53.2
AWS Bewährte grundlegende Sicherheitsmethoden	S3.1	S3.1
AWS Bewährte grundlegende Sicherheitsmethoden	S3.2	S3.2
AWS Bewährte grundlegende Sicherheitsmethoden	S3.3	S3.3
AWS Bewährte grundlegende Sicherheitsmethoden	S3.4	S3.4
AWS Bewährte grundlegende Sicherheitsmethoden	S3.5	S3.5
AWS Bewährte grundlegende Sicherheitsmethoden	S3.6	S3.6
AWS Bewährte grundlegende Sicherheitsmethoden	S3.7	S 3,7
AWS Bewährte grundlegende Sicherheitsmethoden	S3.8	S3.8
AWS Bewährte grundlegende Sicherheitsmethoden	S3.9	S3.9

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	S3.11	S3.11
AWS Bewährte grundlegende Sicherheitsmethoden	S3.12	S3.12
AWS Bewährte grundlegende Sicherheitsmethoden	S3.13	S3.13
AWS Bewährte grundlegende Sicherheitsmethoden	S3.14	S3,14
AWS Bewährte grundlegende Sicherheitsmethoden	S3.15	S3,15
AWS Bewährte grundlegende Sicherheitsmethoden	S3.17	S3,17
AWS Bewährte grundlegende Sicherheitsmethoden	S3.19	S3,19
AWS Bewährte grundlegende Sicherheitsmethoden	S3.19	S3,20
AWS Bewährte grundlegende Sicherheitsmethoden	SageMaker1.	SageMaker1.
AWS Bewährte grundlegende Sicherheitsmethoden	SageMaker2.	SageMaker2.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	SageMaker3.	SageMaker3.
AWS Bewährte grundlegende Sicherheitsmethoden	SecretsManager1.	SecretsManager1.
AWS Bewährte grundlegende Sicherheitsmethoden	SecretsManager2.	SecretsManager2.2
AWS Bewährte grundlegende Sicherheitsmethoden	SecretsManager3.	SecretsManager3.
AWS Bewährte grundlegende Sicherheitsmethoden	SecretsManager4.	SecretsManager4.
AWS Bewährte grundlegende Sicherheitsmethoden	SNS.1	SNS.1
AWS Bewährte grundlegende Sicherheitsmethoden	SNS.2	SNS.2
AWS Bewährte grundlegende Sicherheitsmethoden	SQS.1	SQS.1
AWS Bewährte grundlegende Sicherheitsmethoden	SSM.1	SSM.1
AWS Bewährte grundlegende Sicherheitsmethoden	SSM.2	SSM.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	SSM.3	SSM.3
AWS Bewährte grundlegende Sicherheitsmethoden	SSM.4	SSM.4
AWS Bewährte grundlegende Sicherheitsmethoden	StepFunctions1.	StepFunctions1.
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.1	WAF.1
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.2	WAF.2
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.3	WAF.3
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.4	WAF.4
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.6	WAF.6
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.7	WAF.7
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.8	WAF.8

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard steuer-ID im Security Hub CSPM)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID in Security Hub CSPM)
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.10	WAF.10
AWS Bewährte grundlegende Sicherheitsmethoden	WAF.11	WAF.11
AWS Bewährte Methoden zur grundlegenden Sicherheit	WAF.12	WAF. 12

Weitere Ressourcen

- Hilfe bei Problemen mit der Beweiserhebung für diesen Datenquellentyp finden Sie unter. Meine Bewertung bezieht sich nicht auf die Erfassung von Nachweisen zur Konformitätsprüfung von AWS Security Hub CSPM
- Informationen zum Erstellen eines benutzerdefinierten Steuerelements mit diesem Datenquellentyp finden Sie unterErstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager.
- Informationen zum Erstellen eines benutzerdefinierten Frameworks, das Ihr benutzerdefiniertes Steuerelement verwendet, finden Sie unterErstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager.
- Informationen zum Hinzufügen Ihres benutzerdefinierten Steuerelements zu einem vorhandenen benutzerdefinierten Framework finden Sie unterBearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager.

AWS API-Aufrufe werden unterstützt von AWS Audit Manager

Sie können Audit Manager verwenden, um Schnappschüsse Ihrer AWS Umgebung als Nachweis für Audits zu erfassen. Wenn Sie ein benutzerdefiniertes Steuerelement erstellen oder bearbeiten, können Sie einen oder mehrere AWS API-Aufrufe als Datenquellenzuordnung für die Erfassung von Nachweisen angeben. Audit Manager führt dann API-Aufrufe an die entsprechenden AWS-Services Personen durch und sammelt eine Momentaufnahme der Konfigurationsdetails für Ihre AWS Ressourcen.

Für jede Ressource, die in den Geltungsbereich eines API-Aufrufs fällt, erfasst Audit Manager einen Konfigurations-Snapshot und wandelt ihn in Beweise um. Dies führt zu einem Beweis pro Ressource, im Gegensatz zu einem Beweis pro API-Aufruf.

Wenn der `ec2_DescribeRouteTables`-API-Aufruf beispielsweise Konfigurations-Snapshots aus fünf Routing-Tabellen erfasst, erhalten Sie insgesamt fünf Beweise für den einzelnen API-Aufruf. Jeder Beweis ist eine Momentaufnahme der Konfiguration einer einzelnen Routing-Tabelle.

Themen

Wichtige Punkte

Paginierte API-Aufrufe

Viele AWS-Services sammeln und speichern eine große Datenmenge. Wenn ein `list`, `describe` oder `get` API-Aufruf versucht, Ihre Daten zurückzugeben, kann es daher zu vielen Ergebnissen kommen. Wenn die Datenmenge zu groß ist, um sie in einer einzigen Antwort zurückzugeben, können die Ergebnisse mithilfe einer Seitennummerierung in überschaubarere Teile aufgeteilt werden. Dadurch werden die Ergebnisse in „Seiten“ mit Daten aufgeteilt, sodass die Antworten einfacher zu handhaben sind.

Einige davon Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen sind paginiert. Das bedeutet, dass sie zunächst Teilergebnisse zurückgeben und nachfolgende Anfragen erfordern, um die gesamte Ergebnismenge zurückzugeben. Beispielsweise gibt der Amazon DBInstancesRDS-Describe-Vorgang bis zu 100 Instances gleichzeitig zurück, und nachfolgende Anfragen sind erforderlich, um die nächste Ergebnisseite zurückzugeben.

Ab dem 08. März 2023 unterstützt Audit Manager paginierte API-Aufrufe als Datenquelle für die Beweiserhebung. Wenn bisher ein paginierter API-Aufruf als Datenquelle verwendet wurde, wurde in der API-Antwort nur eine Teilmenge Ihrer Ressourcen zurückgegeben (bis zu 100 Ergebnisse). Jetzt ruft Audit Manager den paginierten API-Vorgang mehrmals auf und ruft jede Ergebnisseite ab, bis alle Ressourcen zurückgegeben wurden. Für jede Ressource erfasst Audit Manager dann einen Konfigurations-Snapshot und speichert ihn als Beweis. Da Ihre gesamten Ressourcen jetzt in der API-Antwort erfasst sind, ist es wahrscheinlich, dass Sie nach dem 08. März 2023 eine Zunahme der gesammelten Beweise feststellen werden.

Audit Manager übernimmt die Paginierung von API-Aufrufen automatisch für Sie. Wenn Sie eine benutzerdefinierte Kontrolle erstellen, die einen paginierten API-Aufruf als Datenquelle verwendet, müssen Sie keine Paginierungsparameter angeben.

Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen

In Ihren benutzerdefinierten Kontrollen können Sie jeden der folgenden API-Aufrufe als Datenquelle verwenden. Audit Manager kann diese API-Aufrufe dann verwenden, um Nachweise über Ihre AWS Nutzung zu sammeln.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
acm_ GetAccountConfiguration	Erstellt einen Überblick über die Kontokonfigurationsoptionen, die mit Ihrem AWS-Konto verknüpft sind.
acm_ ListCertificates	Rufen Sie eine Liste mit Zertifikat- ARNs und Domainnamen ab.
Autoscaling_ DescribeAutoScalingGroups	Sammeln Sie einen Snapshot über die Auto Scaling Scaling-Gruppen in Ihrem AWS-Konto.
backup_ ListBackupPlans	Rufen Sie eine Liste aller aktiven Backup-Pläne in Ihrem ab. AWS-Konto
Grundstein_ GetModelInvocationLoggingConfiguration	Erfassen Sie eine Momentaufnahme der aktuellen Konfigurationswerte für die Protokollierung von Modellaufrufen für Modelle in Ihrem. AWS-Konto

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
cloudfront_ ListDistributions	Rufen Sie eine Liste aller Distributionen in Ihrem ab. AWS-Konto
cloudtrail_ DescribeTrails	Erfasst einen Snapshot der Einstellungen für einen oder mehrere Trails, die mit der aktuellen Region für Ihr AWS-Konto verknüpft sind.
Cloudtrail_ ListTrails	Rufen Sie eine Liste der Trails ab, die sich in Ihrem befinden. AWS-Konto
cloudwatch_ DescribeAlarms	Erfasst einen Konfigurations-Snapshot der Alarme, die für Ihr AWS-Konto verwendet werden.
konfigurieren_ DescribeConfigRules	Rufen Sie Details zu Ihren AWS Config Regeln ab.
config_ DescribeDeliveryChannels	Erfasst einen Konfigurations-Snapshot für die Lieferkanäle in Ihrem AWS-Konto.
direktverbinden_ DescribeDirectConnectGateways	Rufen Sie eine Liste all Ihrer Gateways ab. Direct Connect
directconnect_ DescribeVirtualGateways	Ruft eine Liste der Virtual Private Gateways ab, die zum AWS-Konto gehören.
docdb_ DescribeCertificates	Erfasst eine Liste von Zertifikaten für Ihr AWS-Konto.
docDB_Beschreiben DBClusterParameterGroups	Erfasst eine Liste mit `DBClusterParameterGroup` -Beschreibungen für Ihr AWS-Konto.
DocDB_Beschreiben DBInstances	Erfasst Informationen über bereitgestellte Amazon-DynamoDB-Instances für Ihr AWS-Konto.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
Cloudwatch_ DescribeAlarms	Sammeln Sie Informationen über die Alarme in Ihrem. AWS-Konto
cloudtrail_ DescribeTrails	Erstelle eine Momentaufnahme der Einstellungen für einen oder mehrere Trails, die mit deinem verknüpft sind. AWS-Konto
dynamodb_ DescribeTable	Erfasst Konfigurations-Snapshots für die DynamoDB-Tabellen in Ihrem AWS-Konto. Wenn Sie diese API als Datenquelle verwenden, müssen Sie nicht den Namen einer bestimmten DynamoDB-Tabelle angeben. Stattdessen verwendet Audit Manager den `ListTables` -Vorgang, um alle Ihre Tabellen aufzulisten. Für jede aufgelistete Tabelle führt Audit Manager dann den `DescribeTable` -Vorgang aus, um Beweise für diese Ressource zu generieren.
dynamodb_ ListBackups	Ruft eine Liste der DynamoDB-Backups ab, die mit Ihrem AWS-Konto verknüpft sind.
dynamodb_ ListTables	Ruft eine Liste aller Tabellennamen ab, die mit Ihrem AWS-Konto und Ihrem aktuellen Endpunkt verknüpft sind.
ec2_ DescribeA ddresses	Erstellt einen Snapshot Ihrer Elastic-IP-Adressen.
ec2_ DescribeC ustomerGateways	Erfasst einen Snapshot Ihrer VPN-Kunden-Gateways.
ec2_ DescribeE gressOnlyInternetG ateways	Erfasst einen Snapshot Ihrer Internet-Gateways für ausgehenden Datenverkehr.
ec2_ DescribeF lowLogs	Erfasst einen Snapshot Ihrer Flussprotokolle.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
ec2_ DescribeInstances	Erfasst einen Snapshot Ihrer Instances.
ec2_ DescribeInternetGateways	Erfasst einen Snapshot Ihrer Internet-Gateways.
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Sammeln Sie eine Beschreibung der Verknüpfungen zwischen den virtuellen Schnittstellengruppen und den lokalen Gateway-Routentabellen in Ihrem. AWS-Konto
ec2_ DescribeLocalGateways	Erfasst einen Snapshot Ihrer lokalen Gateways.
ec2_ DescribeLocalGatewayVirtualInterfaces	Erfasst einen Snapshot der virtuellen Schnittstellen Ihres lokalen Gateways.
ec2_ DescribeNatGateways	Erfasst einen Snapshot Ihrer NAT-Gateways.
ec2_ DescribeNetworkAcls	Erfassen Sie einen Snapshot Ihres Netzwerks. ACLs
ec2_ DescribeRouteTables	Erfasst einen Snapshot Ihrer Routing-Tabellen.
ec2_ DescribeSecurityGroups	Erfasst einen Snapshot Ihrer Sicherheitsgruppen.
ec2_ DescribeSecurityGroupRules	Erstellen Sie einen Snapshot einer oder mehrerer Ihrer Sicherheitsgruppenregeln.
ec2_ DescribeTransitGateways	Erfasst einen Snapshot Ihrer Transit-Gateways.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
ec2_ DescribeVolumes	Erfasst einen Snapshot Ihrer VPC-Endpunkte.
ec2_ DescribeVpcs	Sammle einen Schnappschuss von deinem. VPCs
ec2_ DescribeVpcEndpoints	Erfasst einen Snapshot Ihrer VPC-Endpunkte.
ec2_ DescribeVpcEndpointConnections	Erfassen Sie einen Snapshot der VPC-Endpunktverbindungen zu Ihren VPC-Endpunktdiensten, einschließlich aller Endpunkte, deren Annahme noch aussteht.
ec2_ DescribeVpcEndpointServiceConfigurations	Erfassen Sie einen Snapshot der VPC-Endpunktdienstkonfigurationen in Ihrem AWS-Konto.
ec2_ DescribeVpcPeeringConnections	Erfasst einen Snapshot Ihrer VPN-Verbindungen.
ec2_ DescribeVpnConnections	Erfasst einen Snapshot Ihrer VPN-Verbindungen.
ec2_ DescribeVpnGateways	Erfasst einen Snapshot Ihrer virtuellen privaten Gateways.
ec2_ GetEbsDefaultKmsKeyId	Erstellen Sie einen Snapshot der Standardwerte AWS KMS key für die EBS-Verschlüsselung AWS-Konto in Ihrer aktuellen Region.
ec2_ GetEbsEncryptionByDefault	Beschreiben Sie, ob die EBS-Verschlüsselung für Sie AWS-Konto in der aktuellen Region standardmäßig aktiviert ist.
ecs_ DescribeClusters	Erfasst einen Snapshot Ihrer ECS-Cluster.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
eks_ DescribeAddonVersions	Erfasst einen Snapshot Ihrer Add-on-Versionen.
elastischer Cache_ DescribeCacheClusters	Erfasst einen Snapshot Ihrer bereitgestellten Cluster.
elastische_ DescribeServiceUpdates	Erfassen Sie eine Momentaufnahme der Service-Updates für Amazon ElastiCache.
elastisches Dateisystem_ DescribeAccessPoints	Erfassen Sie einen Snapshot der Amazon EFS-Zugriffspunkte in Ihrem AWS-Konto.
elastisches Dateisystem_ DescribeFileSystems	Erfasst einen Snapshot Ihrer Amazon EFS-Dateisysteme.
elastischer Lastenausgleich v2_ DescribeLoadBalancers	Erfassen Sie einen Snapshot der Load Balancer in Ihrem. AWS-Konto
Elastic LoadBalancing v2_DescribeSSLPolicies	Erfasst einen Snapshot der Richtlinien, die Sie für die SSL-Aushandlung verwenden.
elastischer Lastenausgleich v2_ DescribeTargetGroups	Erfasst einen Snapshot Ihrer ELB-Zielgruppen.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
elastisches MapReduce_ ListSecurityConfig urations	Ruft eine Liste der Sicherheitskonfigurationen, die für Ihr AWS-Konto sichtbar sind, zusammen mit Datum und Uhrzeit der Erstellung sowie ihrer Namen ab.
Veranstaltungen_ ListConnections	Rufen Sie eine Liste der EventBridge Amazon-Verbindungen in Ihrem ab AWS-Konto.
Veranstaltungen_ ListEventBuses	Rufen Sie eine Liste der EventBridge Amazon-Eventbusse in Ihrem System ab AWS-Konto, einschließlich des Standard-Event-Busses, benutzerdefinierter Event-Busse und Partner-Eventbusse.
Veranstaltungen_ ListEventSources	Ruft eine Liste der Partner-Ereignisquellen ab, die mit Ihrem AWS-Konto geteilt wurden.
Veranstaltungen_ ListRules	Rufen Sie eine Liste Ihrer EventBridge Amazon-Regeln ab.
firehose_ ListDeliv eryStreams	Ruft eine Liste Ihrer Bereitstellungsstreams ab.
fsx_ DescribeF ileSystems	Erfasst einen Snapshot der Dateisysteme, die Ihrem AWS-Konto angehören.
Wachdienst_ ListDetectors	Rufen Sie eine Liste der Ressourcen `detectorIds` für Ihren GuardDuty Amazon-Detektor ab.
Ich bin _ GenerateC redentialReport	Generiert einen Bericht über Anmeldeinformationen für Ihr AWS-Konto.
ich bin_ GetAccoun tPasswordPolicy	Erfasst einen Snapshot über die Passwortrichtlinie für Ihr AWS-Konto.
ich bin_ GetAccoun tSummary	Erfasst einen Snapshot der IAM-Entity-Nutzung und der IAM-Kontingente in Ihrem AWS-Konto.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
ich bin_ ListGroups	Rufen Sie eine Liste der IAM-Gruppen ab, denen ein Pfadpräfix zugeordnet ist, das in Ihrem verfügbar ist. AWS-Konto
iam_-Anbieter ListOpen IDConnect	Ruft eine Liste der Ressourcenobjekte des IAM OpenID Connect (OIDC)-Anbieters ab, die in Ihrem AWS-Konto definiert sind.
iam_ ListPolicies	Ruft eine Liste aller verwalteten Richtlinien auf, die in Ihrem AWS-Konto verfügbar sind, einschließlich der benutzerdefinierten verwalteten Richtlinien und aller von AWS-verwalteten Richtlinien.
ich bin_ ListRoles	Rufen Sie eine Liste der IAM-Rollen ab, die einem Pfadpräfix zugeordnet sind, das in Ihrem verfügbar ist. AWS-Konto
IAM_List SAMLProviders	Ruft eine Liste der Ressourcenobjekte des SAML-Anbieters ab, die in IAM in Ihrem AWS-Konto definiert sind.
ich bin_ ListUsers	Rufen Sie eine Liste der IAM-Benutzer in Ihrem ab. AWS-Konto
iam_ ListVirtual MFADevices	Ruft eine Liste der virtuellen MFA-Geräte ab, die in Ihrem AWS-Konto definiert sind.
kafka_ ListClusters	Rufen Sie eine Liste der Amazon MSK-Cluster in Ihrem AWS-Konto ab.
kafka_ ListKafka Versions	Ruft eine Liste der Objekte der Apache Kafka-Version in Ihrem AWS-Konto ab.
Kinese_ ListStreams	Ruft eine Liste Ihrer Kinesis-Datenströme ab.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
kms_ GetKeyPolicy	Audit Manager verwendet diese API, um einen Snapshot über die Schlüsselrichtlinien für das AWS KMS keys in Ihrem AWS-Konto zu erfassen. Wenn Sie diese API als Datenquelle verwenden, müssen Sie nicht den Namen einer bestimmten API angeben. AWS KMS key Stattdessen verwendet Audit Manager den `ListKeys`-Vorgang, um alle Ihre KMS-Schlüssel aufzulisten. Für jeden aufgelisteten KMS-Schlüssel führt Audit Manager dann den `GetKeyPolicy` -Vorgang aus, um Beweise für diese Ressource zu generieren.
kms_ GetKeyRotationStatus	Audit Manager verwendet diese API, um eine Momentaufnahme darüber zu sammeln, ob die automatische Rotation für die AWS KMS keys in Ihrem aktiviert ist AWS-Konto. Wenn Sie diese API als Datenquelle verwenden, müssen Sie nicht den Namen einer bestimmten API angeben AWS KMS key. Stattdessen verwendet Audit Manager den `ListKeys`-Vorgang, um alle Ihre KMS-Schlüssel aufzulisten. Für jeden aufgelisteten KMS-Schlüssel führt Audit Manager dann den `GetKeyRotationStatus` -Vorgang aus, um Beweise für diese Ressource zu generieren.
kms_ ListKeys	Rufen Sie eine Liste der AWS KMS keys in Ihrem ab. AWS-Konto
Lambda_ ListFunctions	Rufen Sie eine Liste der Lambda-Funktionen in Ihrem ab AWS-Konto, mit der jeweiligen versionsspezifischen Konfiguration.
RDS_DescribeDBClusters	Erfassen Sie einen Snapshot der vorhandenen Amazon Aurora Aurora-DB-Cluster und Multi-AZ-DB-Cluster in Ihrem AWS-Konto.
RDS_DescribeDBInstances	Erfasst einen Snapshot der bereitgestellten RDS-Instances in Ihrem AWS-Konto.
rds_ DescribeDbInstanceAutomatedBackups	Erfassen Sie einen Snapshot der Backups sowohl für aktuelle als auch für gelöschte Instanzen in Ihrem. AWS-Konto

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
rds_ DescribeDbSecurityGroups	Erfassen Sie eine Momentaufnahme der DBSecurity Gruppen in Ihrem. AWS-Konto
redshift_ DescribeClusters	Erfasst einen Snapshot des bereitgestellten Amazon-Redshift-Clusters in Ihrem AWS-Konto.
s3_ GetBucketEncryption	Erfasst einen Snapshot, der die Standardverschlüsselungskonfiguration für Ihre S3-Buckets zeigt. Wenn Sie diese API als Datenquelle verwenden, müssen Sie nicht den Namen eines bestimmten S3-Buckets angeben. Stattdessen verwendet Audit Manager den `ListBuckets` Vorgang, um die Buckets aufzulisten, die in derselben Weise AWS-Region wie Ihre Bewertung erstellt wurden. Für jeden aufgelisteten Bucket führt Audit Manager dann den `GetBucketEncryption` -Vorgang aus, um Beweise für diese Ressource zu generieren. Audit Manager kann den Verschlüsselungsstatus nur für Buckets angeben, die in derselben Weise AWS-Region wie Ihre Bewertung erstellt wurden. Wenn Sie den Verschlüsselungsstatus all Ihrer S3-Buckets in mehreren einsehen möchten, empfehlen wir Ihnen AWS-Regionen, in jedem Bucket, in AWS-Region dem Sie über einen S3-Bucket verfügen, eine Bewertung zu erstellen.
s3_ ListBuckets	Rufen Sie eine Liste der S3-Buckets in Ihrem ab. AWS-Konto Audit Manager kann nur Buckets auflisten, die in derselben Weise AWS-Region wie Ihre Bewertung erstellt wurden. Wenn Sie alle Ihre S3-Buckets über mehrere AWS-Region s hinweg sehen möchten, empfehlen wir Ihnen, in jedem Bereich, in AWS-Region dem Sie einen S3-Bucket haben, eine Bewertung zu erstellen.
sagemaker_ ListAlgorithms	Rufen Sie eine Liste der Algorithmen für maschinelles Lernen in Ihrem ab. AWS-Konto

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
Sagemaker_ ListDomains	Rufen Sie eine Liste der Domains in Ihrem ab. AWS-Konto
Sagemaker_ ListEndpoints	Rufen Sie eine Liste der Endpunkte in Ihrem ab. AWS-Konto
Sagemaker_ ListEndpointConfigs	Rufen Sie eine Liste der Endpunktkonfigurationen in Ihrem ab. AWS-Konto
sagemaker_ ListFlowDefinitions	Rufen Sie eine Liste der Flow-Definitionen in Ihrem ab. AWS-Konto
Sagemaker_ ListHumanTaskUis	Rufen Sie eine Liste der Benutzeroberflächen für menschliche Aufgaben in Ihrem ab. AWS-Konto
Sagemaker_ ListLabelingJobs	Rufen Sie eine Liste der Kennzeichnungsaufträge in Ihrem ab. AWS-Konto
Sagemaker_ ListModels	Rufen Sie eine Liste der Modelle in Ihrem ab. AWS-Konto
Sagemaker _ ListModel BiasJobDefinitions	Rufen Sie eine Liste der Model Bias-Jobdefinitionen in Ihrem ab. AWS-Konto
Sagemaker_ ListModelCards	Rufen Sie eine Liste der Modellkarten in Ihrem ab. AWS-Konto
Sagemaker_ ListModelQualityJo bDefinitions	Rufen Sie eine Liste der Jobdefinitionen zur Überwachung der Modellqua lität in Ihrem ab. AWS-Konto
Sagemaker_ ListMonitoringAlerts	Ruft eine Liste der Warnungen für einen bestimmten Überwachungsplan ab.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
sagemaker_ ListMonitoringSchedules	Rufen Sie eine Liste aller Überwachungspläne in Ihrem ab. AWS-Konto
Sagemaker_ ListTrainingJobs	Rufen Sie eine Liste der Ausbildungsjobs in Ihrem ab. AWS-Konto
Sagemaker_ ListUserProfiles	Rufen Sie eine Liste von Benutzerprofilen in Ihrem ab. AWS-Konto
secretsmanager_ ListSecrets	Rufen Sie eine Liste der Geheimnisse ab, die in Ihrem gespeichert sind AWS-Konto, ohne Geheimnisse, die zum Löschen markiert sind.
sns_ ListTopics	Rufen Sie eine Liste der SNS-Themen in Ihrem ab. AWS-Konto
sqs_ ListQueues	Rufen Sie eine Liste der SQS-Warteschlangen in Ihrem ab. AWS-Konto
waf-regional_ ListWebAcls	Rufen Sie eine Liste der ACLSummaryWebobjekte für Ihre ab. AWS-Konto
waf-regional_ ListRules	Rufen Sie eine Liste der Objekte für Sie ab. RuleSummary AWS-Konto
waf_ ListRuleGroups	Rufen Sie eine Liste der RuleGroupSummaryObjekte für die Regelgruppen in Ihrem AWS-Konto ab.
waf_ ListRules	Rufen Sie eine Liste der RuleSummaryObjekte für Sie AWS-Konto ab.
waf_ ListWebAcls	Rufen Sie eine Liste der ACLSummaryWebobjekte für Ihre AWS-Konto ab.

Im AWS License Manager Standard-Framework verwendete API-Aufrufe

Im AWS License Manager-Standard-Framework verwendet Audit Manager eine benutzerdefinierte Aktivität mit dem Namen `GetLicenseManagerSummary`, um Beweise zu sammeln. Diese Aktivität ruft die folgenden drei License Manager auf APIs:

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

Die zurückgegebenen Daten werden dann in Beweise umgewandelt und den entsprechenden Kontrollen in Ihrer Bewertung beigefügt.

Beispiel

Nehmen wir an, Sie verwenden zwei lizenzierte Produkte (SQL Dienst 2017 und Oracle Database Enterprise Edition). Zunächst ruft die `GetLicenseManagerSummary` Aktivität die ListLicenseConfigurationsAPI auf, die Einzelheiten zu den Lizenzkonfigurationen in Ihrem Konto bereitstellt. Als Nächstes fügt sie zusätzliche Kontextdaten für jede Lizenzkonfiguration hinzu, indem sie und aufruft ListUsageForLicenseConfiguration. ListAssociationsForLicenseConfiguration Schließlich werden die Lizenzkonfigurationsdaten in Beweise umgewandelt und an die jeweiligen Kontrollen im Framework angehängt (4.5 – vom Kunden verwaltete Lizenz für SQL Server 2017 und 3.0.4 – vom Kunden verwaltete Lizenz für Oracle Database Enterprise Edition).

Wenn Sie ein lizenziertes Produkt verwenden, das durch keine der Kontrollen im Framework abgedeckt wird, werden diese Lizenzkonfigurationsdaten als Beweis an die folgende Kontrolle angehängt: 5.0 – Vom Kunden verwaltete Lizenz für andere Lizenzen.

Weitere Ressourcen

- Hilfe bei Problemen mit der Beweiserhebung für diesen Datenquellentyp finden Sie unter. In meiner Bewertung werden keine Beweise für Konfigurationsdaten für einen AWS API-Aufruf gesammelt
- Informationen zum Erstellen eines benutzerdefinierten Steuerelements mit diesem Datenquellentyp finden Sie unterErstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager.
- Informationen zum Erstellen eines benutzerdefinierten Frameworks, das Ihr benutzerdefiniertes Steuerelement verwendet, finden Sie unterErstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager.
- Informationen zum Hinzufügen Ihres benutzerdefinierten Steuerelements zu einem vorhandenen benutzerdefinierten Framework finden Sie unterBearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager.

AWS CloudTrail Eventnamen werden unterstützt von AWS Audit Manager

Sie können Audit Manager verwenden, um AWS CloudTrail Managementereignisse und globale Serviceereignisse als Nachweis für Audits zu erfassen. Wenn Sie ein benutzerdefiniertes Steuerelement erstellen oder bearbeiten, können Sie einen oder mehrere CloudTrail Ereignisnamen als Datenquellenzuordnung für die Erfassung von Nachweisen angeben. Audit Manager filtert dann Ihre CloudTrail Logs anhand der von Ihnen ausgewählten Keywords und importiert die Ergebnisse als Nachweis für Benutzeraktivitäten.

> **Note**
>
> Audit Manager erfasst nur Managementereignisse und globale Serviceereignisse. Datenereignisse und Ereignisse mit Erkenntnissen stehen nicht als Beweis zur Verfügung. Weitere Informationen zu den verschiedenen CloudTrail Ereignistypen finden Sie unter CloudTrail Konzepte im AWS CloudTrail Benutzerhandbuch.

Als Ausnahme von den oben genannten werden die folgenden CloudTrail Ereignisse von Audit Manager nicht unterstützt:

- kms_ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- Kinesis-Video_ GetDataEndpoint
- Kinesisvideo_ GetSignalingChannelEndpoint
- Kinesisvideo_ DescribeSignalingChannel
- Kinesisvideo_ DescribeStream

Ab dem 11. Mai 2023 unterstützt Audit Manager keine schreibgeschützten CloudTrail Ereignisse mehr als Schlüsselwörter für die Beweiserhebung. Wir haben insgesamt 3.135 schreibgeschützte Keywords entfernt. Da sowohl Kunden AWS-Services als auch beide Seiten Leseanrufe tätigen APIs, kommt es bei schreibgeschützten Ereignissen zu einem hohen Geräuschpegel. Aus diesem Grund sammeln schreibgeschützte Stichwörter eine Menge Beweise, die für Audits weder zuverlässig noch relevant sind. Zu den schreibgeschützten Schlüsselwörtern gehören `ListDescribe`,, und `Get` API-

Aufrufe (z. B. GetObjectund ListBucketsfür Amazon S3). Wenn Sie eines dieser Schlüsselwörter für die Beweiserhebung verwendet haben, müssen Sie nichts unternehmen. Die Schlüsselwörter wurden automatisch aus der Audit Manager-Konsole und aus Ihren Bewertungen entfernt, und es werden keine Beweise mehr für diese Schlüsselwörter gesammelt.

Weitere Ressourcen

- Hilfe bei Problemen mit der Beweiserhebung für diesen Datenquellentyp finden Sie unter. In meiner Bewertung werden von AWS CloudTrail keine Beweise für Benutzeraktivitäten gesammelt
- Informationen zum Erstellen eines benutzerdefinierten Steuerelements mit diesem Datenquellentyp finden Sie unterErstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager.
- Informationen zum Erstellen eines benutzerdefinierten Frameworks, das Ihr benutzerdefiniertes Steuerelement verwendet, finden Sie unterErstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager.
- Informationen zum Hinzufügen Ihres benutzerdefinierten Steuerelements zu einem vorhandenen benutzerdefinierten Framework finden Sie unterBearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager.

Einrichtung AWS Audit Manager mit den empfohlenen Einstellungen

Bevor Sie Audit Manager verwenden, ist es wichtig, dass Sie die folgenden Einrichtungsaufgaben ausführen.

In diesem Kapitel werden die Voraussetzungen, die Kontoeinrichtung, die Benutzerberechtigungen und die erforderlichen Schritte zur Aktivierung und Konfiguration von Audit Manager mit den empfohlenen Funktionen und Integrationen erläutert. Nach Abschluss dieser Aufgaben sind Sie bereit, Audit Manager zu verwenden und mit der Optimierung Ihrer Audit- und Compliance-Bemühungen zu beginnen.

Inhalt

Voraussetzungen für die Einrichtung AWS Audit Manager

Bevor Sie es verwenden können AWS Audit Manager, müssen Sie sicherstellen, dass Sie Ihre Rechte AWS-Konto und Benutzerberechtigungen ordnungsgemäß eingerichtet haben.

Auf dieser Seite werden die notwendigen Schritte beschrieben, um einen AWS-Konto (falls erforderlich) zu erstellen, einen Administratorbenutzer zu konfigurieren und die für den Zugriff und die Aktivierung von Audit Manager erforderlichen Berechtigungen zu gewähren.

Aufgaben

1. Melden Sie sich an für ein AWS-Konto
2. Erstellen eines Benutzers mit Administratorzugriff
3. Fügen Sie die Berechtigungen hinzu, die für Zugriff und Aktivierung des Audit Manager erforderlich sind

> **Important**
>
> Wenn Sie IAM bereits eingerichtet AWS haben, können Sie die Aufgaben 1 und 2 überspringen. Sie müssen jedoch Aufgabe 3 abschließen, um sicherzustellen, dass Sie über die erforderlichen Berechtigungen zum Einrichten von Audit Manager verfügen.

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

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

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

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

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

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

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

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

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

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Fügen Sie die Berechtigungen hinzu, die für Zugriff und Aktivierung des Audit Manager erforderlich sind

Sie müssen den Benutzern die erforderlichen Berechtigungen erteilen, um Audit Manager aktivieren zu können. Verwenden Sie für Benutzer, die vollen Zugriff auf Audit Manager benötigen, die AWSAuditManagerAdministratorAccessverwaltete Richtlinie. Dies ist eine AWS verwaltete Richtlinie, die in Ihrer verfügbar ist AWS-Konto, und sie ist die empfohlene Richtlinie für Audit Manager Manager-Administratoren.

> **Tip**
>
> Aus Sicherheitsgründen empfehlen wir, zunächst mit AWS verwalteten Richtlinien zu beginnen und dann zu Berechtigungen mit den geringsten Rechten überzugehen. AWS verwaltete Richtlinien gewähren Berechtigungen für viele gängige Anwendungsfälle. Beachten Sie jedoch, dass AWS verwaltete Richtlinien, da sie von allen AWS Kunden verwendet werden können, möglicherweise nicht die Berechtigungen mit den geringsten

Rechten für Ihre speziellen Anwendungsfälle gewähren. Daher empfehlen wir Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die spezifisch auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien im AWS Identity and Access Management - Benutzerhandbuch.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in: AWS IAM Identity Center

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Nächste Schritte

Nachdem Sie Ihre Berechtigungen eingerichtet AWS-Konto und die erforderlichen Berechtigungen erteilt haben, können Sie Audit Manager aktivieren. step-by-stepAnweisungen finden Sie unterAktiviert AWS Audit Manager.

Aktiviert AWS Audit Manager

Nachdem Sie die Voraussetzungen für die Einrichtung von Audit Manager erfüllt haben, können Sie den Dienst in Ihrer AWS Umgebung aktivieren.

Auf dieser Seite erfahren Sie, wie Sie Audit Manager mithilfe der Audit Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager Manager-API aktivieren. Wählen Sie die Methode, die Ihren Anforderungen am besten entspricht, und folgen Sie den entsprechenden Schritten, um Audit Manager zum Laufen zu bringen.

Voraussetzungen

Stellen Sie sicher, dass Sie alle unter beschriebenen Aufgaben abgeschlossen habenVoraussetzungen für die Einrichtung AWS Audit Manager.

Verfahren

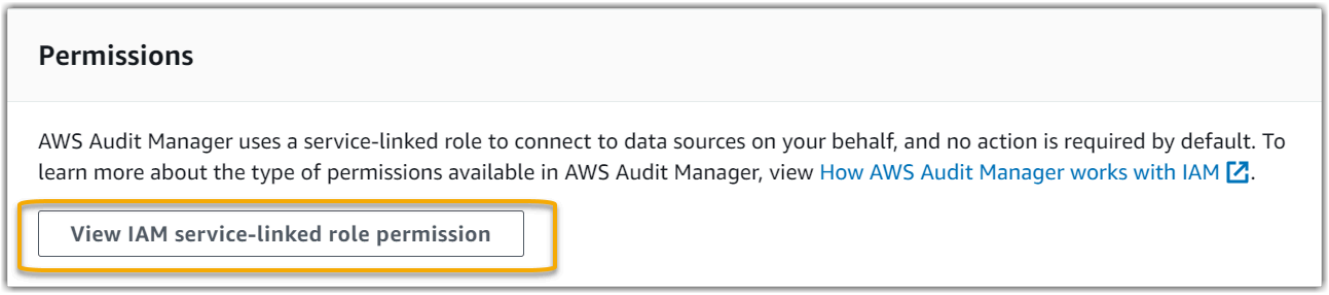
Sie können Audit Manager mithilfe der AWS-Managementkonsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) aktivieren.

Audit Manager console

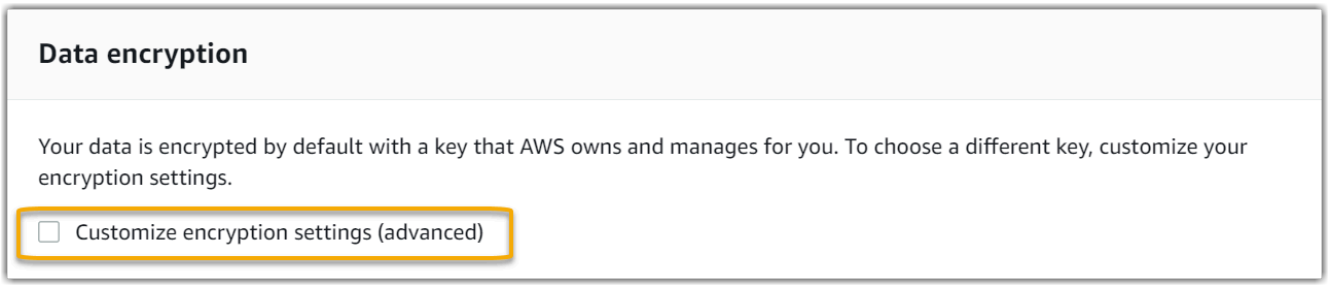
Audit Manager über die Konsole aktivieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Verwenden Sie zur Anmeldung die Daten Ihrer IAM-Identität.
3. Wählen Sie Set up (Festlegen) AWS Audit Manager.

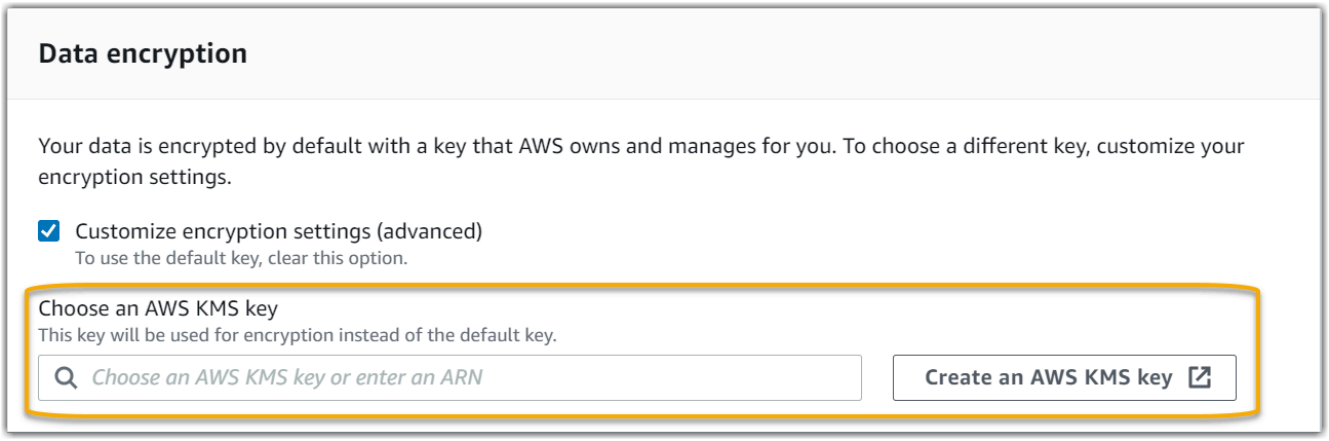
4. Unter Berechtigungen ist keine Aktion erforderlich. Grund dafür ist, dass Audit Manager eine serviceverknüpfte Rolle verwendet, um in Ihrem Namen eine Verbindung zu Datenquellen herzustellen. Sie können die serviceverknüpfte Rolle überprüfen, indem Sie die Berechtigung Serviceverknüpfte IAM-Rolle anzeigen wählen.



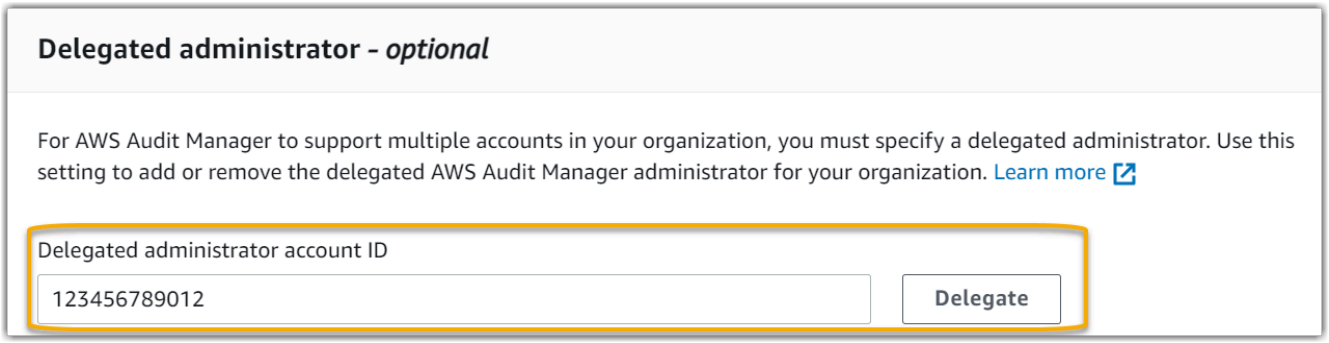
5. Unter Datenverschlüsselung ist die Standardoption, dass Audit Manager Ihre Daten erstellt und verwaltet und sicher speichert. AWS KMS key



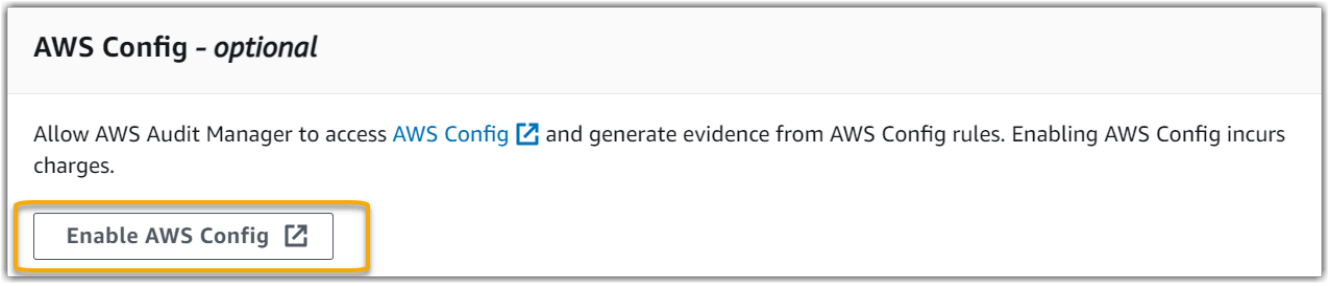
Wenn Sie Ihren eigenen, vom Kunden verwalteten Schlüssel verwenden möchten, um Daten in Audit Manager zu verschlüsseln, aktivieren Sie das Kontrollkästchen neben Verschlüsselung anpassen (erweitert). Sie können dann einen vorhandenen KMS-Schlüssel wählen oder einen neuen Schlüssel erstellen.



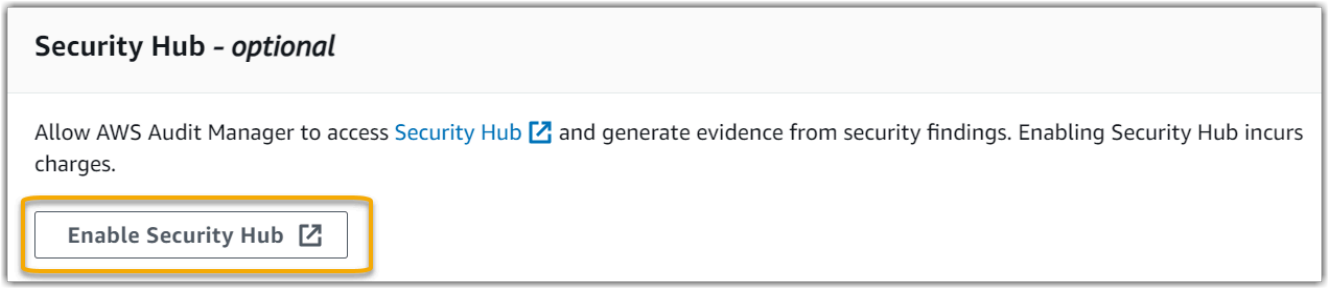
6. (Optional) Unter Delegierter Administrator – optional können Sie ein Konto für einen delegierten Administrator angeben, wenn Sie möchten, dass Audit Manager Bewertungen für mehrere Konten durchführt. Weitere Informationen und Empfehlungen finden Sie unter Aktivieren und einrichten AWS Organizations.



7. (Optional) Wir empfehlen Ihnen, die Option unter AWS Config — optional zu aktivieren, AWS Config um eine optimale Benutzererfahrung zu erzielen. Auf diese Weise kann Audit Manager mithilfe von AWS Config -Regeln Beweise generieren. Anweisungen und empfohlene Einstellungen finden Sie unterAktivieren und einrichten AWS Config.



8. (Optional) Unter Security Hub CSPM — optional empfehlen wir Ihnen, Security Hub CSPM zu aktivieren, um eine optimale Benutzererfahrung zu erzielen. Auf diese Weise kann Audit Manager mithilfe von Security Hub CSPM-Prüfungen Nachweise generieren. Anweisungen und empfohlene Einstellungen finden Sie unter. Aktivieren und einrichten AWS Security Hub CSPM



9. Wählen Sie Setup abschließen, um den Einrichtungsvorgang abzuschließen.

AWS CLI

Um Audit Manager mit dem zu aktivieren AWS CLI

Führen Sie in der Befehlszeile den Befehl register-account mit den folgenden Setup-Parametern aus:

- `--kms-key` (optional) – Verwenden Sie diesen Parameter, um Ihre Audit Manager-Daten mit Ihrem eigenen, vom Kunden verwalteten Schlüssel zu verschlüsseln. Wenn Sie hier keine Option angeben, erstellt und verwaltet Audit Manager AWS KMS key in Ihrem Namen für die sichere Speicherung Ihrer Daten.
- `--delegated-admin-account` (optional) – Verwenden Sie diesen Parameter, um das delegierte Administratorkonto Ihres Unternehmens für Audit Manager festzulegen. Wenn Sie hier keine Option angeben, wird kein delegierter Administrator registriert.

Eingabebeispiel (ersetzen Sie das *`placeholder text`* durch Ihre eigenen Informationen):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Ausgabebeispiel

```
{
    "status": "ACTIVE"
}
```

Weitere Informationen zu den Tools AWS CLI und Anweisungen zur Installation der AWS CLI Tools finden Sie im Folgenden im AWS Command Line Interface Benutzerhandbuch.

- Benutzerhandbuch für AWS Command Line
- Erste Schritte mit dem AWS Command Line Interface

Audit Manager API

Zur Aktivierung von Audit Manager über Audit Manager-API

Verwenden Sie den RegisterAccountVorgang mit den folgenden Setup-Parametern:

- kmsKey (optional) – Verwenden Sie diesen Parameter, um Ihre Audit Manager-Daten mit Ihrem eigenen, vom Kunden verwalteten Schlüssel zu verschlüsseln. Wenn Sie hier keine Option angeben, erstellt und verwaltet Audit Manager AWS KMS key in Ihrem Namen für die sichere Speicherung Ihrer Daten.
- delegatedAdminAccount(optional) — Verwenden Sie diesen Parameter, um das delegierte Administratorkonto Ihrer Organisation für Audit Manager anzugeben. Wenn Sie hier nichts angeben, wird kein delegierter Administrator registriert.

Eingabebeispiel (ersetzen Sie das *placeholder text* durch Ihre eigenen Informationen):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Ausgabebeispiel

```
{
  "status": "ACTIVE"
}
```

Nächste Schritte

Nachdem Sie Audit Manager aktiviert haben, empfehlen wir Ihnen, einige empfohlene Funktionen und Integrationen einzurichten, um ein optimales Erlebnis zu gewährleisten. Weitere Informationen finden Sie unter Aktivierung der empfohlenen Funktionen und für AWS-ServicesAWS Audit Manager.

Aktivierung der empfohlenen Funktionen und für AWS-ServicesAWS Audit Manager

Nach der Aktivierung ist es an der Zeit AWS Audit Manager, die empfohlenen Funktionen und Integrationen einzurichten, um den Service optimal nutzen zu können.

Wichtige Punkte

Für eine optimale Erfahrung mit Audit Manager empfehlen wir, dass Sie die folgenden AWS-Services-Funktionen berücksichtigen und aktivieren.

Aufgaben

- Empfohlene Audit Manager-Setup-Einstellungen
- Richten Sie empfohlene Integrationen mit anderen ein AWS-Services
  - Aktivieren und einrichten AWS Config
  - Aktivieren und einrichten AWS Security Hub CSPM
  - Aktivieren und einrichten AWS Organizations

Empfohlene Audit Manager-Setup-Einstellungen

Nachdem Sie Audit Manager aktiviert haben, empfehlen wir, die Beweissuche zu aktivieren.

Beweissuche bietet eine leistungsstarke Methode zur Suche nach Beweisen in Audit Manager. Anstatt tief verschachtelte Beweisordner zu durchsuchen, um das Gesuchte zu finden, können Sie die Beweissuche verwenden, um Ihre Beweise schnell abzufragen. Wenn Sie ein delegierter Administrator für Audit Manager sind, aktivieren Sie die Beweissuche, um nach Beweisen für alle Mitgliedskonten in Ihrem Unternehmen zu suchen.

Mithilfe einer Kombination aus Filtern und Gruppierungen können Sie den Umfang Ihrer Suchabfrage schrittweise einschränken. Wenn Sie sich beispielsweise einen umfassenden Überblick über den Zustand Ihres Systems verschaffen möchten, führen Sie eine umfassende Suche durch und filtern Sie nach Bewertung, Datumsbereich und Ressourcen-Compliance. Wenn Sie eine bestimmte Ressource korrigieren wollen, können Sie eine eingeschränkte Suche durchführen, um gezielt nach Beweisen für eine bestimmte Kontrollelement- oder Ressourcen-ID zu suchen. Nachdem Sie Ihre Filter definiert haben, können Sie die entsprechenden Suchergebnisse gruppieren und anschließend per Vorschau anzeigen, bevor Sie einen Bewertungsbericht erstellen.

Richten Sie empfohlene Integrationen mit anderen ein AWS-Services

Für ein optimales Erlebnis in Audit Manager empfehlen wir Ihnen dringend, Folgendes zu aktivieren AWS-Services:

- AWS Organizations– Sie können Organizations verwenden, um Audit Manager-Bewertungen für mehrere Konten durchzuführen und Beweise in einem delegierten Administratorkonto zu konsolidieren.
- AWS Security Hub CSPMund AWS Config— Audit Manager stützt sich auf diese AWS-Services als Datenquellen für die Beweiserhebung. Wenn Sie Security Hub CSPM aktivieren AWS Config , kann Audit Manager den vollen Funktionsumfang nutzen, umfassende Nachweise sammeln und die Ergebnisse der Konformitätsprüfungen direkt von diesen Services aus präzise Berichte erstellen.

Important

Wenn Sie Security Hub CSPM nicht aktivieren AWS Config und konfigurieren, können Sie in Ihren Audit Manager Manager-Bewertungen nicht die beabsichtigten Nachweise für viele Kontrollen sammeln. Infolgedessen riskieren Sie, dass die Beweiserhebung für bestimmte Kontrollen unvollständig oder fehlschlägt. Genauer gesagt:

- Wenn Audit Manager versucht, die Daten AWS Config als Kontrolldatenquelle zu verwenden, aber die erforderlichen AWS Config Regeln nicht aktiviert sind, werden keine Nachweise für diese Kontrollen gesammelt.
- Wenn Audit Manager versucht, Security Hub CSPM als Kontrolldatenquelle zu verwenden, aber die erforderlichen Standards in Security Hub CSPM nicht aktiviert sind, werden auch keine Beweise für diese Kontrollen gesammelt.

Um diese Risiken zu minimieren und eine umfassende Beweiserhebung sicherzustellen, folgen Sie den Schritten auf dieser Seite, um Security Hub CSPM zu aktivieren AWS Config und zu konfigurieren, bevor Sie Ihre Audit Manager Manager-Bewertungen erstellen.

Aktivieren und einrichten AWS Config

Für viele Steuerelemente in Audit Manager ist ein Datenquellentyp erforderlich AWS Config . Um diese Kontrollen zu unterstützen, müssen Sie sie für alle Konten in allen Konten aktivieren AWS Config , in AWS-Region denen Audit Manager aktiviert ist.

Audit Manager verwaltet nicht AWS Config für Sie. Sie können die folgenden Schritte ausführen, um AWS Config zu aktivieren und die Einstellungen zu konfigurieren.

> **Important**
>
> AWS Config Die Aktivierung ist eine optionale Empfehlung. Wenn Sie es jedoch AWS Config aktivieren, sind die folgenden Einstellungen erforderlich. Wenn Audit Manager versucht, Nachweise für Kontrollen zu sammeln, die AWS Config als Datenquellentyp verwendet werden, und AWS Config nicht wie unten beschrieben eingerichtet ist, werden keine Nachweise für diese Kontrollen gesammelt.

Aufgaben zur Integration AWS Config mit Audit Manager

- Schritt 1: Aktivieren AWS Config
- Schritt 2: Konfigurieren Sie Ihre AWS Config Einstellungen für die Verwendung mit Audit Manager

Schritt 1: Aktivieren AWS Config

Sie können die Aktivierung AWS Config über die AWS Config Konsole oder die API vornehmen. Anweisungen dazu finden Sie unter Getting Started mit AWS Config im AWS Config Developer Guide.

Schritt 2: Konfigurieren Sie Ihre AWS Config Einstellungen für die Verwendung mit Audit Manager

Stellen Sie nach der Aktivierung sicher AWS Config, dass Sie auch AWS Config Regeln aktivieren oder ein Konformitätspaket für den Compliance-Standard bereitstellen, der sich auf Ihr Audit bezieht. Dieser Schritt stellt sicher, dass Audit Manager die Ergebnisse für die von Ihnen aktivierten AWS Config -Regeln importieren kann.

Nachdem Sie eine AWS Config Regel aktiviert haben, empfehlen wir Ihnen, die Parameter dieser Regel zu überprüfen. Anschließend sollten Sie diese Parameter anhand der Anforderungen des von Ihnen ausgewählten Compliance-Frameworks validieren. Bei Bedarf können Sie die Parameter einer Regel in AWS Config aktualisieren, damit sie den Framework-Anforderungen entsprechen. So können Sie sicherstellen, dass bei Ihren Bewertungen die richtigen Beweise für die Konformitätsprüfung für ein bestimmtes Framework gesammelt werden.

Nehmen wir beispielsweise an, Sie erstellen eine Bewertung für CIS v1.2.0. Dieses Framework hat ein Kontrollelement namens 1.4 – Stellen Sie sicher, dass die Zugriffsschlüssel alle 90 Tage oder weniger gewechselt werden. AWS Config In hat die access-keys-rotatedRegel einen `maxAccessKeyAge` Parameter mit einem Standardwert von 90 Tagen. Dadurch stimmt die Regel mit

den Kontrollanforderungen überein. Wenn Sie nicht den Standardwert verwenden, stellen Sie sicher, dass der von Ihnen verwendete Wert den Anforderungen durch CIS v1.2.0 von 90 Tagen entspricht oder diese überschreitet.

Die Standard-Parameterdetails für jede verwaltete Regel finden Sie in der AWS Config - Dokumentation. Anweisungen zur Konfiguration einer Regel finden Sie unter Arbeiten mit AWS Config verwalteten Regeln.

Aktivieren und einrichten AWS Security Hub CSPM

Viele Steuerelemente in Audit Manager erfordern Security Hub CSPM als Datenquellentyp. Um diese Kontrollen zu unterstützen, müssen Sie Security Hub CSPM für alle Konten in jeder Region aktivieren, in der Audit Manager aktiviert ist.

Audit Manager verwaltet Security Hub CSPM nicht für Sie. Gehen Sie wie folgt vor, um Security Hub CSPM zu aktivieren und die Einstellungen zu konfigurieren.

> **Important**
>
> Die Aktivierung von Security Hub CSPM ist eine optionale Empfehlung. Wenn Sie Security Hub CSPM jedoch aktivieren, sind die folgenden Einstellungen erforderlich. Wenn Audit Manager versucht, Nachweise für Kontrollen zu sammeln, die Security Hub CSPM als Datenquellentyp verwenden, und Security Hub CSPM nicht wie unten beschrieben eingerichtet ist, werden keine Beweise für diese Kontrollen gesammelt.

Aufgaben zur Integration AWS Security Hub CSPM mit Audit Manager

- Schritt 1: Aktivieren AWS Security Hub CSPM
- Schritt 2: Konfigurieren Sie Ihre Security Hub CSPM-Einstellungen für die Verwendung mit Audit Manager
- Schritt 3: Konfigurieren Sie die Organisationseinstellungen für Ihre Organisation

Schritt 1: Aktivieren AWS Security Hub CSPM

Sie können Security Hub CSPM entweder über die Konsole oder die API aktivieren. Eine genaue Anleitung finden Sie unter Setup von AWS Security Hub CSPM im AWS Security Hub CSPM - Benutzerhandbuch.

Schritt 2: Konfigurieren Sie Ihre Security Hub CSPM-Einstellungen für die Verwendung mit Audit Manager

Nachdem Sie Security Hub CSPM aktiviert haben, stellen Sie sicher, dass Sie auch Folgendes tun:

- Ressourcenaufzeichnung aktivieren AWS Config und konfigurieren — Security Hub CSPM verwendet servicebezogene AWS Config Regeln, um die meisten Sicherheitsprüfungen für Kontrollen durchzuführen. Um diese Kontrollen zu unterstützen, AWS Config muss es so aktiviert und konfiguriert sein, dass Ressourcen aufgezeichnet werden, die für die Kontrollen erforderlich sind, die Sie in den einzelnen aktivierten Standards aktiviert haben.
- Alle Sicherheitsstandards aktivieren — Dieser Schritt stellt sicher, dass Audit Manager Ergebnisse für alle unterstützten Compliance-Standards importieren kann.
- Aktivieren Sie die Einstellung für konsolidierte Kontrollergebnisse in Security Hub CSPM — Diese Einstellung ist standardmäßig aktiviert, wenn Sie Security Hub CSPM am oder nach dem 23. Februar 2023 aktivieren.

> **Note**
>
> Wenn Sie konsolidierte Ergebnisse aktivieren, generiert Security Hub CSPM für jede Sicherheitsüberprüfung ein einziges Ergebnis (auch wenn dieselbe Prüfung für mehrere Standards verwendet wird). Jeder Security Hub CSPM-Befund wird als eine einzige Ressourcenbewertung in Audit Manager gesammelt. Infolgedessen führen konsolidierte Ergebnisse zu einem Rückgang der Gesamtzahl der individuellen Ressourcenbewertungen, die Audit Manager für die Ergebnisse des Security Hub CSPM durchführt. Aus diesem Grund kann die Verwendung konsolidierter Ergebnisse häufig zu einer Senkung der Nutzungskosten Ihres Audit Manager führen. Weitere Informationen zur Verwendung von Security Hub CSPM als Datenquellentyp finden Sie unter. AWS Security Hub CSPM Steuerelemente, die unterstützt werden von AWS Audit Manager Weitere Informationen zu Preisen für Audit Manager finden Sie unter AWS Audit Manager Preise.

Schritt 3: Konfigurieren Sie die Organisationseinstellungen für Ihre Organisation

Wenn Sie Security Hub CSPM-Beweise für Ihre Mitgliedskonten verwenden AWS Organizations und von diesen sammeln möchten, müssen Sie auch die folgenden Schritte in Security Hub CSPM ausführen.

So richten Sie die Security Hub CSPM-Einstellungen Ihres Unternehmens ein

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Security Hub CSPM Konsole unter. https://console.aws.amazon.com/securityhub/
2. Benennen Sie mit Ihrem AWS Organizations Verwaltungskonto ein Konto als delegierten Administrator für Security Hub CSPM. Weitere Informationen finden Sie unter Benennen eines Security Hub CSPM-Administratorkontos im AWS Security Hub CSPM Benutzerhandbuch.

   > **Note**
   >
   > Stellen Sie sicher, dass das delegierte Administratorkonto, das Sie in Security Hub CSPM angeben, dasselbe ist, das Sie in Audit Manager verwenden.

3. Gehen Sie über Ihr delegiertes Organizations-Administratorkonto zu Einstellungen, Konten, wählen Sie alle Konten aus und fügen Sie sie dann als Mitglieder hinzu, indem Sie Automatische Registrierung auswählen. Weitere Informationen finden Sie unter Aktivieren von Mitgliedskonten Ihres Unternehmens im AWS Security Hub CSPM -Benutzerhandbuch.
4. AWS Config Für jedes Mitgliedskonto der Organisation aktivieren. Weitere Informationen finden Sie unter Aktivieren von Mitgliedskonten Ihres Unternehmens im AWS Security Hub CSPM -Benutzerhandbuch.
5. Aktivieren Sie den PCI DSS-Sicherheitsstandard für jedes Mitgliedskonto des Unternehmens. Der Benchmark-Standard der AWS CIS Foundations und der AWS Foundational Best Practices-Standard sind bereits standardmäßig aktiviert. Weitere Informationen finden Sie im AWS Security Hub CSPM -Benutzerhandbuch unter Aktivieren eines Sicherheitsstandards.

Aktivieren und einrichten AWS Organizations

Audit Manager unterstützt mehrere Konten durch Integration mit AWS Organizations. Audit Manager kann Bewertungen für mehrere Konten durchzuführen und Beweise in einem delegierten Administratorkonto konsolidieren. Der delegierte Administrator verfügt über Berechtigungen zum Erstellen und Verwalten von Audit Manager-Ressourcen mit dem Unternehmen als Vertrauenszone. Nur das Management-Konto kann einen delegierten Administrator festlegen.

> **Important**
>
> AWS Organizations Die Aktivierung ist eine optionale Empfehlung. Wenn Sie es jedoch aktivieren AWS Organizations, sind die folgenden Einstellungen erforderlich.

Aufgaben zur Integration AWS Organizations mit Audit Manager

- Schritt 1: Erstellen eines Unternehmens oder Beitritt
- Schritt 2: Aktivieren aller Features in Ihrem Unternehmen
- Schritt 3: Geben Sie einen delegierten Administrator für Audit Manager an

Schritt 1: Erstellen eines Unternehmens oder Beitritt

Wenn Sie AWS-Konto nicht Teil einer Organisation sind, können Sie eine Organisation erstellen oder einer Organisation beitreten. Entsprechende Anweisungen finden Sie unter Erstellen und Konfigurieren eines Unternehmens im AWS Organizations -Benutzerhandbuch.

Schritt 2: Aktivieren aller Features in Ihrem Unternehmen

Nun müssen Sie alle Features in Ihrem Unternehmen aktivieren. Weitere Informationen finden Sie unter Aktivieren aller Features in Ihrem Unternehmen im AWS Organizations -Benutzerhandbuch.

Schritt 3: Geben Sie einen delegierten Administrator für Audit Manager an

Wir empfehlen, dass Sie Audit Manager über ein Organizations-Verwaltungskonto aktivieren und dann einen delegierten Administrator bestimmen. Danach können Sie sich mit dem Konto des delegierten Administrators anmelden und Bewertungen ausführen. Als bewährte Methode empfehlen wir, dass Sie Bewertungen nur über das delegierte Administratorkonto und nicht über das Verwaltungskonto erstellen.

Informationen zum Hinzufügen oder Ändern eines delegierten Administrators nach der Aktivierung von Audit Manager finden Sie unter Hinzufügen eines delegierten Administrators undEinen delegierten Administrator ändern.

Nächste Schritte

Nachdem Sie Audit Manager mit den empfohlenen Einstellungen eingerichtet haben, können Sie mit der Nutzung des Dienstes beginnen.

- Informationen zu den ersten Tests finden Sie unterTutorial für Audit-Verantwortliche: Eine Bewertung erstellen.
- Informationen zum future Aktualisieren Ihrer Einstellungen finden Sie unterÜberprüfung und Konfiguration Ihrer AWS Audit Manager Einstellungen.

Erste Schritte mit AWS Audit Manager

In den step-by-step Tutorials in diesem Abschnitt erfahren Sie, wie Sie Aufgaben mithilfe von ausführen AWS Audit Manager.

Tip

Die folgenden Tutorials sind nach Zielgruppen kategorisiert. Wählen Sie das Tutorial, das für Sie geeignet ist, basierend auf Ihrer Rolle als Audit-Verantwortlicher oder Delegierter.

- Audit-Verantwortliche sind Audit Manager-Benutzer, die für die Erstellung und Verwaltung von Bewertungen verantwortlich sind. In der Geschäftswelt handelt es sich bei den Audit-Verantwortlichen in der Regel um Experten für Unternehmensführung, Risikomanagement und Compliance (Governance, Risk Management, and Compliance, GRC). Im Zusammenhang mit Audit Manager können Personen aus SecOps unseren DevOps Teams jedoch auch die Benutzerpersönlichkeit eines Audit-Inhabers annehmen. Audit-Verantwortliche können einen Fachexperten – auch Delegierte genannt – um Unterstützung bitten, um bestimmte Kontrollen zu überprüfen und Nachweise zu validieren. Audit-Verantwortliche müssen über die erforderlichen Berechtigungen verfügen, um eine Bewertung zu verwalten.
- Bei den Delegierten handelt es sich um Fachexperten mit spezialisiertem technischem oder geschäftlichem Fachwissen. Obwohl sie die Bewertungen von Audit Manager nicht besitzen oder verwalten, können sie dennoch zu ihnen beitragen. Delegierte unterstützen die Audit-Verantwortlichen bei Aufgaben wie der Validierung von Nachweisen für die Kontrollen, die in ihren Zuständigkeitsbereich fallen. Delegierte haben eingeschränkte Berechtigungen in Audit Manager. Das basiert auf der Tatsache, dass Audit-Verantwortliche bestimmte Kontrollsätze zur Überprüfung delegieren, aber keine ganzen Bewertungen.

Weitere Informationen zu diesen Personas und anderen Konzepten von Audit Manager finden Sie unter audit owner und delegate im AWS Audit Manager Konzepte und Terminologie verstehen Abschnitt dieses Handbuchs.
Weitere Informationen über die empfohlenen IAM-Berechtigungen für jeden Nutzertyp finden Sie unter Empfohlene Richtlinien für Benutzerrollen in AWS Audit Manager.

Tutorials für Audit Manager

Erstellen einer Bewertung

Zielgruppe:Audit-Verantwortliche

Überblick: Folgen Sie den step-by-step Anweisungen, um Ihr erstes Assessment zu erstellen und schnell loszulegen. In diesem Tutorial erfahren Sie, wie Sie mithilfe eines Standard-Frameworks eine Bewertung erstellen und mit der automatisierten Beweiserhebung beginnen können.

Einen Kontrollsatz prüfen

Zielgruppe: Delegierte

Überblick: Unterstützen Sie einen Audit-Verantwortlichen, indem Sie Nachweise für Kontrollen überprüfen, die in Ihren Zuständigkeitsbereich fallen. Erfahren Sie, wie Sie Kontrollgruppen und die zugehörigen Nachweise überprüfen, Kommentare hinzufügen, Beweise hochladen und den Status einer Kontrolle aktualisieren.

Tutorial für Audit-Verantwortliche: Eine Bewertung erstellen

Dieses Tutorial bietet eine Einführung in AWS Audit Manager. In diesem Tutorial erstellen Sie eine Bewertung mit demAWS Audit Manager Beispiel für ein Framework. Durch die Erstellung einer Bewertung starten Sie den laufenden Prozess der automatisierten Erfassung von Nachweisen für die Kontrollen in diesem Framework.

> **Note**
>
> AWS Audit Manager hilft beim Sammeln von Nachweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Rahmenbedingungen und Vorschriften relevant sind. Ihre Einhaltung wird jedoch nicht bewertet. Die auf diese Weise gesammelten Nachweise enthalten AWS Audit Manager daher möglicherweise nicht alle Informationen über Ihre AWS Nutzung, die für Audits erforderlich sind. AWS Audit Manager ist kein Ersatz für Rechtsbeistand oder Compliance-Experten.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, stellen Sie sicher, dass Sie die folgenden Bedingungen erfüllen:

- Sie haben alle Voraussetzungen erfüllt, die unter Einrichtung AWS Audit Manager mit den empfohlenen Einstellungen beschrieben sind. Sie müssen Ihr Gerät AWS-Konto und die AWS Audit Manager Konsole verwenden, um dieses Tutorial abzuschließen.
- Ihrer IAM-Identität werden die entsprechenden Berechtigungen zum Erstellen und Verwalten einer Bewertung in AWS Audit Manager erteilt. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.
- Sie sind mit der Terminologie und Funktionalität von Audit Manager vertraut. Eine allgemeine Übersicht finden Sie unter Was ist AWS Audit Manager? und AWS Audit Manager Konzepte und Terminologie verstehen.

Verfahren

Aufgaben

- Schritt 1: Bewertungsdetails festlegen
- Schritt 2: Geben Sie AWS-Konten den Umfang an
- Schritt 3: Geben Sie die Audit-Inhaber an
- Schritt 4: Überprüfen und Erstellen

Schritt 1: Bewertungsdetails festlegen

Wählen Sie im ersten Schritt ein Framework aus und geben Sie grundlegende Informationen für Ihre Bewertung an.

Um die Einzelheiten der Bewertung zu spezifizieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie Launch AWS Audit Manager (Starten) aus.
3. Wählen Sie im grünen Banner oben auf dem Bildschirm die Option Mit einem Framework beginnen aus.

4. Wählen Sie das gewünschte Framework aus, und wählen Sie dann Bewertung aus Framework erstellen. Verwenden Sie für dieses Tutorial das AWS Audit Manager Sample Framework.
5. Geben Sie unter Bewertungsname einen Namen für Ihre Bewertung ein.
6. (Optional) Geben Sie unter Beschreibung der Bewertung eine Beschreibung für Ihre Bewertung ein.
7. Wählen Sie unter Ziel für Bewertungsberichte den S3-Bucket aus, in dem Sie Ihre Bewertungsberichte speichern möchten.
8. Vergewissern Sie sich unter Frameworks, dass AWS Audit Manager Sample Framework ausgewählt ist.
9. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um Ihrer Bewertung ein Tag zuzuordnen. Sie können für jedes Tag einen Schlüssel und einen Wert angeben. Der Tag-Schlüssel ist obligatorisch und kann als Suchkriterium verwendet werden, wenn Sie nach dieser Bewertung suchen.
10. Wählen Sie Weiter aus.

Schritt 2: Geben Sie AWS-Konten den Umfang an

Geben Sie als Nächstes die AWS Konten an, die Sie in den Umfang Ihrer Bewertung einbeziehen möchten.

AWS Audit Manager integriert in AWS Organizations, sodass Sie eine Audit Manager Manager-Bewertung für mehrere Konten durchführen und Nachweise in einem delegierten Administratorkonto konsolidieren können. Informationen zur Aktivierung von Organizations in Audit Manager (falls Sie dies noch nicht getan haben) finden Sie in Aktivieren und einrichten AWS Organizations auf der Seite Einrichtung dieses Handbuchs.

> **Note**
>
> Audit Manager kann im Rahmen einer Bewertung bis zu 200 Konten unterstützen. Wenn Sie versuchen, mehr als 200 Konten einzubeziehen, schlägt die Erstellung der Bewertung fehl. Wenn Sie außerdem versuchen, über 250 eindeutige Konten für all Ihre Bewertungen hinzuzufügen, schlägt die Erstellung der Bewertung fehl.

Um die Konten im Geltungsbereich anzugeben

1. Wählen Sie unter AWS-Konten die Option aus AWS-Konten, die Sie in den Umfang Ihrer Bewertung einbeziehen möchten.
   - Wenn Sie Organizations in Audit Manager aktiviert haben, werden mehrere Konten aufgeführt.
   - Wenn Sie Organizations in Audit Manager nicht aktiviert haben, wird nur Ihr aktuelles Konto aufgeführt.
2. Wählen Sie Weiter aus.

Schritt 3: Geben Sie die Audit-Inhaber an

In diesem Schritt geben Sie die Audit-Verantwortlichen für Ihre Bewertung an. Auditverantwortliche sind die Personen an Ihrem Arbeitsplatz — in der Regel aus GRC oder DevOps Teams — SecOps, die für die Verwaltung der Prüfung durch den Audit Manager verantwortlich sind. Wir empfehlen ihnen, die Richtlinie zu verwenden. AWSAuditManagerAdministratorAccess

Um die Audit-Verantwortlichen anzugeben

1. Wählen Sie unter Audit-Verantwortliche die Audit-Verantwortlichen für Ihre Bewertung aus. Um weitere Prüfinhaber zu finden, verwenden Sie die Suchleiste, um nach Namen oder zu suchen AWS-Konto.
2. Wählen Sie Weiter aus.

Schritt 4: Überprüfen und Erstellen

Überprüfen Sie die Informationen für Ihre Bewertung. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten. Wenn Sie fertig sind, wählen Sie Bewertung erstellen aus, um mit der fortlaufenden Erfassung von Nachweisen zu beginnen.

Nachdem Sie eine Bewertung erstellt haben, wird die Beweiserhebung fortgesetzt, bis Sie den Bewertungsstatus auf inaktiv ändern. Alternativ können Sie die Erfassung von Beweisen für eine bestimmte Kontrolle beenden, indem Sie den Kontrollstatus auf inaktiv ändern.

> **Note**
>
> Automatisierte Nachweise sind 24 Stunden nach der Erstellung der Bewertung verfügbar. Audit Manager sammelt automatisch Beweise aus mehreren Datenquellen, und die Häufigkeit dieser Beweiserhebung hängt von der Art der Beweise ab. Weitere Informationen finden Sie unter Häufigkeit der Beweissuche in diesem Handbuch.

Weitere Ressourcen

Wir empfehlen Ihnen, sich weiter mit den Konzepten und Tools vertraut zu machen, die in diesem Tutorial vorgestellt werden. Lesen Sie dazu die folgenden Ressourcen durch:

- Überprüfung der Bewertungsdetails in AWS Audit Manager— Führt Sie zur Seite mit den Bewertungsdetails ein, auf der Sie die verschiedenen Komponenten Ihrer Bewertung untersuchen können.
- Verwaltung von Bewertungen in AWS Audit Manager– Baut auf diesem Tutorial auf und enthält detaillierte Informationen über die Konzepte und Aufgaben für die Verwaltung einer Bewertung. In diesem Kapitel empfehlen wir Ihnen insbesondere, sich mit den folgenden Themen zu befassen:
  - Wie man eine Bewertung aus einem anderen Framework erstellt
  - Wie man die in einer Bewertung enthaltenen Nachweise überprüft und einen Bewertungsbericht erstellt
  - Wie man den Status einer Bewertung ändert oder eine Bewertung löscht
- Verwendung der Framework-Bibliothek zur Verwaltung von Frameworks in AWS Audit Manager– Stellt die Framework-Bibliothek vor und erklärt, wie Sie ein benutzerdefiniertes Framework für Ihre eigenen spezifischen Compliance-Anforderungen erstellen können.
- Verwenden der Steuerbibliothek zur Verwaltung von Steuerelementen in AWS Audit Manager– Stellt die Kontrollbibliothek vor und erklärt, wie Sie ein benutzerdefiniertes Steuerelement für die Verwendung in Ihrem benutzerdefinierten Framework erstellen.
- AWS Audit Manager Konzepte und Terminologie verstehen– Enthält Definitionen für die in Audit Manager verwendeten Konzepte und Terminologie.
- [Video] Nachweise sammeln und Prüfungsdaten verwalten mithilfe AWS Audit Manager — Zeigt den in diesem Tutorial beschriebenen Prozess zur Erstellung von Bewertungen sowie weitere Aufgaben wie die Überprüfung einer Kontrolle und die Erstellung eines Bewertungsberichts.

Tutorial für Delegierte: Überprüfung eines Kontrollsatzes

In diesem Tutorial wird beschrieben, wie Sie einen Kontrollsatz überprüfen, der Ihnen von einem Audit-Inhaber in AWS Audit Manager zur Verfügung gestellt wurde.

Auditverantwortliche verwenden Audit Manager, um Bewertungen zu erstellen und Nachweise für die Kontrollen in dieser Bewertung zu sammeln. Manchmal haben Audit-Verantwortliche Fragen oder benötigen Unterstützung bei der Validierung der Nachweise für einen Kontrollsatz. In diesem Fall kann ein Audit-Verantwortlicher einen Kontrollsatz zur Überprüfung an einen Fachexperten delegieren.

Als Delegierter können Sie Audit-Verantwortlichen dabei helfen, die gesammelten Nachweise für die Kontrollen zu überprüfen, die in ihren Zuständigkeitsbereich fallen.

Voraussetzungen

Stellen Sie vor Beginn dieses Tutorial sicher, dass folgenden Bedingungen erfüllt sind:

- Ihr AWS-Konto ist eingerichtet. Um dieses Tutorial abzuschließen, müssen Sie sowohl Ihre AWS-Konto als auch die Audit Manager Manager-Konsole verwenden. Weitere Informationen finden Sie unter Einrichtung AWS Audit Manager mit den empfohlenen Einstellungen.
- Sie sind mit der Terminologie und Funktionalität von Audit Manager vertraut. Einen allgemeinen Überblick über Audit Manager finden Sie unter Was ist AWS Audit Manager? und AWS Audit Manager Konzepte und Terminologie verstehen.

Verfahren

Aufgaben

- Schritt 1: Überprüfen Sie Ihre Benachrichtigungen
- Schritt 2: Überprüfen Sie einen Kontrollsatz und die zugehörigen Nachweise
- Schritt 3. Manuelle Nachweise hinzufügen (optional)
- Schritt 4. Einen optionalen Kommentar hinzufügen (optional)
- Schritt 5: Markieren Sie eine Kontrolle als überprüft (optional)
- Schritt 6: Rückgabe des überprüften Kontrollsatzes an den Audit-Verantwortlichen

Schritt 1: Überprüfen Sie Ihre Benachrichtigungen

Melden Sie sich zunächst bei Audit Manager an, wo Sie auf Ihre Benachrichtigungen zugreifen können, um die Kontrollsätze zu sehen, die Ihnen zur Überprüfung delegiert wurden.

Um Ihre Benachrichtigungen zu überprüfen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen.
3. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze an, die Ihnen zur Prüfung delegiert wurden. Die Benachrichtigungs-Tabelle enthält die folgenden Informationen:

Name	Beschreibung
Date (Datum)	Das Datum, an dem der Kontrollsatz delegiert wurde.
Bewertung	Der Name der Bewertung, die dem Kontrollsatz zugeordnet ist. Sie können einen Bewertungsnamen wählen, um die Seite mit den Bewertungsdetails zu öffnen.
Kontrollsatz	Der Name des Kontrollsatzes, der zur Überprüfung an Sie delegiert wurde.
Quelle	Der Benutzer oder die Rolle, die den Kontrollsatz an Sie delegiert hat.
Beschreibung	Die Überprüfungsanweisungen, die vom Prüfungsverantwort lichen bereitgestellt wurden.

> **Tip**
>
> Sie können auch ein SNS-Thema abonnieren, um E-Mails zu erhalten, wenn ein Kontrollsatz zur Überprüfung an Sie vergeben wurde. Weitere Informationen finden Sie unter Benachrichtigungen in AWS Audit Manager.

Schritt 2: Überprüfen Sie einen Kontrollsatz und die zugehörigen Nachweise

Der nächste Schritt besteht darin, die Kontrollsätze zu überprüfen, die der Audit-Verantwortliche an Sie delegiert hat. Indem Sie die Kontrollen und die damit verbundenen Nachweise überprüfen, können Sie feststellen, ob zusätzliche Maßnahmen erforderlich sind. Zusätzliche Maßnahmen können das manuelle Hochladen zusätzlicher Nachweise zum Nachweis der Einhaltung der Vorschriften oder das Hinterlassen eines Kommentars zu dieser Kontrolle umfassen.

Um einen Kontrollsatz zu prüfen

1. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze an, die Ihnen zur Prüfung delegiert wurden. Geben Sie dann an, welche Sie überprüfen möchten, und wählen Sie den Namen der zugehörigen Bewertung.
2. Scrollen Sie auf der Seite mit den Bewertungsdetails auf der Registerkarte Kontrollen nach unten zur Tabelle Kontrollsätze.
3. Erweitern Sie in der Spalte Nach Kontrollsatz gruppierte Kontrollsätze den Namen eines Kontrollsatzes, um dessen Steuerelemente anzuzeigen. Wählen Sie dann den Namen einer Kontrolle, um die Kontrolldetailseite zu öffnen.
4. (Optional) Wählen Sie Kontrollstatus aktualisieren, um den Status der Kontrolle zu ändern. Während Ihre Überprüfung in Bearbeitung ist, können Sie den Status als Wird geprüft markieren.
5. Informationen zum Steuerelement finden Sie in den Ordnern „Nachweise“, „Details“, „Nachweisquellen“, „Kommentare“ und „Changelog“. Weitere Informationen zu den einzelnen Registerkarten und zum besseren Verständnis der darin enthaltenen Daten finden Sie unter Überprüfung einer Bewertungskontrolle in AWS Audit Manager.

So überprüfen Sie die Nachweise für eine Kontrolle

1. Wählen Sie auf der Kontrollseite die Registerkarte Beweisordner aus.
2. Navigieren Sie zur Tabelle Beweisordner, wo eine Liste der Ordner angezeigt wird, die Nachweise für diese Kontrolle enthalten. Diese Ordner sind auf der Grundlage des Datums angeordnet und benannt, an dem die Nachweise im Ordner gesammelt wurden.
3. Wählen Sie den Namen eines Beweisordners, um ihn zu öffnen. Hier sehen Sie dann eine Zusammenfassung aller an diesem Datum gesammelten Nachweise. Weitere Informationen zu diesen Informationen finden Sie unter Überprüfung eines Beweisordners in AWS Audit Manager.
4. Navigieren Sie auf der Übersichtsseite der Beweisordner zur Tabelle Nachweise. Wählen Sie in der Spalte Zeit eine Zeile aus, um die Details der Nachweise, die zu diesem Zeitpunkt

gesammelt wurden, zu öffnen und zu überprüfen. Weitere Informationen zu diesen Informationen finden Sie unterÜberprüfung von Nachweisen in AWS Audit Manager.

Schritt 3. Manuelle Nachweise hinzufügen (optional)

Sammelt zwar AWS Audit Manager automatisch Beweise für viele Kontrollen, in einigen Fällen müssen Sie jedoch möglicherweise zusätzliche Nachweise vorlegen. In diesen Fällen können Sie manuell Ihre eigenen Nachweise hinzufügen, anhand derer Sie die Einhaltung dieser Kontrollen nachweisen können.

Um einer Kontrolle manuelle Nachweise hinzuzufügen

Es gibt mehrere Möglichkeiten, einer Kontrolle manuelle Nachweise hinzuzufügen. Sie können eine Datei aus Amazon S3 importieren, eine Datei aus Ihrem Browser hochladen oder eine Textantwort eingeben. Anweisungen für die einzelnen Methoden finden Sie unterManuelle Nachweise hinzufügen in AWS Audit Manager.

Schritt 4. Einen optionalen Kommentar hinzufügen (optional)

Sie können Kommentare zu allen Kontrollelementen hinzufügen, die Sie überprüfen. Diese Kommentare sind für den Audit-Verantwortlichen sichtbar. Sie können beispielsweise einen Kommentar hinterlassen, um den Status zu aktualisieren und zu bestätigen, dass Sie alle Probleme mit dieser Kontrolle behoben haben.

Um einen Kommentar zu einem Kontrollelement hinzufügen

1. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze an, die Ihnen zur Prüfung delegiert wurden. Suchen Sie nach dem Kontrollsatz, für den Sie einen Kommentar hinterlassen möchten, und wählen Sie den Namen der zugehörigen Bewertung.
2. Wählen Sie die Registerkarte Kontrolle, scrollen Sie nach unten zu Kontrollsätze, und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.
3. Wählen Sie die Registerkarte Kommentare.
4. Geben Sie unter Kommentare senden Ihren Kommentar in das Textfeld ein.
5. Wählen Sie Kommentare einreichen, um Ihren Kommentar hinzuzufügen. Ihr Kommentar wird nun zusammen mit allen anderen Kommentaren zu diesem Steuerelement im Bereich Frühere Kommentare der Seite angezeigt.

Schritt 5: Markieren Sie eine Kontrolle als überprüft (optional)

Das Ändern des Status einer Kontrolle ist optional. Wir empfehlen jedoch, dass Sie den Status jeder Kontrolle auf Überprüft ändern, wenn Sie Ihre Überprüfung für diese Kontrolle abgeschlossen haben. Unabhängig vom Status der einzelnen Kontrollen können Sie die Kontrollen dennoch an den Audit-Verantwortlichen weiterleiten.

Um eine Kontrolle als überprüft zu markieren

1. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze an, die Ihnen zur Prüfung delegiert wurden. Suchen Sie den Kontrollsatz, der die Kontrolle enthält, die Sie als überprüft markieren möchten. Wählen Sie dann den Namen der zugehörigen Bewertung aus, um die Seite mit den Bewertungsdetails zu öffnen.
2. Scrollen Sie auf der Seite mit den Bewertungsdetails auf der Registerkarte Kontrollen nach unten zur Tabelle Kontrollsätze.
3. Erweitern Sie in der Spalte Nach Kontrollsatz gruppierte Kontrollsätze den Namen eines Kontrollsatzes, um dessen Steuerelemente anzuzeigen. Wählen Sie den Namen einer Kontrolle, um die Kontrolldetailseite zu öffnen.
4. Wählen Sie Kontrollstatus aktualisieren und ändern Sie den Status zu Überprüft.
5. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option Kontrollstatus aktualisieren, um zu bestätigen, dass Sie die Überprüfung der Kontrolle abgeschlossen haben.

Schritt 6: Rückgabe des überprüften Kontrollsatzes an den Audit-Verantwortlichen

Wenn Sie mit der Überprüfung aller Kontrollen fertig sind, senden Sie den Kontrollsatz zurück an den Audit-Verantwortlichen, damit dieser weiß, dass Sie Ihre Prüfung abgeschlossen haben.

Um einen überprüften Kontrollsatz an den Audit-Verantwortlichen zurückzugeben

1. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze, die Ihnen zur Prüfung übergeben wurden. Suchen Sie nach dem Kontrollsatz, den Sie dem Audit-Verantwortlichen senden möchten, und wählen Sie den Namen der zugehörigen Bewertung.
2. Scrollen Sie nach unten zur Tabelle Kontrollsätze, wählen Sie den Kontrollsatz aus, den Sie an den Audit-Verantwortlichen zurücksenden möchten, und wählen Sie dann Zur Prüfung einreichen aus.
3. In dem daraufhin angezeigten Popup-Fenster können Sie allgemeine High-Level-Kommentare zu diesem Kontrollsatz hinzufügen, bevor Sie Zur Überprüfung einreichen wählen.

Nachdem Sie die Kontrolle an den Audit-Verantwortlichen übermittelt haben, kann dieser alle Kommentare einsehen, die Sie für ihn hinterlassen haben.

Weitere Ressourcen

Sie können sich weiter mit dem Wissen über die Konzepte und Tools vertraut machen, die in diesem Tutorial vorgestellt werden. Hier sind einige empfohlene Ressourcen:

- Überprüfung der Bewertungsdetails in AWS Audit Manager- Führt Sie zur Seite mit den Bewertungsdetails ein, auf der Sie sich mit den verschiedenen Komponenten einer Audit Manager-Bewertung vertraut machen können.
- Überprüfung einer Bewertungskontrolle in AWS Audit Managerund Überprüfung von Nachweisen in AWS Audit Manager — Enthält Definitionen, die Ihnen helfen, die Kontrollen und Nachweise einer Bewertung zu verstehen.
- AWS Audit Manager Konzepte und Terminologie verstehen – Enthält Definitionen für die in Audit Manager verwendeten Konzepte und Terminologie.

Verwenden des Audit Manager-Dashboards

Mit dem Audit Manager-Dashboard können Sie Beweise für Verstöße in Ihren aktiven Bewertungen visualisieren. Es ist eine bequeme und schnelle Möglichkeit, Ihre Bewertungen zu überwachen, auf dem Laufenden zu bleiben und Probleme proaktiv anzugehen. Standardmäßig bietet das Dashboard eine aggregierte Top-Down-Ansicht all Ihrer aktiven Bewertungen. Mithilfe dieser Ansicht können Sie Probleme in Ihren Bewertungen visuell identifizieren, ohne große Mengen an Einzelbeweisen durchsuchen zu müssen.

Das Dashboard ist der erste Bildschirm, den Sie sehen, wenn Sie sich bei der Audit-Manager-Konsole anmelden. Es enthält zwei Widgets, die die Daten und wichtigen Leistungsindikatoren (KPIs) anzeigen, die für Sie am relevantesten sind. Mithilfe eines Bewertungsfilters können Sie diese Daten so verfeinern, dass sie sich auf die KPIs für eine bestimmte Bewertung eignen. Von dort aus können Sie die Gruppierungen der Kontrolldomänen überprüfen, um festzustellen, bei welchen Kontrollelementen die meisten nicht konformen Beweise existieren. Anschließend können Sie die zugrunde liegenden Kontrollelemente untersuchen, um Probleme zu untersuchen und zu beheben.

> **Note**
>
> Wenn Sie Audit Manager zum ersten Mal verwenden oder keine aktiven Bewertungen haben, werden im Dashboard keine Daten angezeigt. Um loszulegen, erstellen Sie eine Bewertung. Damit wird die fortlaufende Erfassung von Beweisen gestartet. Nach 24 Stunden werden aggregierte Beweisdaten im Dashboard angezeigt. In den folgenden Abschnitten erfahren Sie, wie Sie diese Daten verstehen und interpretieren können.

Diese Seite deckt die folgenden Themen ab:

Topics

Dashboard-Konzepte und Terminologie

In diesem Abschnitt werden wichtige Dinge behandelt, die Sie zum Audit Manager-Dashboard wissen sollten, bevor Sie es verwenden.

Berechtigungen und Sichtbarkeit

Sowohl Audit-Verantwortliche als auch Delegierte haben Zugriff auf das Dashboard. Das bedeutet, dass diese beiden Personas die Kennzahlen und Aggregate für alle aktiven Bewertungen in Ihrem sehen können. AWS-Konto Durch den Zugriff auf dieselben Informationen kann sich Ihr gesamtes Team auf dieselben KPIs Ziele konzentrieren.

Filter

Audit Manager bietet eine Seitenebene the section called “Bewertungsfilter”, die Sie auf alle Widgets in Ihrem Dashboard anwenden können.

Beweise für Nonkonformitäten

Das Dashboard markiert die Kontrollelemente in Ihren Bewertungen, bei denen die Compliance-Überprüfung zu einem nicht konformen Ergebnis geführt hat. Der Nachweis der Konformitätsprüfung bezieht sich auf Kontrollen, die AWS Config oder AWS Security Hub CSPM als Datenquellentyp verwenden. Für diese Art von Beweisen meldet Audit Manager das Ergebnis einer Compliance-Überprüfung direkt über diese Services. Wenn Security Hub CSPM ein Fehlerergebnis oder ein nicht konformes Ergebnis AWS Config meldet, stuft Audit Manager die Beweise als nicht konform ein.

Unklare Beweise

Beweise sind unklar, wenn keine Compliance-Überprüfung verfügbar oder anwendbar ist. Daher kann keine Bewertung der Konformität vorgenommen werden. Dies ist der Fall, wenn ein Steuerelement AWS Config oder AWS Security Hub CSPM als Datenquellentyp verwendet, Sie diese Dienste jedoch nicht aktiviert haben. Dies ist auch der Fall, wenn das Steuerelement einen Datenquellentyp verwendet, der keine Konformitätsprüfungen unterstützt, z. B. manuelle Nachweise, AWS API-Aufrufe oder AWS CloudTrail. In der Konsole werden Nachweise mit dem Konformitätsprüfungsstatus „Nicht zutreffend“ im Dashboard als nicht eindeutig eingestuft.

Sie können die nicht schlüssigen Nachweise verwenden, um die Konformität einer Kontrolle manuell zu bewerten.

> **Note**
>
> Unschlüssige Beweise deuten nicht auf ein Versagen hin, sondern signalisieren, dass Sie die Nachweise manuell auf ihre Einhaltung hin auswerten sollten.

Konforme Beweise

Der Beweis gilt als konform, wenn bei einer Compliance-Überprüfung keine Probleme festgestellt wurden. Dies ist der Fall, wenn Security Hub CSPM ein Pass-Ergebnis oder ein Compliance-Ergebnis AWS Config meldet.

Kontrolldomänen

Das Dashboard führt das Konzept einer Kontrolldomäne ein. Sie können sich eine Kontrolldomäne als eine allgemeine Kategorie von Kontrollen vorstellen, die nicht spezifisch für ein bestimmtes Framework ist. Gruppierungen von Kontrolldomänen sind eine der leistungsstärksten Funktionen des Dashboards. Audit Manager hebt die Kontrollen in Ihren Bewertungen hervor, die nachweislich nicht konform sind, und gruppiert sie nach Kontrolldomänen. Auf diese Weise können Sie sich bei der Vorbereitung eines Audits auf bestimmte Themenbereiche konzentrieren.

> **Note**
>
> Eine Kontrolldomäne unterscheidet sich von einem Kontrollsatz. Ein Kontrollsatz ist eine framework-spezifische Gruppierung von Kontrollen, die in der Regel von einer Aufsichtsbehörde definiert wird. Das PCI-DSS-Framework verfügt beispielsweise über einen Kontrollsatz mit dem Namen Anforderung 8: Identifizieren und Authentifizieren des Zugriffs auf Systemkomponenten. Dieser Kontrollsatz fällt unter die Kontrolldomäne Identitäts- und Zugriffsmanagement.

Eventuelle Datenkonsistenz

Für die Dashboard-Daten gilt eine eventuelle Konsistenz. Dashboard-Daten geben also möglicherweise nicht sofort alle Ergebnisse eines kürzlich abgeschlossenen Schreib- oder Aktualisierungsvorgangs wieder. Wenn Sie innerhalb weniger Stunden erneut nachschauen, sollte das Dashboard die neuesten Daten enthalten.

Daten aus gelöschten und inaktiven Bewertungen

Das Dashboard zeigt Daten aus aktiven Bewertungen an. Wenn Sie am selben Tag, an dem Sie das Dashboard aufrufen, eine Bewertung löschen oder deren Status auf inaktiv ändern, werden diese Daten wie folgt berücksichtigt.

- Inaktive Bewertungen – Wenn Audit Manager Beweise für Ihre Bewertung erfasst hat, bevor Sie sie in inaktiv geändert haben, werden diese Beweisdaten für diesen Tag im Dashboard berücksichtigt.
- Gelöschte Bewertungen – Wenn Audit Manager Beweise für Ihre Bewertung erfasst hat, bevor Sie sie gelöscht haben, zählen diese Beweisdaten für diesen Tag nicht im Dashboard.

Dashboard-Elemente

In den folgenden Abschnitten werden die verschiedenen Komponenten des Dashboards behandelt.

Themen

Bewertungsfilter

Sie können den Bewertungsfilter verwenden, um nur bestimmte aktive Bewertung einzubeziehen.

Standardmäßig zeigt das Dashboard aggregierte Daten für alle Ihre aktiven Bewertungen an. Wenn Sie Daten für eine bestimmte Bewertung anzeigen möchten, können Sie einen Bewertungsfilter verwenden. Dies ist ein Filter auf Seitenebene, der für alle Widgets im Dashboard gilt.

Um einen Bewertungsfilter anzuwenden, wählen Sie eine Bewertung aus der Dropdown-Liste oben im Dashboard aus. In dieser Liste werden bis zu 10 Ihrer aktiven Bewertungen angezeigt. Zuletzt erstellte Bewertungen werden zuerst angezeigt. Wenn Sie über viele aktive Bewertungen verfügen, können Sie mit der Eingabe des Namens einer Bewertung beginnen, um diese schnell zu finden. Nachdem Sie eine Bewertung ausgewählt haben, zeigt das Dashboard nur Daten für diese Bewertung an.

Tägliche Snapshots

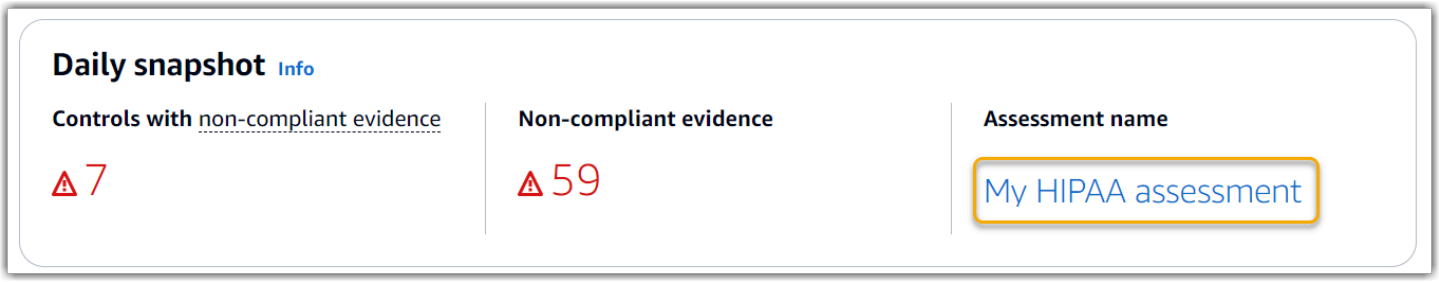
Dieses Widget zeigt eine Momentaufnahme des aktuellen Compliance-Status Ihrer aktiven Bewertungen.

Der tägliche Snapshot spiegelt die neuesten Daten wider, die am oben im Dashboard angezeigten Datum erfasst wurden. Datum und Uhrzeit im Dashboard entsprechen der Koordinierten Weltzeit (UTC) Beachten Sie, dass es sich bei diesen Zahlen um tägliche Zählungen handelt, die auf diesem Zeitstempel basieren. Sie zeigen keine Gesamtsumme zu einem bestimmten Datum.

Standardmäßig zeigt der tägliche Snapshot die folgenden Daten für all Ihre aktiven Bewertungen:

1. Kontrollelement mit nicht konformen Beweisen – Die Gesamtzahl der Kontrollelemente, die mit nicht konformen Beweisen verknüpft sind.
2. Nichtkonforme Nachweise — Die Gesamtmenge der Nachweise aus der Konformitätsprüfung, die zu dem Ergebnis geführt haben, dass sie nicht konform sind.
3. Aktive Bewertungen – Die Gesamtzahl Ihrer aktiven Bewertungen. Wählen Sie diese Zahl, um Links zu diesen Bewertungen zu sehen.

Die täglichen Snapshot-Daten ändern sich je nach the section called “Bewertungsfilter”, das Sie anwenden. Wenn Sie eine Bewertung spezifizieren, spiegeln die Daten nur die täglichen Zahlen für diese Bewertung wider. In diesem Fall zeigt der tägliche Snapshot den Namen der von Ihnen angegebenen Bewertung. Sie können den Namen der Bewertung wählen, um sie zu öffnen.

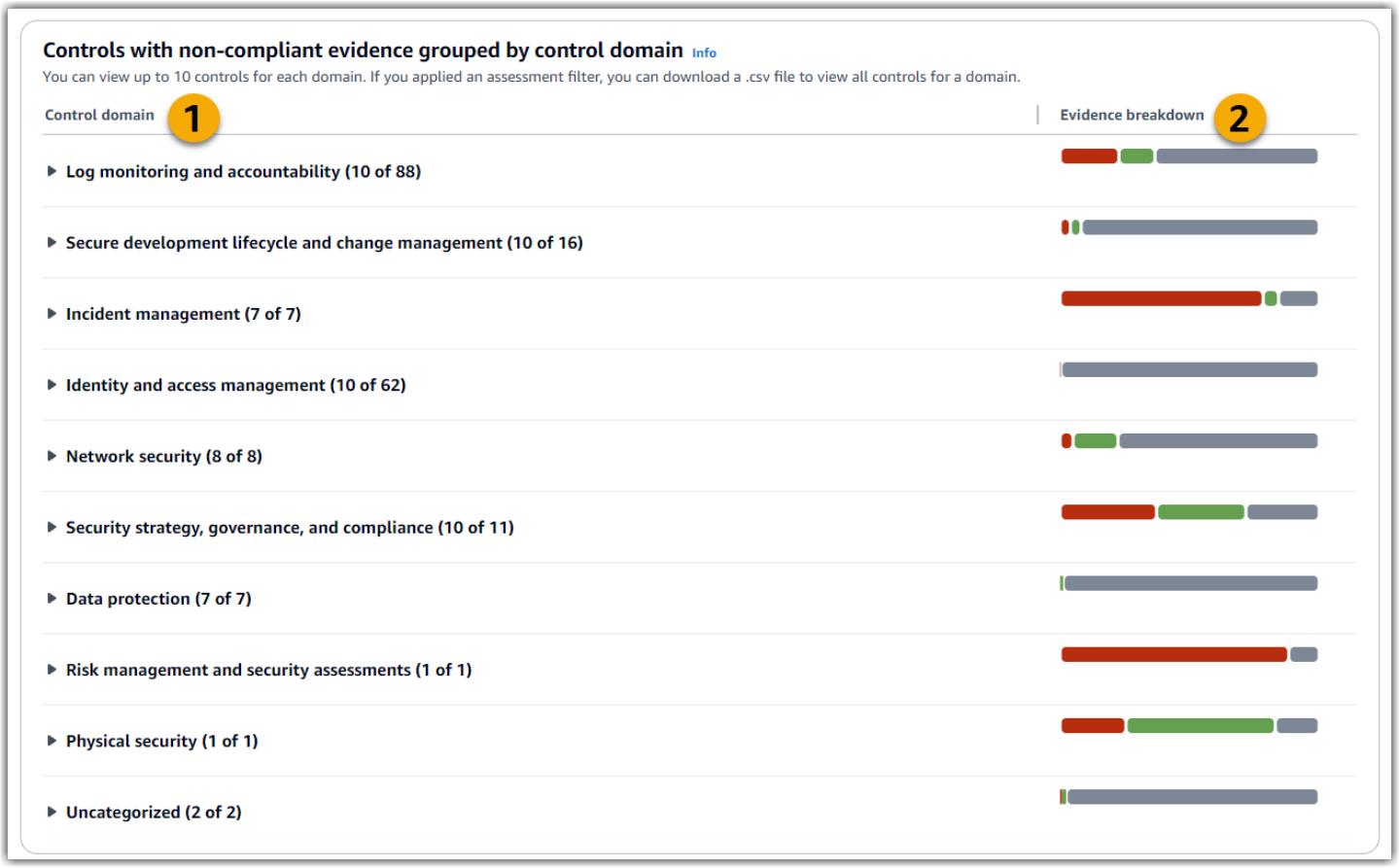


Kontrollelemente mit nicht konformen Beweisen, gruppiert nach Kontrolldomänen

Mithilfe dieses Widgets können Sie ermitteln, für welche Kontrollelemente die meisten nicht konformen Beweise vorliegen.

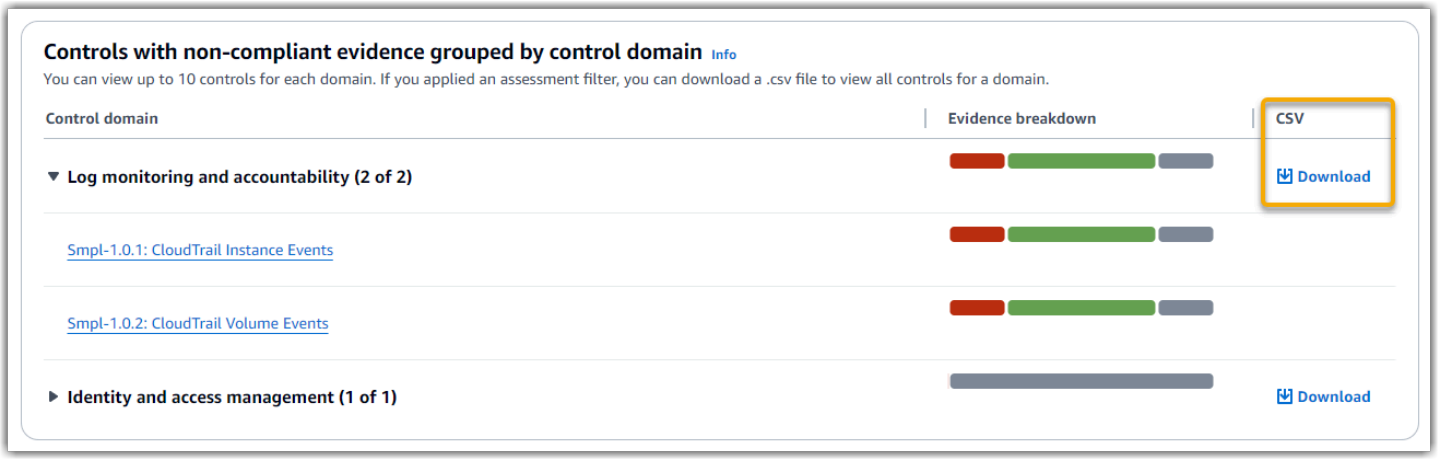
Standardmäßig zeigt das Widget die folgenden Daten für alle Ihre aktiven Bewertungen:

1. Kontrolldomäne – Eine Liste von control domains, die mit Ihren aktiven Bewertungen verknüpft sind.
2. Aufschlüsselung der Beweise – Ein Balkendiagramm, das eine Aufschlüsselung des Compliance-Status der Beweise zeigt.



Um eine Kontrolldomäne zu erweitern, wählen Sie den Pfeil neben dem Namen aus. Wenn die Konsole erweitert ist, werden bis zu 10 Kontrollelemente für jede Domain angezeigt. Diese Kontrollelemente werden nach der höchsten Gesamtzahl an nicht konformen Beweisen eingestuft.

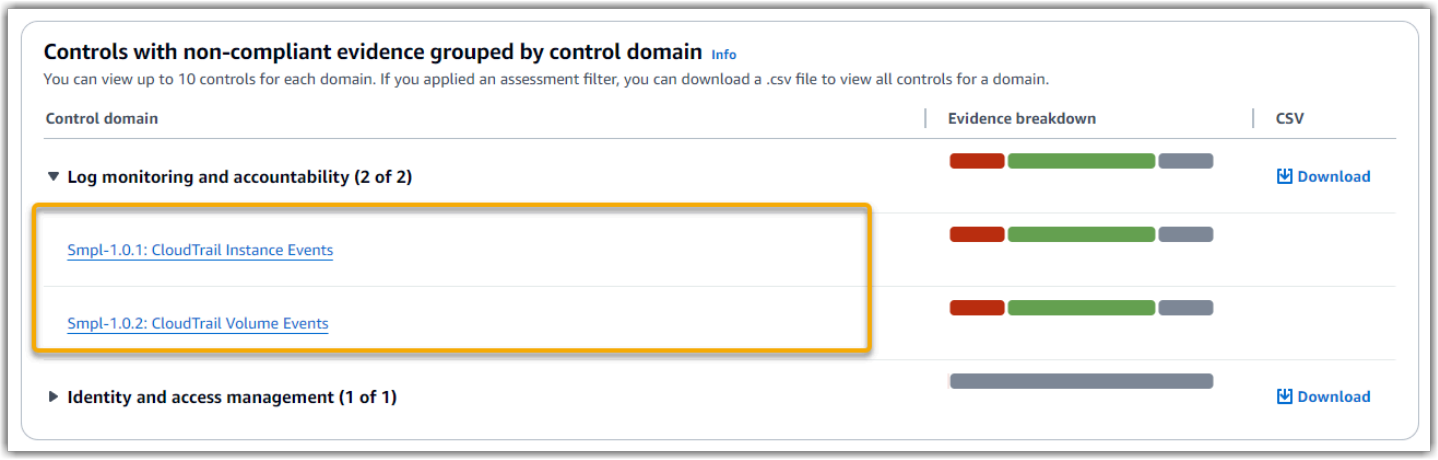
Die Daten in diesem Widget ändern sich je nach the section called “Bewertungsfilter”, das Sie anwenden. Wenn Sie eine Bewertung angeben, werden Ihnen nur Daten für diese Bewertung angezeigt. Darüber hinaus können Sie auch eine CSV-Datei für jede verfügbare Kontrolldomäne in der Bewertung herunterladen.



Die CSV-Datei enthält die vollständige Liste der Kontrollelemente in der Domäne, die mit nicht konformen Beweisen verknüpft sind. Das folgende Beispiel zeigt die CSV-Datenspalten mit fiktionalisierten Werten.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Wenn Sie schließlich einen Bewertungsfilter anwenden, werden die Name des Kontrollelements unter jeder Domäne mit einem Hyperlink versehen. Wählen Sie ein beliebiges Kontrollelement aus, um die Seite mit den Kontrolldetails in der angegebenen Bewertung zu öffnen.



> **Tip**
>
> Wenn Sie die Seite mit den Kontrolldetails als Startpunkt verwenden, können Sie von einer Detailebene zur nächsten wechseln.
>
> 1. Seite mit Kontrolldetails — Auf dieser Seite Registerkarte „Beweisordner“ werden die täglichen Ordner mit Nachweisen aufgeführt, die Audit Manager für diese Kontrolle gesammelt hat. Wählen Sie für weitere Informationen einen Ordner.
> 2. Ordner mit Nachweisen — Als Nächstes können Sie einen Übersicht der Beweismappe und eine Liste der Nachweise in diesem Ordner überprüfen. Für weitere Einzelheiten wählen Sie ein einzelnes Beweiselement aus.
> 3. Einzelbeweise – Schließlich können Sie die Einzelheiten zu einzelnen Beweisen untersuchen. Dies ist die detaillierteste Ebene der Beweisdaten.

Nächste Schritte

Hier sind einige der nächsten Schritte, die Sie nach der Überprüfung des Dashboards ergreifen können.

- Laden Sie eine CSV-Datei herunter — Suchen Sie den Bewertungs- und Kontrollbereich, auf den Sie sich konzentrieren möchten, und laden Sie die vollständige Liste der zugehörigen Kontrollen mit nicht konformen Nachweisen herunter.
- Kontrollelement überprüfen – Nachdem Sie ein Kontrollelement identifiziert haben, können Sie das Kontrollelement überprüfen.

- Ein Kontrollelement zur Überprüfung delegieren – Wenn Sie Hilfe bei der Überprüfung eines Kontrollelements benötigen, können Sie einen Kontrollsatz zur Überprüfung delegieren.
- Bearbeiten Ihrer Bewertung – Wenn Sie den Umfang einer aktiven Bewertung ändern möchten, können Sie die Bewertung bearbeiten.
- Aktualisieren Sie den Status Ihrer Bewertung — Wenn Sie das Sammeln von Nachweisen für eine Bewertung beenden möchten, können Sie den Bewertungsstatus auf inaktiv ändern.

Weitere Ressourcen

Antworten auf häufig gestellte Fragen und Probleme finden Sie Fehlerbehebung bei Dashboard-Problemen im Abschnitt zur Fehlerbehebung in diesem Handbuch.

Verwaltung von Bewertungen in AWS Audit Manager

Eine Bewertung durch den Audit Manager basiert auf einem Framework, bei dem es sich um eine Gruppierung von Kontrollen handelt. Wenn Sie ein Framework als Ausgangspunkt verwenden, können Sie eine Bewertung erstellen, in der Beweise für die Kontrollen in diesem Framework gesammelt werden. In Ihrer Bewertung können Sie auch den Umfang Ihrer Prüfung definieren. Dazu gehört auch AWS-Konten die Angabe der Beweise, für die Sie Beweise sammeln möchten.

Wichtige Punkte

Sie können eine Bewertung anhand eines beliebigen Frameworks erstellen. Sie können entweder ein Standard-Framework verwenden, das von Audit Manager bereitgestellt wird. Oder Sie können eine Bewertung anhand eines benutzerdefinierten Frameworks erstellen, das Sie selbst erstellt haben. Standard-Frameworks enthalten vorgefertigte Kontrollsätze, die einen bestimmten Compliance-Standard oder eine bestimmte Compliance-Verordnung unterstützen. Im Gegensatz dazu enthalten benutzerdefinierte Frameworks Steuerelemente, die Sie nach Ihren eigenen Anforderungen anpassen und gruppieren können.

Wenn Sie eine Bewertung erstellen, beginnt damit die fortlaufende Erfassung von Beweisen. Wenn es Zeit für ein Audit ist, können Sie oder ein Delegierter diese Nachweise überprüfen und sie dann einem Bewertungsbericht hinzufügen.

> **Note**
>
> AWS Audit Manager hilft beim Sammeln von Nachweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Standards und -Vorschriften relevant sind. Ihre Einhaltung wird jedoch nicht bewertet. Die auf diese Weise gesammelten Nachweise enthalten AWS Audit Manager daher möglicherweise nicht alle Informationen über Ihre AWS Nutzung, die für Audits erforderlich sind. AWS Audit Manager ist kein Ersatz für Rechtsbeistand oder Compliance-Experten.

Weitere Ressourcen

Um Bewertungen in Audit Manager zu erstellen und zu verwalten, folgen Sie den hier beschriebenen Verfahren.

Erstellen Sie eine Bewertung in AWS Audit Manager

Dieses Thema baut auf dem aufTutorial für Audit-Verantwortliche: Eine Bewertung erstellen. Auf dieser Seite finden Sie detaillierte Anweisungen, die Ihnen zeigen, wie Sie eine Bewertung anhand

eines Frameworks erstellen. Gehen Sie wie folgt vor, um eine Bewertung zu erstellen und mit der laufenden Beweiserhebung zu beginnen.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, stellen Sie sicher, dass Sie die folgenden Bedingungen erfüllen:

- Sie haben alle Voraussetzungen erfüllt, die unter Einrichtung AWS Audit Manager mit den empfohlenen Einstellungen beschrieben sind. Sie müssen Ihre AWS-Konto und die Audit Manager Manager-Konsole verwenden, um dieses Tutorial abzuschließen.
- Ihre IAM-Identität verfügt über die entsprechenden Berechtigungen, um eine Bewertung in Audit Manager zu erstellen und zu verwalten. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Aufgaben

- Schritt 1: Bewertungsdetails festlegen
- Schritt 2: Geben Sie den Geltungsbereich AWS-Konten an
- Schritt 3: Geben Sie die Audit-Verantwortlichen an
  - Berechtigungen des Audit-Inhabers
- Schritt 4: Überprüfen und Erstellen

Schritt 1: Bewertungsdetails festlegen

Wählen Sie zunächst ein Framework aus und geben Sie grundlegende Informationen für Ihre Bewertung an.

Um die Einzelheiten der Bewertung zu spezifizieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Bewertungen und danach Bewertung erstellen.
3. Geben Sie unter Name einen Namen für Ihre Bewertung ein.

4. (Optional) Geben Sie unter Beschreibung eine Beschreibung für Ihre Bewertung ein.
5. Wählen Sie unter Ziel der Bewertungsberichte den S3-Bucket aus, in dem Sie Ihre Bewertungsberichte speichern möchten.

> **Tip**
>
> Das Standardziel für Bewertungsberichte basiert auf Ihren Bewertungseinstellungen. Wenn Sie möchten, können Sie mehrere S3-Buckets erstellen und verwenden, um Ihre Bewertungsberichte für verschiedene Bewertungen zu organisieren. AWS Audit Manager unterstützt den Export von Bewertungsberichten in Amazon S3 S3-Buckets, einschließlich kontoübergreifender Ziele. Für optimale Sicherheit und Leistung empfehlen wir, einen S3-Bucket in demselben AWS Konto und derselben Region wie Ihre Bewertung zu verwenden.

6. Wählen Sie unter Framework auswählen das Framework aus, aus dem Sie Ihre Bewertung erstellen möchten. Sie können die Suchleiste auch verwenden, um ein Framework nach Namen oder nach Compliance-Standards oder -Vorschriften zu suchen.

> **Tip**
>
> Um mehr über ein Framework zu erfahren, wählen Sie den Namen des Frameworks aus, um die Seite mit den Framework-Details aufzurufen.

7. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um Ihrer Bewertung ein Tag zuzuordnen. Sie können für jedes Tag einen Schlüssel und einen Wert angeben. Der Tag-Schlüssel ist obligatorisch und kann als Suchkriterium verwendet werden, wenn Sie nach dieser Bewertung suchen.
8. Wählen Sie Weiter aus.

> **Note**
>
> Es ist wichtig, sicherzustellen, dass bei Ihrer Bewertung die richtigen Beweise für ein bestimmtes Framework gesammelt werden. Bevor Sie mit der Beweiserhebung beginnen, empfehlen wir Ihnen, die Anforderungen für das von Ihnen gewählte Framework zu überprüfen. Überprüfen Sie diese Anforderungen anschließend anhand Ihrer aktuellen AWS Config -Regelparameter. Um sicherzustellen, dass Ihre Regelparameter den Framework-Anforderungen entsprechen, können Sie die Regel unter AWS Config aktualisieren.

Nehmen wir beispielsweise an, Sie erstellen eine Bewertung für CIS v1.2.0. Dieses Framework hat eine Kontrolle namens 1.9 – Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert. In AWS Config hat die iam-password-policyRegel einen `MinimumPasswordLength` Parameter, der die Passwortlänge überprüft. Der Standardwert für diesen Parameter ist 14 Zeichen. Dadurch stimmt die Regel mit den Kontrollanforderungen überein. Wenn Sie nicht den Standardparameterwert verwenden, stellen Sie sicher, dass der von Ihnen verwendete Wert den Anforderungen durch CIS v1.2.0 von 14 Zeichen entspricht oder diese überschreitet. Die Standard-Parameterdetails für jede verwaltete Regel finden Sie in der AWS Config -Dokumentation.

Schritt 2: Geben Sie den Geltungsbereich AWS-Konten an

Sie können mehrere angeben AWS-Konten , die in den Umfang einer Bewertung fallen sollen. Audit Manager unterstützt mehrere Konten durch Integration mit AWS Organizations. Das bedeutet, dass Audit Manager Manager-Bewertungen für mehrere Konten ausgeführt werden können und die gesammelten Nachweise in einem delegierten Administratorkonto zusammengefasst werden. Informationen zum Aktivieren von Organizations in Audit Manager finden Sie unter Aktivieren und einrichten AWS Organizations.

Note

Audit Manager kann im Rahmen einer Bewertung bis zu 200 Konten unterstützen. Wenn Sie versuchen, mehr als 200 Konten einzubeziehen, schlägt die Erstellung der Bewertung fehl. Darüber hinaus schlägt die Erstellung der Bewertung fehl, wenn Sie versuchen, mehr als 250 eindeutige Konten für alle Ihre Bewertungen hinzuzufügen.

Um den Umfang zu AWS-Konten spezifizieren

1. Wählen Sie unter AWS-Kontendenjenigen aus AWS-Konten , den Sie in den Umfang Ihrer Bewertung einbeziehen möchten.
   - Wenn Sie Organizations in Audit Manager aktiviert haben, werden mehrere Konten angezeigt. Sie können ein oder mehrere Konten aus der Liste auswählen. Alternativ können Sie auch anhand des Kontonamens, der ID oder der E-Mail-Adresse nach einem Konto suchen.

- Wenn Sie Organizations in Audit Manager nicht aktiviert haben, werden nur Ihre aktuellen AWS-Konto Organisationen aufgeführt.

2. Wählen Sie Weiter aus.

> **Note**
>
> Wenn ein in den Bewertungsumfang fallendes Konto aus Ihrer Organisation entfernt wird, sammelt Audit Manager keine Beweise mehr für dieses Konto. Das Konto wird jedoch weiterhin in Ihrer Bewertung unter der Registerkarte „AWS-Konten“ angezeigt. Um das Konto aus der Liste der Konten im Gültigkeitsbereich zu entfernen, gehen Sie zu die Bewertung bearbeiten. Das entfernte Konto wird während der Bearbeitung nicht mehr in der Liste angezeigt, und Sie können Ihre Änderungen speichern, ohne dass dieses Konto im Gültigkeitsbereich enthalten ist.

Schritt 3: Geben Sie die Audit-Verantwortlichen an

In diesem Schritt geben Sie die Audit-Verantwortlichen für Ihre Bewertung an. Auditverantwortliche sind die Personen an Ihrem Arbeitsplatz — in der Regel aus GRC oder DevOps Teams — SecOps, die für die Verwaltung der Prüfung durch den Audit Manager verantwortlich sind. Wir empfehlen ihnen, die Richtlinie zu verwenden. AWSAuditManagerAdministratorAccess

Um die Audit-Verantwortlichen anzugeben

1. Sehen Sie sich unter Audit-Verantwortliche die aktuelle Liste der Audit-Verantwortlichen an. In der Spalte Audit Owner werden der Benutzer IDs und die Rollen angezeigt. In der AWS-KontoSpalte werden die Daten AWS-Konto dieses Audit-Inhabers angezeigt.
2. Audit-Verantwortliche, für die ein Kontrollkästchen aktiviert ist, werden in Ihre Bewertung aufgenommen. Deaktivieren Sie das Kontrollkästchen für alle Audit-Verantwortlichen, um sie aus der Bewertung zu entfernen. Sie können weitere Audit-Verantwortliche finden, indem Sie die Suchleiste verwenden, um nach Namen oder AWS-Konto zu suchen.
3. Wählen Sie Weiter aus, sobald Sie fertig sind.

Berechtigungen des Audit-Inhabers

Die folgende Richtlinie gilt für alle Prüfungsverantwortlichen einer Bewertung.

Audit Manager *placeholder text* ersetzt die durch Ihre Konto- und Ressourcen-IDs, bevor die Richtlinie angehängt wird.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AuditOwner",
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who are the audit owners of the
 Assessment"
            },
            "Action": [
                "auditmanager:GetAssessment",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAssessmentReportUrl"
            ],
            "Resource": [
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID",
```

```
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID/*"
            ]
        }
    ]
}
```

Schritt 4: Überprüfen und Erstellen

Überprüfen Sie die Informationen für Ihre Bewertung. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten. Wenn Sie fertig sind, wählen Sie Bewertung erstellen aus.

Mit dieser Aktion wird die fortlaufende Erfassung von Beweisen für Ihre Bewertung gestartet. Nachdem Sie eine Bewertung erstellt haben, wird die Beweiserhebung fortgesetzt, bis Sie den Bewertungsstatus auf inaktiv ändern. Alternativ können Sie die Erfassung von Nachweisen für eine bestimmte Kontrolle beenden, indem Sie den Kontrollstatus auf inaktiv ändern.

> **Note**
>
> Automatisierte Nachweise sind 24 Stunden nach der Erstellung Ihrer Bewertung verfügbar. Audit Manager sammelt automatisch Beweise aus mehreren Datenquellen, und die Häufigkeit dieser Beweiserhebung hängt von der Art der Beweise ab. Weitere Informationen finden Sie unter Häufigkeit der Beweissuche in diesem Leitfaden.

Nächste Schritte

Informationen dazu, wie Sie Ihre Bewertung zu einem späteren Zeitpunkt erneut überprüfen können, finden Sie unterSie finden Ihre Bewertungen in AWS Audit Manager. Gehen Sie wie folgt vor, um Ihre Bewertung zu finden, sodass Sie sie ansehen, bearbeiten oder weiterbearbeiten können.

Weitere Ressourcen

Lösungen für Bewertungsprobleme in Audit Manager finden Sie unterFehlersuche bei der Bewertung und Beweiserhebung.

Sie finden Ihre Bewertungen in AWS Audit Manager

Nachdem Sie Bewertungen in erstellt haben AWS Audit Manager, finden Sie sie auf der Bewertungsseite der Audit Manager Manager-Konsole.

Von dieser Seite aus können Sie verschiedene Aktionen an Ihren Bewertungen durchführen. Sie können beispielsweise Bewertungsdetails anzeigen, Bewertungskonfigurationen bearbeiten oder Bewertungen löschen, die nicht mehr benötigt werden. Darüber hinaus dient die Bewertungsseite als Ausgangspunkt für die Erstellung neuer Bewertungen.

Sie können Ihre Bewertungen auch programmgesteuert mithilfe der Audit Manager Manager-API oder der AWS Command Line Interface ()AWS CLI anzeigen.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor mindestens eine Bewertung erstellt haben. Wenn Sie noch keine Bewertung erstellt haben, werden Ihnen keine Ergebnisse angezeigt, wenn Sie diese Schritte ausführen.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können Ihre Bewertungen mit der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) anzeigen.

Audit Manager console

So zeigen Sie Ihre Bewertungen in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Bewertungen aus, um eine Liste Ihrer Bewertungen anzuzeigen.
3. Wählen Sie einen beliebigen Bewertungsnamen, um die Details zu dieser Bewertung anzuzeigen.

AWS CLI

So sehen Sie sich Ihre Bewertungen an (CLI)

Um Bewertungen in Audit Manager anzuzeigen, führen Sie den Befehl Bewertungen auflisten aus. Sie können den `--status`-Unterbefehl verwenden, um aktive oder inaktive Bewertungen anzuzeigen.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Um Ihre Bewertungen mithilfe der API einzusehen

Verwenden Sie den ListAssessmentsVorgang, um Bewertungen in Audit Manager anzuzeigen. Sie können das Attribut Status verwenden, um aktive oder inaktive Bewertungen anzuzeigen.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr in der AWS Audit Manager API-Referenz zu erfahren. Dazu gehören Informationen zur Verwendung der `ListAssessments` Operation und der Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Wenn Sie bereit sind, sich mit den Inhalten Ihrer Prüfung vertraut zu machen, folgen Sie den Anweisungen unter. Überprüfung einer Bewertung in AWS Audit Manager Diese Seite führt Sie durch die Einzelheiten der Prüfung und erklärt die Informationen, die Sie dort sehen.

Auf der Bewertungsseite können Sie auch eine Bewertung bearbeiten, eine Bewertung löschen oder eine Bewertung erstellen.

Weitere Ressourcen

Lösungen für Bewertungsprobleme in Audit Manager finden Sie unterFehlersuche bei der Bewertung und Beweiserhebung.

Überprüfung einer Bewertung in AWS Audit Manager

Nachdem Sie Bewertungen in Audit Manager erstellt haben, können Sie Ihre Bewertungen jederzeit öffnen und überprüfen.

Wichtige Punkte

Wenn Sie bereit sind, sich mit Ihrer Bewertung zu befassen, können Sie sich Schritt für Schritt eingehender mit den Einzelheiten befassen und Ihre Bewertung mit zunehmender Detailgenauigkeit überprüfen.

1. Einzelheiten der Bewertung — Sehen Sie sich zunächst die allgemeinen Einzelheiten Ihrer Bewertung an. Auf dieser Seite können Sie den Namen, die Beschreibung, den Umfang und andere Details der Prüfung überprüfen. Auf diese Weise erhalten Sie einen allgemeinen Überblick über die Bewertung.
2. Einzelheiten der Bewertungskontrolle — Als Nächstes sollten Sie sich eingehender mit der Bewertung befassen, indem Sie die Einzelheiten der einzelnen Bewertungskontrollen überprüfen. Auf diese Weise können Sie die spezifischen Anforderungen und Ziele der einzelnen Kontrollen verstehen.
3. Details zum Nachweisordner — Für jede Bewertungskontrolle können Sie die entsprechenden Nachweisordner überprüfen, die die Nachweise für eine bestimmte Kontrolle enthalten. In diesen Ordnern sind die Belege organisiert, die sich auf die einzelnen Kontrollen beziehen.
4. Einzelheiten zu den Nachweisen — Gehen Sie abschließend genauer vor, um die einzelnen Beweise in den einzelnen Ordnern zu überprüfen. Dazu können Konfigurationsschnappschüsse, Benutzeraktivitätsprotokolle, Konformitätserkenntnisse oder manuell hochgeladene Nachweise wie Dokumente und Screenshots gehören. Wenn Sie sich diese Nachweise ansehen, können Sie besser verstehen, wie Ihr Unternehmen die Anforderungen der Kontrolle erfüllt.

Wenn Sie diese Schritte befolgen, können Sie Ihre Bewertung gründlich untersuchen, ihre Bestandteile verstehen und die Nachweise überprüfen, die die Compliance-Bemühungen Ihres Unternehmens belegen.

Weitere Ressourcen

Um mit der Überprüfung einer Bewertung in Audit Manager zu beginnen, folgen Sie den hier beschriebenen Verfahren.

- Überprüfung der Bewertungsdetails in AWS Audit Manager
- Überprüfung einer Bewertungskontrolle in AWS Audit Manager

- Überprüfung eines Beweisordners in AWS Audit Manager
- Überprüfung von Nachweisen in AWS Audit Manager

Überprüfung der Bewertungsdetails in AWS Audit Manager

Wenn Sie die Einzelheiten einer Prüfung überprüfen möchten, finden Sie die Informationen auf der Seite mit den Prüfungsdetails in mehreren Abschnitten. Diese Abschnitte helfen Ihnen, auf einfache Weise auf die für Ihre Aufgabe relevanten Informationen zuzugreifen und diese zu verstehen.

Inhalt

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor mindestens eine Bewertung erstellt haben. Wenn Sie noch keine Bewertung erstellt haben, werden Ihnen keine Ergebnisse angezeigt, wenn Sie diese Schritte ausführen.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Um eine Seite mit Prüfungsdetails zu öffnen und zu überprüfen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Bewertungen aus, um eine Liste Ihrer Bewertungen anzuzeigen.
3. Wählen Sie den Namen der Bewertung, um sie zu öffnen.
4. Überprüfen Sie die Bewertungsdetails anhand der folgenden Informationen als Referenz.

Abschnitte der Seite mit den Bewertungsdetails

- Abschnitt mit den Einzelheiten zur Bewertung
- Registerkarte „Kontrollen“
- Registerkarte „Auswahl für den Bewertungsbericht“
- AWS-Konten Registerkarte
- AWS-Services Registerkarte
- Registerkarte Audit-Verantwortliche
- Registerkarte „Tags“
- Registerkarte „Änderungsprotokoll“

Abschnitt mit den Einzelheiten zur Bewertung

Sie können den Abschnitt mit den Bewertungsdetails verwenden, um eine Zusammenfassung Ihrer Bewertung einzusehen.

Im Abschnitt mit den Prüfungsdetails können Sie die folgenden Informationen überprüfen:

Name	Description
1. Beschreibung	Die Beschreibung der Bewertung.
2. Art der Einhaltung	Der Konformitätsstandard oder die Verordnung, die durch die Bewertung unterstützt wird.
3. Ziel der Bewertung sberichte	Der S3-Bucket, in dem Audit Manager den Bewertungsbericht speichert.
4. Beweise insgesamt	Die Gesamtzahl der Beweismittel, die für diese Bewertung gesammelt wurden.
5. Auswahl des Bewertung sberichts	Die Anzahl der Belege, die ausgewählt wurden, um in den Bewertungsbericht aufgenommen zu werden.
6. Erstellungsdatum	Das Datum, an dem die Bewertung erstellt wurde.
7. Letzte Aktualisierung	Das Datum, an dem die Bewertung zuletzt bearbeitet wurde.
8. Status	Der Status der Bewertung. • Aktiv — Im Rahmen der Bewertung werden derzeit Beweise gesammelt. • Inaktiv — Bei der Bewertung werden keine Beweise mehr gesammelt.

Registerkarte „Kontrollen“

Auf dieser Registerkarte können Sie Informationen zu den Kontrollen in der Bewertung einsehen.

Unter Übersicht über den Kontrollstatus können Sie die folgenden Informationen überprüfen:

Name	Description
Kontrollen insgesamt	Die Gesamtzahl der Kontrollen in dieser Bewertung.
Überprüft	Die Anzahl der Kontrollen, die von einem Prüfinhaber oder einem Delegierten überprüft wurden.

Name	Description
Wird geprüft	Die Anzahl der Kontrollen, die derzeit überprüft werden.
Inaktiv	Die Anzahl der Kontrollen, die nicht mehr aktiv Beweise sammeln

In der Tabelle Kontrollsätze können Sie eine Liste von Kontrollen einsehen, die nach Kontrollsätzen gruppiert sind. Sie können die Kontrollen in jedem Kontrollsatz erweitern oder reduzieren. Sie können auch nach Namen suchen, wenn Sie nach einem bestimmten Steuerelement suchen.

In dieser Tabelle können Sie die folgenden Informationen überprüfen:

Name	Description
Steuerelemente, gruppiert nach Steuerungssätzen	Der Name des Kontrollsatzes.
Status der Steuerung	Der Status der Kontrolle. • Wird überprüft bedeutet, dass diese Kontrolle noch nicht überprüft wurde. Für diese Kontrolle werden noch Beweise gesammelt, und Sie können manuelle Nachweise hinzufügen. Dies ist die Standardeinstellung. • Überprüft bedeutet, dass die Beweise für diese Kontrolle überprüft wurden. Es werden immer noch Beweise gesammelt, und Sie können manuelle Beweise hinzufügen. • Inaktiv bedeutet, dass die automatische Beweiserhebung für diese Kontrolle gestoppt wurde. Sie können keine manuellen Beweise mehr hinzufügen.
Delegiert an	Der Prüfer dieser Kontrolle, falls sie einem Delegierten zur Überprüfung zugewiesen wurde.
Gesamtzahl der Beweise	Die Anzahl der Beweisstücke, die für diese Kontrolle gesammelt wurden.

Registerkarte „Auswahl für den Bewertungsbericht“

Auf dieser Registerkarte können Sie sich die Nachweise anzeigen lassen, die in den Bewertungsbericht aufgenommen werden. Die Nachweise sind nach Nachweisordnern gruppiert, die nach dem Datum ihrer Erstellung geordnet sind.

Sie können diese Ordner durchsuchen und auswählen, welche Beweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Anweisungen zum Hinzufügen von Nachweisen zu einem Bewertungsbericht finden Sie unterHinzufügen von Beweisen zu einem Bewertungsbericht.

In diesem Abschnitt können Sie sich die folgenden Informationen ansehen:

Name	Description
Ordner mit Nachweisen	Der Name des Beweisordners. Der Ordnername basiert auf dem Datum, an dem die Beweise gesammelt wurden.
Ausgewählte Beweise	Die Anzahl der Beweiselemente innerhalb des Ordners, die im Bewertungsbericht enthalten sind.
Name des Steuerelements	Der Name des Steuerelements, das diesem Beweisordner zugeordnet ist.

AWS-Konten Registerkarte

Auf dieser Registerkarte können Sie sehen AWS-Konten , welche Punkte Gegenstand der Bewertung sind.

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Konto-ID	Die ID der AWS-Konto.
Account name (Kontoname)	Der Name der AWS-Konto.
E-Mail	Geben Sie die E-Mail-Adresse an, die dem AWS-Konto zugeordnet ist.

AWS-Services Registerkarte

Möglicherweise sehen Sie diese Registerkarte in Ihrer Bewertung oder auch nicht.

Wenn der AWS-Services Tab nicht angezeigt wird (idealer Zustand)

Wenn Sie diese Registerkarte nicht sehen, verwaltet Audit Manager, welche AWS-Services Bereiche für Ihre Bewertung relevant sind.

Audit Manager leitet diesen Umfang ab, indem er Ihre Bewertungskontrollen und deren Datenquellen untersucht und diese Informationen dann den entsprechenden AWS-Services zuordnet. Immer wenn sich eine zugrunde liegende Datenquelle für Ihre Bewertung ändert, aktualisiert Audit Manager den Umfang automatisch nach Bedarf, um die richtigen Daten widerzuspiegeln AWS-Services. Dadurch wird sichergestellt, dass bei Ihrer Bewertung genaue und umfassende Nachweise über alle relevanten Services in Ihrer AWS Umgebung gesammelt werden.

Wenn die AWS-Services Registerkarte angezeigt wird

Wenn Sie diese Registerkarte sehen, verwaltet Audit Manager nicht, welche AWS-Services Bereiche für Ihre Bewertung relevant sind.

In diesem Fall werden Ihnen die folgenden Informationen zu den Services im Umfang angezeigt, die Sie definiert haben:

Name	Description
AWS-Service	Der Name der AWS-Service.
Kategorie	Die Dienstkategorie, z. B. Datenverarbeitung oder Datenbank.
Beschreibung	Die Beschreibung von AWS-Service.

Audit Manager führt Ressourcenbewertungen für die Services in dieser Tabelle durch.
Wenn Amazon S3 beispielsweise aufgeführt ist, kann Audit Manager Beweise über Ihre S3-Buckets sammeln. Die genauen Beweise, die gesammelt werden, werden von einer Kontrolle bestimmtdata source. Wenn der Datenquellentyp beispielsweise ist AWS Config und es sich bei der Datenquellenzuordnung um eine AWS Config Regel handelt (z. B.`s3-bucket-public-write-prohibited`), erfasst Audit Manager das Ergebnis dieser Regelauswertung als Nachweis. Weitere Informationen finden Sie unter Was ist der Unterschied zwischen einem Service im Umfang und einem Datenquellentyp? in diesem Handbuch.

Wenn Ihre Bewertung in der Konsole anhand eines Standard-Frameworks erstellt wurde, hat Audit Manager die Services für Sie ausgewählt und deren Datenquellen gemäß den Anforderungen des Frameworks zugeordnet. Wenn das Standardrahmen nur manuelle Kontrollen enthält, AWS-Services sind keine im Geltungsbereich enthalten.

> **Note**
>
> Wenn Sie Ihre Bewertung das nächste Mal bearbeiten oder eine der benutzerdefinierten Kontrollen in Ihrer Bewertung ändern, übernimmt Audit Manager die Verwaltung der im Leistungsumfang enthaltenen Services für Sie. In diesem Fall wird die AWS-ServicesRegisterkarte aus Ihrer Bewertung entfernt.

Registerkarte Audit-Verantwortliche

Auf dieser Registerkarte können Sie die Prüfungsverantwortlichen für die Bewertung einsehen.

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Audit-Verantwortlicher	Der Name des Prüfinhabers.
AWS-Konto	Die AWS-Konto ID des Prüfinhabers.

Registerkarte „Tags“

Auf dieser Registerkarte können Sie die Tags für Ihre Bewertung einsehen. Diese Tags werden von dem Framework übernommen, das zur Erstellung der Bewertung verwendet wurde. Weitere Informationen zur Verwendung von Tags in Audit Manager finden Sie unter Ressourcen taggen AWS Audit Manager.

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Key (Schlüssel)	Der Schlüssel des Tags, z. B. ein Konformitätsstandard, eine Vorschrift oder eine Kategorie.

Name	Description
Wert	Der Wert des Tags.

Registerkarte „Änderungsprotokoll“

Auf dieser Registerkarte können Sie sich die Benutzeraktivitäten für die Bewertung ansehen.

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Date (Datum)	Das Datum der Aktivität.
Nutzer	Der Benutzer, der die Aktion ausgeführt hat.
Action (Aktion)	Die Aktion, die stattgefunden hat, z. B. eine Bewertung, die gerade erstellt wurde.
Typ	Der Objekttyp, der sich geändert hat, z. B. eine Bewertung.
Ressource	Die Ressource, die von der Änderung betroffen war, z. B. das Framework, aus dem die Bewertung erstellt wurde.

Nächste Schritte

Gehen Sie wie unter beschrieben vor, um den Inhalt Ihrer Bewertung weiter zu überprüfenÜberprüfung einer Bewertungskontrolle in AWS Audit Manager. Diese Seite führt Sie durch die Einzelheiten der Bewertungskontrolle und erklärt die dort angezeigten Informationen.

Weitere Ressourcen

- Auf meiner Seite mit den Bewertungsdetails werde ich aufgefordert, meine Bewertung erneut zu erstellen
- Ich kann in meiner Bewertung keine Kontrollen oder Kontrollsätze sehen
- Ich kann nicht sehen, welche Dienste in den Geltungsbereich meiner Bewertung fallen

Überprüfung einer Bewertungskontrolle in AWS Audit Manager

Wenn Sie die Kontrollen in einer Bewertung überprüfen müssen, finden Sie die Informationen auf der Seite mit den Details zur Bewertungskontrolle in mehreren Abschnitten. Diese Abschnitte helfen Ihnen, auf einfache Weise auf die für Ihre Aufgabe relevanten Informationen zuzugreifen und diese zu verstehen.

Inhalt

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor mindestens eine Bewertung erstellt haben. Wenn Sie noch keine Bewertung erstellt haben, werden Ihnen keine Ergebnisse angezeigt, wenn Sie diese Schritte ausführen.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

So öffnen und überprüfen Sie eine Seite mit den Details einer Bewertungskontrolle

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.

2. Wählen Sie im Navigationsbereich Assessments und dann den Namen einer Bewertung aus, um sie zu öffnen.
3. Wählen Sie auf der Bewertungsseite die Registerkarte Kontrollen aus, scrollen Sie nach unten zur Tabelle Kontrollsätze und wählen Sie dann den Namen einer Kontrolle aus, um es zu öffnen.
4. Überprüfen Sie die Einzelheiten der Bewertungskontrolle und verwenden Sie dabei die folgenden Informationen als Referenz.

Abschnitte der Seite mit den Details zur Bewertungskontrolle

- Abschnitt mit den Kontrolldetails
- Registerkarte „Beweisordner“
- Registerkarte Details
- Registerkarte „Quellen der Beweise“
- Registerkarte „Kommentare“
- Registerkarte „Änderungsprotokoll“

Abschnitt mit den Kontrolldetails

Im Abschnitt Kontrolldetails finden Sie eine Zusammenfassung der Bewertungskontrolle.

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Beschreibung	Die Beschreibung, die für dieses Steuerelement bereitgestellt wurde.
Status der Steuerung	Der Status der Kontrolle. • Wird überprüft — Das Steuerelement wurde noch nicht überprüft . Für diese Kontrolle werden noch Beweise gesammelt, und Sie können manuelle Nachweise hinzufügen. Dies ist die Standarde instellung. • Geprüft — Die Beweise für diese Kontrolle werden überprüft. Beweise werden noch gesammelt, und Sie können manuelle Beweise hinzufügen.

Name	Description
	• Inaktiv — Die automatische Beweiserhebung wurde für diese Kontrolle gestoppt. Sie können keine manuellen Beweise mehr hinzufügen.

Registerkarte „Beweisordner“

Auf dieser Registerkarte können Sie sich die Beweise ansehen, die für diese Kontrolle gesammelt wurden. Sie wird täglich in Ordnern organisiert. Von hier aus können Sie auch die folgenden Aktionen ausführen:

- Einen Beweisordner überprüfen — Um Details zu einem Beweisordner anzuzeigen, wählen Sie den Namen des Ordners, auf den ein Hyperlink verweist.
- Einen Beweisordner zu einem Bewertungsbericht hinzufügen — Um einen Beweisordner hinzuzufügen, wählen Sie ihn aus und klicken Sie auf Zum Bewertungsbericht hinzufügen.
- Einen Ordner mit Nachweisen aus einem Bewertungsbericht entfernen — Um einen Ordner auszuschließen, wählen Sie ihn aus und klicken Sie auf Aus Bewertungsbericht entfernen.
- Manuelle Nachweise hinzufügen — Anweisungen finden Sie unterManuelle Nachweise hinzufügen in AWS Audit Manager.

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Ordner mit Nachweisen	Der Name des Beweisordners. Der Name basiert auf dem Datum, an dem die Beweise gesammelt oder manuell hinzugefügt wurden.
Überprüfung der Einhaltung der Vorschriften	Die Anzahl der Probleme im Beweisordner. Diese Zahl steht für die Gesamtzahl der Sicherheitsprobleme, die direkt von AWS Security Hub CSPM AWS Config, oder beiden gemeldet wurden. Wenn Sie Nicht zutreffend sehen, bedeutet dies, dass Sie Security Hub CSPM entweder nicht AWS Config aktiviert haben oder dass der Nachweis aus einem anderen Datenquellentyp stammt.
Beweise insgesamt	Die Gesamtzahl der Beweiselemente im Ordner.

Name	Description
Auswahl des Bewertungsberichts	Die Anzahl der Nachweise innerhalb des Ordners, die im Bewertungsbericht enthalten sind.

> **Tip**
>
> Wenn Sie den Ordner mit den Nachweisen, nach dem Sie suchen, nicht finden können, ändern Sie den Dropdownfilter auf Alle Zeiten. Andernfalls werden standardmäßig die Ordner der letzten sieben Tage angezeigt.

Registerkarte Details

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Informationen zum Testen	Das empfohlene Verfahren, um zu testen, ob die Steuerung wie vorgesehen funktioniert.
Aktionsplan	Die empfohlenen Maßnahmen, die ergriffen werden müssen, falls die Kontrolle behoben werden muss.

Registerkarte „Quellen der Beweise“

Auf dieser Registerkarte können Sie sehen, woher die Bewertungskontrolle Beweise sammelt. Die Evidenzquellen können eine der folgenden Quellen umfassen:

Name	Description
Allgemeine Kontrollen	Dies sind die gemeinsamen Kontrollen, bei denen Beweise gesammelt werden, um die Bewertungskontrolle zu stützen. Bei den allgemeinen Kontrollen werden Nachweise anhand der zugrunde liegenden Datenquellen gesammelt, die für Sie AWS verwaltet werden. Für jede aufgelistete gemeinsame Kontrolle

Name	Description
	sammelt Audit Manager die relevanten Nachweise für alle unterstützenden Kernkontrollen. Wählen Sie eine gemeinsame Kontrolle aus, um die zugehörigen Kernkontrollen zu sehen.
Zentrale Steuerelemente	Dies sind die wichtigsten Kontrollen, mit denen Nachweise gesammelt werden, um die Bewertungskontrolle zu unterstützen. Kernkontrollen sammeln Beweise mithilfe einer vordefinierten Gruppe von Datenquellen, die für Sie AWS verwaltet werden. Wählen Sie ein zentrales Steuerelement aus, um die zugrunde liegenden Datenquellen zu sehen.

Name	Description

Datenquellen	Dies sind die einzelnen Datenquellen, die Beweise zur Unterstützung der Bewertungskontrolle sammeln.
	• Name — Der Name der Datenquelle.
	• Typ — Der Typ der Datenquelle, aus der die Beweise stammen.
	  • Wenn Audit Manager die Beweise sammelt, kann es sich bei dem Typ um AWS Security Hub CSPMAWS Config, AWS CloudTrail, oder AWS API-Aufrufe handeln.
	  • Wenn Sie Ihre eigenen Nachweise hochladen, ist der Typ Manuell. Eine Beschreibung gibt an, ob es sich bei den erforderlichen manuellen Beweisen um einen Datei-Upload oder eine Textantwort handelt.
	• Zuordnung — Das spezifische Schlüsselwort, das zum Sammeln von Beweisen verwendet wird.
	  • Wenn der Typ ist AWS Config, handelt es sich bei der Zuordnung um eine AWS Config Regel `SNS_ENCRYPTED_KMS` (z. B.
	  • Wenn der Typ ist AWS Security Hub CSPM, handelt es sich bei der Zuordnung um ein Security Hub CSPM-Steuerelement (z. B.`EC2.1`).
	  • Handelt es sich bei dem Typ um AWS API-Aufrufe, handelt es sich bei der Zuordnung um einen API-Aufruf (z. B.`kms_ListKeys`).
	  • Wenn der Typ ist AWS CloudTrail, handelt es sich bei der Zuordnung um ein CloudTrail Ereignis (z. B.`CreateAccessKey`).
	• Häufigkeit — Wie oft Audit Manager Beweise für eine AWS API-Aufruf-Datenquelle sammelt.

Registerkarte „Kommentare“

Auf dieser Registerkarte können Sie einen Kommentar zur Kontrolle und ihren Nachweisen hinzufügen. Sie können auch eine Liste früherer Kommentare einsehen.

- Unter Kommentare senden können Sie Kommentare zu einer Kontrolle hinzufügen, indem Sie Text eingeben und dann Kommentare einreichen auswählen.
- Unter Frühere Kommentare können Sie eine Liste früherer Kommentare zusammen mit dem Datum, an dem der Kommentar abgegeben wurde, und der zugehörigen Benutzer-ID einsehen.

Registerkarte „Änderungsprotokoll“

Auf dieser Registerkarte können Sie sich die Benutzeraktivitäten für die Bewertungskontrolle ansehen. Dieselben Informationen sind verfügbar, wenn sich der Audit Trail anmeldet. AWS CloudTrail Mit der Benutzeraktivität, die direkt in Audit Manager erfasst wird, können Sie ganz einfach einen Audit Trail mit Aktivitäten für eine bestimmte Kontrolle überprüfen.

In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
Date (Datum)	Datum und Uhrzeit der Aktivität, dargestellt in koordinierter Weltzeit (UTC).
Nutzer	Der Benutzer oder die Rolle, die die Aktivität ausgeführt hat.
Action (Aktion)	Die Aktion, die stattgefunden hat, z. B. eine Bewertung, die erstellt wurde.
Typ	Der Objekttyp, der sich geändert hat, z. B. eine Bewertung.
Ressource	Die Ressource, die von der Änderung betroffen war, z. B. das Framework, aus dem die Bewertung erstellt wurde.

Audit Manager verfolgt die folgenden Benutzeraktivitäten in Änderungsprotokollen:

- Erstellen einer Bewertung
- Bearbeiten einer Bewertung
- Abschluss einer Bewertung
- Löschen einer Bewertung
- Delegieren eines Kontrollsatzes zur Überprüfung

- Rückgabe eines überprüften Kontrollsatzes an den Audit-Verantwortlichen
- Manuelle Beweise hochladen
- Aktualisierung eines Kontrollstatus
- Generieren von Bewertungsberichten

Nächste Schritte

Gehen Sie wie unter beschrieben vor, um Ihre Bewertung weiter zu überprüfenÜberprüfung eines Beweisordners in AWS Audit Manager. Diese Seite führt Sie durch die Ordner mit Nachweisen und zeigt Ihnen, wie Sie die angezeigten Informationen verstehen können.

Weitere Ressourcen

- Ich kann in meiner Bewertung keine Kontrollen oder Kontrollsätze sehen

Überprüfung eines Beweisordners in AWS Audit Manager

Während Ihre Bewertung Beweise sammelt, organisiert Audit Manager diese zur besseren Übersicht in Ordnern. Wenn Sie einen Beweisordner überprüfen müssen, finden Sie die Informationen, die in mehrere Abschnitte unterteilt sind.

Inhalt

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor mindestens eine Bewertung erstellt haben. Wenn Sie noch keine Bewertung erstellt haben, werden Ihnen keine Ergebnisse angezeigt, wenn Sie diese Schritte ausführen.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Denken Sie daran, dass es bis zu 24 Stunden dauern kann, bis eine Bewertung mit der automatischen Erfassung von Nachweisen beginnt. Wenn für Ihre Bewertung noch keine Beweise vorliegen, werden Sie keine Ergebnisse sehen, wenn Sie diese Schritte ausführen.

Verfahren

Um einen Beweisordner zu öffnen und zu überprüfen

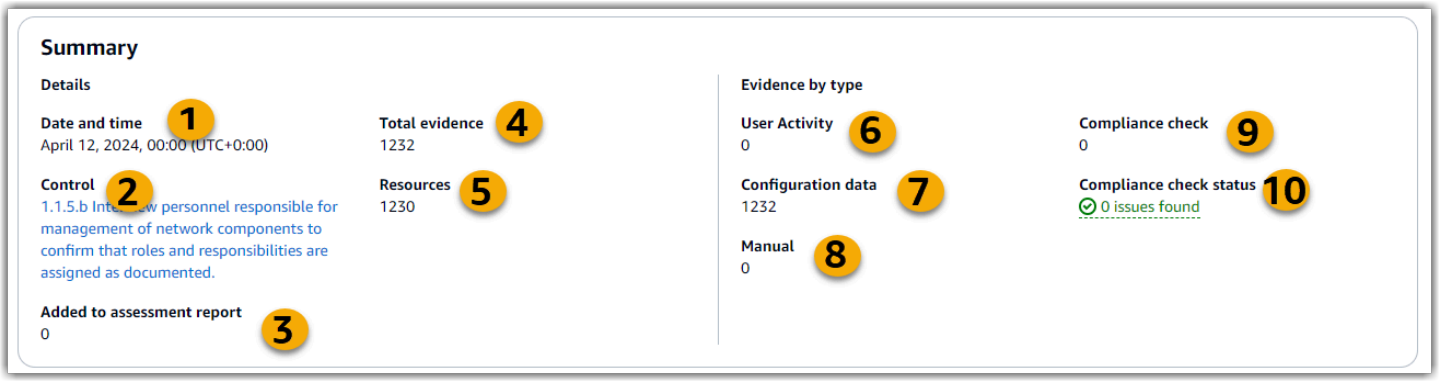
1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Assessments und anschließend eine Bewertung aus.
3. Wählen Sie auf der Bewertungsseite die Registerkarte Kontrollen aus, scrollen Sie nach unten zur Tabelle Kontrollen, und wählen Sie dann eine Bewertungskontrolle aus.
4. Wählen Sie auf der Seite „Bewertungskontrolle“ die Registerkarte „Nachweisordner“ aus.
5. Wählen Sie in der Tabelle Nachweisordner den Namen eines Nachweisordners aus.
6. Prüfen Sie den Beweisordner anhand der folgenden Informationen als Referenz.

Abschnitte einer Seite mit einer Beweismappe

- Übersicht der Beweismappe
- Beweistabelle

Übersicht der Beweismappe

Sie können den Abschnitt Zusammenfassung der Seite verwenden, um einen allgemeinen Überblick über die Beweise im Beweisordner zu erhalten. Weitere Informationen zu den verschiedenen Beweisarten finden Sie unter Beweise.



In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
1. Datum und Uhrzeit	Uhrzeit und Datum der Erstellung des Beweisordners. Dies wird in koordinierter Weltzeit (UTC) dargestellt.
2. Kontrolle	Der Name der Kontrolle, die mit dem Beweisordner verknüpft ist.
3. Zum Bewertungsbericht hinzugefügt	Die Anzahl der Beweismittel, die für den Bewertungsbericht ausgewählt wurden.
4. Beweise insgesamt	Die Gesamtzahl der Beweisstücke in der Beweismappe.
5. Ressourcen	Die Gesamtzahl der AWS Ressourcen, die bei der Erfassung der Beweise in diesem Ordner bewertet wurden.
6. Benutzeraktivität	Die Anzahl der Nachweise, die unter die Kategorie Benutzera ktivität fallen. Diese Beweise werden aus AWS CloudTrail Protokoll en gesammelt.
7. Konfigurationsdaten	Die Anzahl der Nachweiselemente, die unter die Kategorie Konfigurationsdaten fallen. Diese Beweise werden anhand von API-Aufrufen gesammelt, die Konfigurationsschnappschüsse anderer AWS-Services Benutzer erstellen.
8. Manuell	Die Anzahl der Beweisstücke, die unter die Kategorie manuell fallen. Diese Nachweise werden manuell hinzugefügt.

Name	Description
9. Überprüfung der Einhaltung der Vorschriften	Die Anzahl der Nachweise, die unter die Kategorie Konformit ätsprüfung fallen. Diese Nachweise wurden von AWS Config AWS Security Hub CSPM, oder beiden gesammelt.
10. Status der Konformit ätsprüfung	Die Gesamtzahl der Probleme, die direkt von AWS Security Hub CSPM oder beiden gemeldet wurden. AWS Config

Beweistabelle

In der Tabelle Beweise können Sie sich die Beweise ansehen, die im Beweisordner enthalten sind. Von dieser Tabelle aus können Sie auch die folgenden Aktionen ausführen:

- Einzelne Beweise überprüfen — Wenn Sie Einzelheiten zu einem beliebigen Beweisstück anzeigen möchten, wählen Sie in der Spalte Zeit den Namen des mit einem Hyperlink versehenen Beweismittels aus.
- Beweise zu einem Beurteilungsbericht hinzufügen — Um Beweise hinzuzufügen, wählen Sie diese aus und wählen Sie „Zum Bewertungsbericht hinzufügen“.
- Beweise aus einem Bewertungsbericht entfernen — Um Nachweise auszuschließen, wählen Sie sie aus und wählen Sie „Aus Bewertungsbericht entfernen“.
- Manuelle Nachweise hinzufügen — Anweisungen finden Sie unterManuelle Nachweise hinzufügen in AWS Audit Manager.

In dieser Tabelle können Sie sich die folgenden Informationen ansehen:

Name	Description
Time (Zeit)	Gibt an, wann die Beweise gesammelt wurden. Dies dient auch als Name der Beweise. Die Zeit wird im UTC-Format (Coordinated Universal Time) dargestellt.
Überprüfung der Einhaltung der Vorschriften	Der Bewertungsstatus von Nachweisen, die unter die Kategorie Konformitätsprüfung fallen.

Name	Description
	• Bei Nachweisen, die von Security Hub CSPM gesammelt wurden, wird das Ergebnis „Bestanden oder nicht bestanden“ direkt vom Security Hub CSPM gemeldet. • Bei Nachweisen, die von gesammelt wurden AWS Config, wird das Ergebnis „Konform“ oder „Nicht konform“ direkt von gemeldet. AWS Config • Wenn Nicht zutreffend angezeigt wird, bedeutet dies, dass Sie entweder Security Hub CSPM nicht aktiviert haben AWS Config oder dass der Nachweis aus einem anderen Datenquellentyp stammt.
Nachweise nach Typ	Die Art der Beweise. • Nachweise zur Konformitätsprüfung werden von AWS Config od er gesammelt AWS Security Hub CSPM. • Nachweise über Benutzeraktivitäten werden von gesammelt AWS CloudTrail. • Nachweise für Konfigurationsdaten werden aus API-Aufrufen an andere gesammelt AWS-Services. • Manuelle Nachweise sind Nachweise, die Sie manuell hinzufüge n.
Datenquelle	Die Datenquelle, aus der die Beweise gesammelt werden.
Ereignisname	Der Name des Ereignisses, das die Beweiserhebung ausgelöst hat.
Ereignisquelle	Der Dienstleiter, der die AWS-Service für das Ereignis relevanten Personen identifiziert.
Ressourcen	Die Anzahl der Ressourcen, die bei der Beweiserhebung bewertet wurden.

Name	Description
Auswahl des Bewertungsberichts	Gibt an, ob die Nachweise im Bewertungsbericht enthalten sind. • Um Beweise aufzunehmen, wählen Sie die Beweise aus und klicken Sie auf Zum Bewertungsbericht hinzufügen. • Um Beweise auszuschließen, wählen Sie die Beweise aus und klicken Sie auf Aus Bewertungsbericht entfernen.

Nächste Schritte

Wenn Sie bereit sind, die einzelnen Beweise in einem Ordner zu untersuchen, folgen Sie den Schritten unterÜberprüfung von Nachweisen in AWS Audit Manager. Diese Seite führt Sie durch die Einzelheiten der Beweise und zeigt Ihnen, wie Sie die darin enthaltenen Informationen interpretieren können.

Weitere Ressourcen

- Lösungen für Probleme mit Nachweisen in Audit Manager finden Sie unterFehlersuche bei der Bewertung und Beweiserhebung.

Überprüfung von Nachweisen in AWS Audit Manager

Wenn Sie ein bestimmtes Beweisstück überprüfen müssen, folgen Sie den Anweisungen auf dieser Seite. Die Einzelheiten zu den Beweisen sind in mehrere Abschnitte unterteilt.

Inhalt

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor mindestens eine Bewertung erstellt haben. Wenn Sie noch keine Bewertung erstellt haben, werden Ihnen keine Ergebnisse angezeigt, wenn Sie diese Schritte ausführen.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Denken Sie daran, dass es bis zu 24 Stunden dauern kann, bis eine Bewertung mit der automatischen Erfassung von Nachweisen beginnt. Wenn für Ihre Bewertung noch keine Beweise vorliegen, werden Sie keine Ergebnisse sehen, wenn Sie diese Schritte ausführen.

Verfahren

Um eine Seite mit Nachweisdetails zu öffnen und zu überprüfen

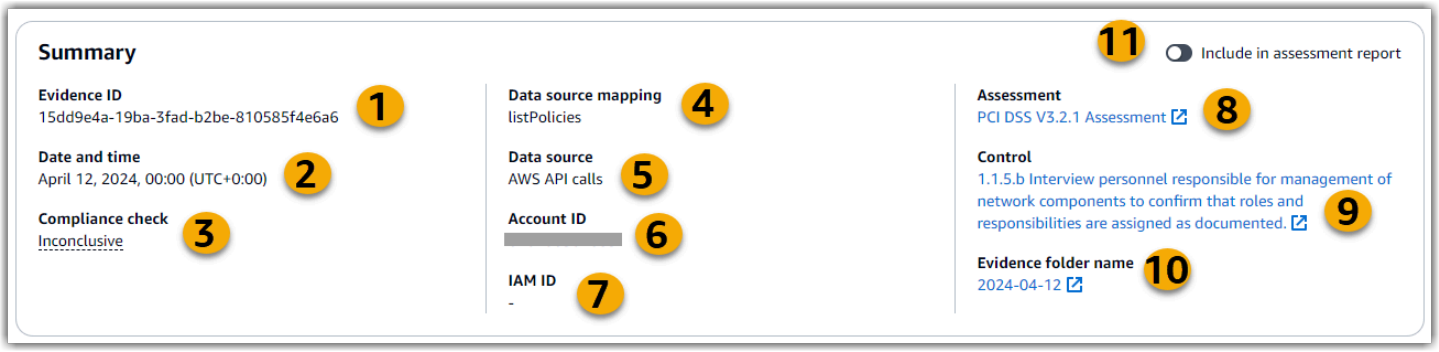
1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Assessments und anschließend eine Bewertung aus.
3. Wählen Sie auf der Bewertungsseite die Registerkarte Kontrollen aus, scrollen Sie nach unten zur Tabelle Kontrollen, und wählen Sie dann ein Steuerelement aus.
4. Wählen Sie auf der Kontrollseite die Registerkarte Beweisordner aus.
5. Wählen Sie in der Tabelle Nachweisordner den Namen eines Nachweisordners aus.
6. Wählen Sie den Namen der Beweise in der Spalte Zeit aus, um die Seite mit den Nachweisdetails zu öffnen.
7. Überprüfen Sie die Beweisdetails anhand der folgenden Informationen als Referenz.

Abschnitte einer Seite mit Beweisdetails

- Zusammenfassung
- Attribute
- Enthaltene Ressourcen

Zusammenfassung

Sie können den Abschnitt Zusammenfassung verwenden, um einen Überblick über die Beweise zu erhalten.



In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Description
1. ID des Nachweises	Die eindeutige Kennung für die Beweise.
2. Datum und Uhrzeit	Die Uhrzeit und das Datum, an dem die Beweise gesammelt wurden. Dies wird in koordinierter Weltzeit (UTC) dargestellt.
3. Überprüfung der Einhaltung der Vorschriften	Der Bewertungsstatus der Nachweise für die Konformitätsprüfung. • Für Nachweise, die von gesammelt wurden AWS Security Hub CSPM, wird das Ergebnis „Bestanden oder Nicht bestanden“ direkt von gemeldet AWS Security Hub CSPM. • Bei Nachweisen, die von gesammelt wurden AWS Config, wird das Ergebnis „Konform“ oder „Nicht konform“ direkt von AWS Config gemeldet. • Wenn „Nicht zutreffend“ angezeigt wird, weist dies auf eines von zwei Dingen hin. Entweder haben Sie es nicht AWS Security Hub CSPM oder es AWS Config ist aktiviert. Oder die Beweise stammen aus einer anderen Datenquelle.
4. Zuordnung von Datenquellen	Das Zuordnungsschlüsselwort, das zum Sammeln der Beweise verwendet wurde.

Name	Description
5. Data source type (Datenquellentyp)	Die Art der Datenquelle, aus der die Beweise gesammelt wurden.
6. Konto-ID	Das AWS-Konto , was mit den Beweisen zusammenhängt.
7. ICH BIN ID	Der entsprechende Benutzer oder die entsprechende Rolle, falls zutreffend.
8. Bewertung	Der Name der Bewertung, die mit den Beweisen verknüpft ist.
9. Kontrolle	Der Name der Kontrolle, die mit den Beweisen verknüpft ist.
10. Name des Beweisordners	Der Name des Beweisordners, der die Beweise enthält.
11. In den Bewertungsbericht aufnehmen	Der Schalter, mit dem Sie die Nachweise in den Bewertungsbericht aufnehmen oder daraus ausschließen können.

Attribute

In der Tabelle mit den Attributen können Sie sich die Nachweisattribute im Detail ansehen.

In dieser Tabelle können Sie die folgenden Informationen überprüfen:

Name	Description
Attributname	Der Schlüssel für das Attribut.
Wert	Der Wert des Attributs. In einigen Fällen wird ein Link zu einer JSON-Datei mit weiteren Informationen bereitgestellt.

Enthaltene Ressourcen

In der Tabelle „Eingeschlossene Ressourcen“ können Sie sich die Ressourcen ansehen, die für die Erstellung dieser Nachweise bewertet wurden.

In diesem Abschnitt können Sie sich die folgenden Informationen ansehen:

Name	Description
ARN	Der Amazon-Ressourcenname (ARN) der -Ressource. Ein ARN ist möglicherweise nicht für alle Beweisarten verfügbar.
Ressourcen-Compliance	Der Bewertungsstatus für die Ressource. • Für Beweise, die gesammelt wurden AWS Security Hub CSPM, wird das Ergebnis „Bestanden oder nicht bestanden“ direkt vom Security Hub CSPM gemeldet. • Bei Nachweisen, die gesammelt wurden AWS Config, wird das Ergebnis „Konform“ oder „Nicht konform“ direkt von gemeldet. AWS Config • Wenn Nicht zutreffend angezeigt wird, bedeutet dies, dass Sie entweder Security Hub CSPM nicht aktiviert haben AWS Config oder dass die Beweise aus einer anderen Datenquelle stammen.
Wert	Weitere Informationen zur Ressourcenbewertung. In einigen Fällen wird ein Link zu einer JSON-Datei mit weiteren Informationen bereitgestellt.

Weitere Ressourcen

- Lösungen für Probleme mit Nachweisen in Audit Manager finden Sie unterFehlersuche bei der Bewertung und Beweiserhebung.

Eine Bewertung bearbeiten in AWS Audit Manager

Möglicherweise stoßen Sie auf Situationen, in denen Sie Ihre vorhandenen Bewertungen in bearbeiten müssen AWS Audit Manager. Möglicherweise hat sich der Umfang Ihrer Prüfung geändert, sodass die in der Bewertung AWS-Konten enthaltenen Punkte aktualisiert werden müssen. Oder Sie müssen möglicherweise aufgrund personeller Veränderungen die Liste der Prüfungsverantwortlichen, die der Bewertung zugewiesen wurden, überarbeiten. In solchen Fällen können Sie Ihre aktiven Prüfungen bearbeiten und die erforderlichen Anpassungen vornehmen, ohne Ihre Beweiserhebung zu unterbrechen.

Auf der folgenden Seite werden die Schritte beschrieben, mit denen Sie Ihre Prüfungsdetails bearbeiten, AWS-Konten den Umfang ändern, die Prüfungsverantwortlichen aktualisieren und Ihre Änderungen überprüfen und speichern können.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor mindestens eine Bewertung erstellt haben und diese sich im aktiven Status befindet.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Bearbeiten einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Aufgaben

- Schritt 1: Bewertungsdetails bearbeiten
- Schritt 2: Den Umfang bearbeiten AWS-Konten
- Schritt 3: Audit-Inhaber bearbeiten
  - Berechtigungen des Inhabers prüfen
- Schritt 4: Überprüfen und speichern

Schritt 1: Bewertungsdetails bearbeiten

Befolgen Sie diese Schritte, um die Details Ihrer Bewertung zu bearbeiten.

Um eine Bewertung zu bearbeiten

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Bewertungen aus.
3. Wählen Sie eine Bewertung aus und klicken Sie auf Bearbeiten.
4. Bearbeiten Sie unter Bewertungsdetails bearbeiten Ihre Bewertungsdetails nach Bedarf.
5. Wählen Sie Weiter aus.

Schritt 2: Den Umfang bearbeiten AWS-Konten

In diesem Schritt können Sie ändern, welche Konten in Ihrer Bewertung enthalten sind. Audit Manager kann im Rahmen einer Bewertung bis zu 200 Konten und 250 einzelne Mitgliedskonten für alle Bewertungen unterstützen.

Um den Umfang AWS-Konten zu bearbeiten

1. Um einen hinzuzufügen AWS-Konto, aktivieren Sie das Kontrollkästchen neben dem Kontonamen.
2. Um einen zu entfernen AWS-Konto, deaktivieren Sie das Kontrollkästchen neben dem Kontonamen.
3. Wählen Sie Weiter aus.

> **Note**
>
> Informationen zum Bearbeiten des delegierten Administrators für Audit Manager finden Sie unterEinen delegierten Administrator ändern.

Schritt 3: Audit-Inhaber bearbeiten

In diesem Schritt können Sie ändern, welche Prüfungsverantwortlichen in Ihre Bewertung einbezogen werden.

Um die Audit-Verantwortlichen zu bearbeiten

1. Um einen Prüfinhaber hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dem Kontonamen.
2. Um einen Prüfinhaber zu entfernen, deaktivieren Sie das Kontrollkästchen neben dem Kontonamen.
3. Wählen Sie Weiter aus.

Berechtigungen des Inhabers prüfen

Die folgende Richtlinie gilt für alle Prüfungsverantwortlichen einer Bewertung.

Audit Manager *placeholder text* ersetzt die durch Ihre Konto- und Ressourcen-IDs, bevor die Richtlinie angehängt wird.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AuditOwner",
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who are the audit owners of the
 Assessment"
            },
            "Action": [
                "auditmanager:GetAssessment",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAssessmentReportUrl"
            ],
            "Resource": [
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID",
```

```
                "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID/*"
            ]
        }
    ]
}
```

Schritt 4: Überprüfen und speichern

Überprüfen Sie die Informationen für Ihre Bewertung. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten. Wenn Sie mit der Bearbeitung fertig sind, wählen Sie Änderungen speichern.

Nachdem Sie Ihre Änderungen abgeschlossen haben, werden die Änderungen an der Bewertung am darauffolgenden Tag um 00:00 Uhr UTC wirksam.

Nächste Schritte

Wenn Sie keine Nachweise mehr für eine bestimmte Bewertungskontrolle sammeln müssen, können Sie den Status dieser Kontrolle ändern. Detaillierte Anweisungen finden Sie unter Den Status einer Bewertungskontrolle ändern in AWS Audit Manager.

Wenn Sie keine Nachweise mehr für die gesamte Prüfung sammeln müssen, können Sie den Bewertungsstatus auf inaktiv ändern. Detaillierte Anweisungen finden Sie unter Den Status einer Bewertung in inaktiv ändern in AWS Audit Manager.

Weitere Ressourcen

- Lösungen für Bewertungsprobleme in Audit Manager finden Sie unterFehlersuche bei der Bewertung und Beweiserhebung.
- Informationen darüber, warum es nicht mehr möglich ist, Services im Umfang zu bearbeiten, finden Sie Ich kann die Services, die für meine Bewertung gelten, nicht bearbeiten im Abschnitt Problembehandlung dieses Handbuchs.

Manuelle Nachweise hinzufügen in AWS Audit Manager

Audit Manager kann automatisch Beweise für viele Kontrollen sammeln. Für einige Kontrollen sind jedoch möglicherweise Nachweise erforderlich, die nicht automatisch gesammelt werden können. In solchen Fällen können Sie Ihre eigenen Beweise manuell hinzufügen.

Betrachten Sie die folgenden Beispiele:

- Einige Kontrollen beziehen sich auf die Bereitstellung physischer Aufzeichnungen (wie Signaturen) oder auf Ereignisse, die nicht in der Cloud generiert werden (wie Beobachtungen und Interviews). In diesen Fällen können Sie Dateien manuell als Beweismittel hinzufügen. Wenn für eine Kontrolle beispielsweise Informationen über Ihre Organisationsstruktur erforderlich sind, können Sie eine Kopie des Organigramms Ihres Unternehmens als manuellen Beweis hochladen.
- Bei einigen Kontrollen handelt es sich um eine Frage zur Risikobewertung des Lieferanten. Für eine Frage zur Risikobewertung sind möglicherweise Unterlagen als Beweis erforderlich (z. B. ein Organigramm). Oder es ist möglicherweise nur eine einfache Textantwort erforderlich (z. B. eine Liste mit Berufsbezeichnungen). In letzterem Fall können Sie auf die Frage antworten und Ihre Antwort als manuellen Nachweis speichern.

Sie können auch das manuelle Upload-Feature verwenden, um Beweise aus mehreren Umgebungen zu verwalten. Wenn Ihr Unternehmen ein Hybrid-Cloud- oder ein Multi-Cloud-Modell verwendet, können Sie Beweise aus Ihrer lokalen Umgebung, einer in der Cloud gehosteten Umgebung oder Ihren SaaS-Anwendungen hochladen. Auf diese Weise können Sie Ihre Beweise organisieren (unabhängig davon, woher sie stammen), indem Sie sie in der Struktur einer Audit Manager-Bewertung speichern, bei der jeder Beweis einer bestimmten Kontrolle zugeordnet ist.

Wichtige Punkte

Wenn es darum geht, manuelle Nachweise zu Ihren Bewertungen in Audit Manager hinzuzufügen, stehen Ihnen drei Methoden zur Auswahl.

1. Eine Datei aus Amazon S3 importieren — Diese Methode ist ideal, wenn Sie Beweisdateien in einem S3-Bucket gespeichert haben, z. B. Dokumentationen, Berichte oder andere Artefakte, die nicht automatisch von Audit Manager gesammelt werden können. Indem Sie diese Dateien direkt aus S3 importieren, können Sie diese manuellen Beweise nahtlos in die automatisch gesammelten Beweise integrieren.
2. Eine Datei aus Ihrem Browser hochladen — Wenn Sie Nachweisdateien haben, die lokal auf Ihrem Computer oder Netzwerk gespeichert sind, können Sie sie mit dieser Methode manuell in Audit Manager hochladen. Dieser Ansatz ist besonders nützlich, wenn Sie physische Aufzeichnungen

wie gescannte Dokumente oder Bilder einbeziehen müssen, die in Ihrer AWS Umgebung nicht in digitalem Format verfügbar sind.

3. Hinzufügen von Text in freier Form als Nachweis — In einigen Fällen müssen Sie den Nachweis nicht in Form einer Datei, sondern in Form einer Textantwort oder Erklärung vorlegen. Mit dieser Methode können Sie Text in freier Form direkt in Audit Manager eingeben. Dies kann besonders hilfreich sein, wenn Sie Fragen zur Risikobeurteilung von Anbietern beantworten.

Weitere Ressourcen

- Anweisungen zum Hinzufügen manueller Nachweise zu einer Bewertungskontrolle finden Sie in den folgenden Ressourcen. Denken Sie daran, dass Sie jeweils nur eine Methode verwenden können.
  - Manuelle Nachweisdateien aus Amazon S3 importieren
  - Dateien mit manuellen Nachweisen aus Ihrem Browser hochladen
  - Textantworten in freier Form als manuelles Beweismittel eingeben
- Informationen zu den Dateiformaten, die Sie verwenden können, finden Sie unterUnterstützte Dateiformate für manuelle Beweise.
- Weitere Informationen zu den verschiedenen Arten von Nachweisen in Audit Manager finden Sie evidence im Abschnitt Konzepte und Terminologie dieses Handbuchs.
- Unterstützung bei der Problembehebung finden Sie unterIch kann keine manuellen Beweise in eine Kontrolle hochladen.

Manuelle Nachweisdateien aus Amazon S3 importieren

Sie können Nachweisdateien manuell aus einem Amazon S3 S3-Bucket in Ihre Bewertung importieren. Auf diese Weise können Sie die automatisch gesammelten Beweise durch zusätzliches unterstützendes Material ergänzen.

Voraussetzungen

- Die maximal unterstützte Größe für eine einzelne Datei mit manuellen Beweisen beträgt 100 MB.
- Sie müssen einen der verwendenUnterstützte Dateiformate für manuelle Beweise.
- Jeder AWS-Konto kann täglich bis zu 100 Beweisdateien manuell auf eine Kontrolle hochladen. Eine Überschreitung dieses täglichen Kontingents führt dazu, dass alle zusätzlichen manuellen

Uploads für diese Kontrolle fehlschlagen. Wenn Sie eine große Menge manueller Beweise auf eine einzelne Kontrolle hochladen müssen, laden Sie Ihre Beweise stapelweise über mehrere Tage hinweg hoch.

- Wenn eine Kontrolle inaktiv ist, können Sie dieser Kontrolle keine manuellen Beweise hinzufügen. Um manuelle Nachweise hinzuzufügen, müssen Sie zunächst den Kontrollstatus auf Wird geprüft oder geprüft ändern.
- Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen für die Verwaltung einer Bewertung in AWS Audit Manager verfügt. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können eine Datei mit der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) importieren.

AWS console

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel zu importieren. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

So importieren Sie eine Datei aus S3 auf der Audit Manager Manager-Konsole

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Assessments und anschließend ein Assessment aus.
3. Wählen Sie die Registerkarte „Steuerelemente“, scrollen Sie nach unten zu „Kontrollsätze“ und wählen Sie dann ein Steuerelement aus.
4. Wählen Sie auf der Registerkarte Beweisordner die Option Manuelle Beweise hinzufügen und dann Datei aus S3 importieren aus.

5. Geben Sie auf der nächsten Seite die S3-URI der Beweise ein. Sie finden den S3-URI, indem Sie in der Amazon-S3-Konsole zu dem Objekt navigieren und S3-URI kopieren auswählen.
6. Klicken Sie auf Upload.

AWS CLI

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel zu importieren. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Ersetzen Sie die im folgenden Verfahren *placeholder text* durch Ihre eigenen Informationen.

Um eine Datei aus S3 zu importieren, AWS CLI

1. Führen Sie den `list-assessments`-Befehl aus, um eine Liste Ihrer Bewertungen anzuzeigen.

   ```
   aws auditmanager list-assessments
   ```

   Suchen Sie in der Antwort nach der Bewertung, zu der Sie Beweise hochladen möchten, und notieren Sie sich die Bewertungs-ID.
2. Führen Sie den `get-assessment`-Befehl aus und geben Sie die Bewertungs-ID aus Schritt eins an.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   Suchen Sie in der Antwort den Kontrollsatz und das Steuerelement, für das Sie Beweise hochladen möchten, und notieren Sie sich deren IDs.
3. Verwenden Sie den `batch-import-evidence-to-assessment-control`-Befehl mit den folgenden Parametern:

   - `--assessment-id`– Verwenden Sie die Bewertungs-ID aus Schritt eins.

- `--control-set-id`– Verwenden Sie die Kontrollsatz-ID aus Schritt zwei.
- `--control-id`– Verwenden Sie die Kontroll-ID aus Schritt zwei.
- `--manual-evidence`– Verwenden Sie `s3ResourcePath` als den manuellen Beweistyp und geben Sie den S3-URI des Beweises an. Sie finden den S3-URI, indem Sie in der Amazon-S3-Konsole zu dem Objekt navigieren und S3-URI kopieren auswählen.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
amzn-s3-demo-bucket/EXAMPLE-FILE.extension
```

Audit Manager API

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel zu importieren. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Um eine Datei mit der API aus S3 zu importieren

1. Rufen Sie den `ListAssessments`-Vorgang auf, um eine Liste Ihrer Bewertungen einzusehen. Suchen Sie in der Antwort nach der Bewertung, zu der Sie Beweise hochladen möchten, und notieren Sie sich die Bewertungs-ID.
2. Rufen Sie den `GetAssessment`-Vorgang auf und geben Sie die Bewertungs-ID aus Schritt eins an. Suchen Sie in der Antwort nach dem Kontrollsatz und dem Steuerelement, für das Sie Beweise hochladen möchten, und notieren Sie sich diese IDs.
3. Rufen Sie die `BatchImportEvidenceToAssessmentControl`-Operation mit folgenden Parametern auf:
   - `assessmentId`– Verwenden Sie die Bewertungs-ID aus Schritt eins.
   - `controlSetId`– Verwenden Sie die Kontrollsatz-ID aus Schritt zwei.
   - `controlId`– Verwenden Sie die Kontroll-ID aus Schritt zwei.

- `manualEvidence`– Verwenden Sie `s3ResourcePath` als den manuellen Beweistyp und geben Sie den S3-URI des Beweises an. Sie finden den S3-URI, indem Sie in der Amazon-S3-Konsole zu dem Objekt navigieren und S3-URI kopieren auswählen.

Weitere Informationen erhalten Sie, indem Sie auf einen der Links im vorherigen Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Nachdem Sie die Nachweise für Ihre Bewertung hinzugefügt und überprüft haben, können Sie einen Bewertungsbericht erstellen. Weitere Informationen finden Sie unter Erstellung eines Bewertungsberichts in AWS Audit Manager.

Weitere Ressourcen

Informationen zu den Dateiformaten, die Sie verwenden können, finden Sie unterUnterstützte Dateiformate für manuelle Beweise.

Dateien mit manuellen Nachweisen aus Ihrem Browser hochladen

Sie können Nachweisdateien manuell von Ihrem Browser in Ihre Audit Manager Manager-Bewertung hochladen. Auf diese Weise können Sie die automatisch gesammelten Nachweise durch zusätzliches unterstützendes Material ergänzen.

Voraussetzungen

- Die maximal unterstützte Größe für eine einzelne Datei mit manuellen Beweisen beträgt 100 MB.
- Sie müssen einen der verwendenUnterstützte Dateiformate für manuelle Beweise.
- Jeder AWS-Konto kann täglich bis zu 100 Beweisdateien manuell auf eine Kontrolle hochladen. Eine Überschreitung dieses täglichen Kontingents führt dazu, dass alle zusätzlichen manuellen Uploads für diese Kontrolle fehlschlagen. Wenn Sie eine große Menge manueller Beweise auf eine einzelne Kontrolle hochladen müssen, laden Sie Ihre Beweise stapelweise über mehrere Tage hinweg hoch.

- Wenn eine Kontrolle inaktiv ist, können Sie dieser Kontrolle keine manuellen Beweise hinzufügen. Um manuelle Nachweise hinzuzufügen, müssen Sie zunächst den Kontrollstatus auf Wird geprüft oder geprüft ändern.
- Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen für die Verwaltung einer Bewertung in AWS Audit Manager verfügt. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können eine Datei über die Audit Manager Manager-Konsole, die Audit Manager Manager-API oder die AWS Command Line Interface (AWS CLI) hochladen.

AWS console

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel hochzuladen. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Um eine Datei von Ihrem Browser auf die Audit Manager Manager-Konsole hochzuladen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Assessments und anschließend ein Assessment aus.
3. Scrollen Sie auf der Registerkarte Steuerelemente nach unten zu Kontrollgruppen und wählen Sie dann ein Steuerelement aus.
4. Wählen Sie auf der Registerkarte Nachweisordner die Option Manuelle Beweise hinzufügen aus.
5. Wählen Sie Datei aus Browser hochladen aus.
6. Wählen Sie die Datei aus, die Sie hochladen möchten.
7. Klicken Sie auf Upload.

AWS CLI

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel hochzuladen. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Ersetzen Sie die im folgenden Verfahren *placeholder text* durch Ihre eigenen Informationen.

Um eine Datei aus Ihrem Browser hochzuladen AWS CLI

1. Führen Sie den `list-assessments`-Befehl aus, um eine Liste Ihrer Bewertungen anzuzeigen.

   ```
   aws auditmanager list-assessments
   ```

   Suchen Sie in der Antwort nach der Bewertung, zu der Sie Beweise hochladen möchten, und notieren Sie sich die Bewertungs-ID.

2. Führen Sie den `get-assessment`-Befehl aus und geben Sie die Bewertungs-ID aus Schritt eins an.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   Suchen Sie in der Antwort den Kontrollsatz und das Steuerelement, für das Sie Beweise hochladen möchten, und notieren Sie sich deren IDs.

3. Führen Sie den `get-evidence-file-upload-url`-Befehl aus und geben Sie die Datei an, die Sie hochladen möchten.

   ```
   aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
   ```

   Notieren Sie sich in der Antwort die vorsignierte URL und die`evidenceFileName`.

4. Verwenden Sie die vorsignierte URL aus Schritt drei, um die Datei aus Ihrem Browser hochzuladen. Diese Aktion lädt Ihre Datei in Amazon S3 hoch, wo sie als Objekt gespeichert

wird, das an eine Bewertungskontrolle angehängt werden kann. Im folgenden Schritt verweisen Sie mithilfe des `evidenceFileName`-Parameters auf das neu erstellte Objekt.

> **Note**
>
> Wenn Sie eine Datei mit einer vorsignierten URL hochladen, schützt und speichert Audit Manager Ihre Daten mithilfe der serverseitigen Verschlüsselung mit AWS Key Management Service. Um dies zu unterstützen, müssen Sie den `x-amz-server-side-encryption`-Header in Ihrer Anfrage verwenden, wenn Sie die vorsignierte URL zum Hochladen Ihrer Datei verwenden.
> Wenn Sie einen Kunden verwenden, der AWS KMS key in Ihren Audit Manager Konfiguration Ihrer Datenverschlüsselungseinstellungen Manager-Einstellungen verwaltet wird, stellen Sie sicher, dass Sie auch den `x-amz-server-side-encryption-aws-kms-key-id` Header in Ihre Anfrage aufnehmen. Wenn der `x-amz-server-side-encryption-aws-kms-key-id`-Header in der Anforderung nicht vorhanden ist, geht Amazon S3 davon aus, dass Sie den Von AWS verwalteter Schlüssel verwenden möchten.
> Weitere Informationen finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung mit AWS Key Management Service Schlüsseln (SSE-KMS) im Amazon Simple Storage Service-Benutzerhandbuch.

5. Verwenden Sie den `batch-import-evidence-to-assessment-control`-Befehl mit den folgenden Parametern:

   - `--assessment-id`– Verwenden Sie die Bewertungs-ID aus Schritt eins.
   - `--control-set-id`– Verwenden Sie die Kontrollsatz-ID aus Schritt zwei.
   - `--control-id`– Verwenden Sie die Kontroll-ID aus Schritt zwei.
   - `--manual-evidence`– Verwenden Sie `evidenceFileName` als den manuellen Beweistyp und geben Sie den Namen der Beweisdatei aus Schritt drei an.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel hochzuladen. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Um eine Datei mithilfe der API von Ihrem Browser hochzuladen

1. Aufrufen der `ListAssessments`-Operation. Suchen Sie in der Antwort nach der Bewertung, zu der Sie Beweise hochladen möchten, und notieren Sie sich die Bewertungs-ID.
2. Rufen Sie den `GetAssessment`-Vorgang auf und geben Sie den `assessmentId` ab Schritt eins an. Suchen Sie in der Antwort den Kontrollsatz und das Steuerelement, für das Sie Beweise hochladen möchten, und notieren Sie sich diese IDs.
3. Rufen Sie den `GetEvidenceFileUploadUrl`-Vorgang auf und geben Sie den `fileName` an, den Sie hochladen möchten. Notieren Sie sich in der Antwort die vorsignierte URL und die`evidenceFileName`.
4. Verwenden Sie die vorsignierte URL aus Schritt drei, um die Datei aus Ihrem Browser hochzuladen. Diese Aktion lädt Ihre Datei in Amazon S3 hoch, wo sie als Objekt gespeichert wird, das an eine Bewertungskontrolle angehängt werden kann. Im folgenden Schritt verweisen Sie mithilfe des `evidenceFileName`-Parameters auf das neu erstellte Objekt.

   > **Note**
   >
   > Wenn Sie eine Datei mit einer vorsignierten URL hochladen, schützt und speichert Audit Manager Ihre Daten mithilfe der serverseitigen Verschlüsselung mit AWS Key Management Service. Um dies zu unterstützen, müssen Sie den `x-amz-server-side-encryption`-Header in Ihrer Anfrage verwenden, wenn Sie die vorsignierte URL zum Hochladen Ihrer Datei verwenden.
   > Wenn Sie einen Kunden verwenden, der AWS KMS key in Ihren Audit Manager Konfiguration Ihrer Datenverschlüsselungseinstellungen Manager-Einstellungen verwaltet wird, stellen Sie sicher, dass Sie auch den `x-amz-server-side-encryption-aws-kms-key-id` Header in Ihre Anfrage aufnehmen. Wenn der `x-amz-server-side-encryption-aws-kms-key-id`-Header in der Anforderung

nicht vorhanden ist, geht Amazon S3 davon aus, dass Sie den Von AWS verwalteter Schlüssel verwenden möchten.
Weitere Informationen finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung mit AWS Key Management Service Schlüsseln (SSE-KMS) im Amazon Simple Storage Service-Benutzerhandbuch.

5. Rufen Sie die `BatchImportEvidenceToAssessmentControl`-Operation mit folgenden Parametern auf:

   - `assessmentId`– Verwenden Sie die Bewertungs-ID aus Schritt eins.
   - `controlSetId`– Verwenden Sie die Kontrollsatz-ID aus Schritt zwei.
   - `controlId`– Verwenden Sie die Kontroll-ID aus Schritt zwei.
   - `manualEvidence`– Verwenden Sie `evidenceFileName` als den manuellen Beweistyp und geben Sie den Namen der Beweisdatei aus Schritt drei an.

Für weitere Informationen klicken Sie auf einen der Links im vorherigen Verfahren, um mehr in der AWS Audit Manager API-Referenz zu lesen. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Nachdem Sie die Nachweise für Ihre Bewertung gesammelt und geprüft haben, können Sie einen Bewertungsbericht erstellen. Weitere Informationen finden Sie unter Erstellung eines Bewertungsberichts in AWS Audit Manager.

Weitere Ressourcen

Informationen zu den Dateiformaten, die Sie verwenden können, finden Sie unterUnterstützte Dateiformate für manuelle Beweise.

Textantworten in freier Form als manuelles Beweismittel eingeben

Sie können zusätzliche Kontext- und Zusatzinformationen für eine Bewertungskontrolle bereitstellen, indem Sie Text in freier Form eingeben und diesen Text als Nachweis speichern. Auf diese Weise können Sie Details, die nicht im Rahmen der automatischen Beweiserhebung erfasst wurden, manuell dokumentieren.

Beispielsweise können Sie Audit Manager verwenden, um benutzerdefinierte Kontrollen zu erstellen, die Fragen in einem Fragebogen zur Lieferantenrisikobewertung darstellen. In diesem Fall ist der Name jeder Kontrolle eine spezifische Frage, die nach Informationen über den Sicherheits- und Compliance-Status Ihres Unternehmens fragt. Um Ihre Antwort auf eine bestimmte Frage zur Risikobeurteilung eines Anbieters aufzuzeichnen, können Sie eine Textantwort eingeben und diese als manuellen Nachweis für die Kontrolle speichern.

Voraussetzungen

- Wenn eine Kontrolle inaktiv ist, können Sie dieser Kontrolle keine manuellen Beweise hinzufügen. Um manuelle Nachweise hinzuzufügen, müssen Sie zunächst den Status der Kontrolle entweder auf Wird geprüft oder Geprüft ändern.
- Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen für die Verwaltung einer Bewertung in AWS Audit Manager verfügt. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können Textantworten über die Audit Manager Manager-Konsole, die Audit Manager Manager-API oder die AWS Command Line Interface (AWS CLI) eingeben.

AWS console

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel einzugeben. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Um eine Textantwort in der Audit Manager Manager-Konsole einzugeben

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Assessments und anschließend ein Assessment aus.

3. Wählen Sie die Registerkarte „Steuerelemente“, scrollen Sie nach unten zu „Kontrollsätze“ und wählen Sie dann ein Steuerelement aus.
4. Wählen Sie auf der Registerkarte Nachweisordner die Option Manuelle Beweise hinzufügen aus.
5. Wählen Sie Textantwort eingeben.
6. Geben Sie in dem daraufhin angezeigten Popup-Fenster Ihre Antwort im Klartextformat ein.
7. Wählen Sie Bestätigen aus.

AWS CLI

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel einzugeben. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Ersetzen Sie die im folgenden Verfahren *placeholder text* durch Ihre eigenen Informationen.

Um eine Textantwort in das Feld einzugeben AWS CLI

1. Führen Sie den Befehl `list-assessments` aus.

   ```
   aws auditmanager list-assessments
   ```

   Suchen Sie in der Antwort nach der Bewertung, zu der Sie Beweise hochladen möchten, und notieren Sie sich die Bewertungs-ID.
2. Führen Sie den `get-assessment`-Befehl aus und geben Sie die Bewertungs-ID aus Schritt eins an.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   Suchen Sie in der Antwort nach dem Kontrollsatz und der Kontrolle, für die Sie Beweise hochladen möchten, und notieren Sie sich deren IDs.

3. Verwenden Sie den `batch-import-evidence-to-assessment-control`-Befehl mit den folgenden Parametern:

   - `--assessment-id`– Verwenden Sie die Bewertungs-ID aus Schritt eins.
   - `--control-set-id`– Verwenden Sie die Kontrollsatz-ID aus Schritt zwei.
   - `--control-id`– Verwenden Sie die Kontroll-ID aus Schritt zwei.
   - `--manual-evidence`– Verwenden Sie `textResponse` als manuellen Beweistyp und geben Sie den Text ein, den Sie als manuellen Beweis speichern möchten.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

> **Important**
>
> Wir empfehlen dringend, niemals sensible oder persönlich identifizierbare Informationen (PII) als manuelles Beweismittel einzugeben. Dazu gehören unter anderem Sozialversicherungsnummern, Adressen, Telefonnummern oder andere Informationen, die zur Identifizierung einer Person verwendet werden könnten.

Um eine Textantwort über die API einzugeben

1. Aufrufen der `ListAssessments`-Operation. Suchen Sie in der Antwort nach der Bewertung, zu der Sie Beweise hochladen möchten, und notieren Sie sich die Bewertungs-ID.
2. Rufen Sie den `GetAssessment`-Vorgang auf und geben Sie den `assessmentId` ab Schritt eins an. Suchen Sie in der Antwort nach dem Kontrollsatz und der Kontrolle, für die Sie Beweise hochladen möchten, und notieren Sie sich diese IDs.
3. Rufen Sie die `BatchImportEvidenceToAssessmentControl`-Operation mit folgenden Parametern auf:

   - `assessmentId`– Verwenden Sie die Bewertungs-ID aus Schritt eins.
   - `controlSetId`– Verwenden Sie die Kontrollsatz-ID aus Schritt zwei.

- `controlId`– Verwenden Sie die Kontroll-ID aus Schritt zwei.
- `manualEvidence`– Verwenden Sie `textResponse` als manuellen Beweistyp und geben Sie den Text ein, den Sie als manuellen Beweis speichern möchten.

Weitere Informationen erhalten Sie, indem Sie auf einen der Links im vorherigen Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Nachdem Sie die Nachweise für Ihre Bewertung gesammelt und geprüft haben, können Sie einen Bewertungsbericht erstellen. Weitere Informationen finden Sie unter Erstellung eines Bewertungsberichts in AWS Audit Manager.

Unterstützte Dateiformate für manuelle Beweise

In der folgenden Liste werden die Arten von Dateien aufgeführt und beschrieben, die Sie als manuellen Beweis hochladen können. Für jeden Dateityp sind in der Tabelle auch die unterstützten Dateierweiterungen aufgeführt.

Dateityp	Description	Unterstützte Dateierweiterungen
Komprimierung oder Archivieren	GNU-Zip-komprimierte Archive und ZIP-komprimierte Archive	`.gz`, `.zip`
Dokument	Allgemeine Dokumentdateien wie PDFs Microsoft Office-Dateien	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Image	Bild- und Grafikdateien	`.jpeg`, `.jpg`, `.png`, `.svg`
Text	Andere nicht-binäre Textdateien, wie Klartext-	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Dateityp	Description	Unterstützte Dateierweiterungen
	Dokumente und Markup-Sprachdateien	

Weitere Ressourcen

Auf den folgenden Seiten erfahren Sie mehr über die verschiedenen Möglichkeiten, wie Sie Ihre eigenen Nachweise zu einer Bewertungskontrolle hinzufügen können.

- Manuelle Nachweisdateien aus Amazon S3 importieren
- Dateien mit manuellen Nachweisen aus Ihrem Browser hochladen
- Textantworten in freier Form als manuelles Beweismittel eingeben

Erstellung eines Bewertungsberichts in AWS Audit Manager

Nachdem Sie die Beweise für Ihre Bewertung gesammelt und geprüft haben, können Sie einen Bewertungsbericht erstellen. Ein Bewertungsbericht fasst Ihre Bewertung zusammen und enthält Links zu einer Reihe von Ordnern, die die entsprechenden Nachweise enthalten.

Wichtige Punkte

Neu gesammelte Nachweise erscheinen nicht automatisch in einem Bewertungsbericht. Das bedeutet, dass Sie kontrollieren können, welche Beweise Sie in den Bericht aufnehmen möchten. Nachdem Sie die Nachweise ausgewählt haben, die Sie aufnehmen möchten, können Sie den abschließenden Bewertungsbericht erstellen, den Sie Ihren Prüfern zur Verfügung stellen können.

Wenn Sie einen Bewertungsbericht erstellen, wird er in dem S3-Bucket platziert, den Sie als Ziel für Ihren Bewertungsbericht ausgewählt haben. Sie können den Bewertungsbericht auch vom Download-Center in Audit Manager herunterladen.

Weitere Ressourcen

Weitere Informationen zu Bewertungsberichten und deren Verwaltung finden Sie in den folgenden Ressourcen.

- Hinzufügen von Beweisen zu einem Bewertungsbericht

- Beweise aus einem Bewertungsbericht entfernen
- Generieren eines Bewertungsberichts
- Einen Bewertungsbericht herunterladen
- In einem Bewertungsbericht navigieren und sich mit seinem Inhalt vertraut machen
- Validierung eines Bewertungsberichts
- Löschen eines Bewertungsberichts
- Generierung von Bewertungsberichten anhand der Suchergebnisse Ihres Evidence Finders
- Konfiguration Ihres Standardziels für Bewertungsberichte
- Behebung von Bewertungsberichtfehlern

Hinzufügen von Beweisen zu einem Bewertungsbericht

Bevor Sie einen Bewertungsbericht erstellen können, müssen Sie Ihrem Bewertungsbericht mindestens einen Beweis hinzufügen. Sie können entweder einen ganzen Beweisordner hinzufügen, oder Sie können bestimmte Nachweiselemente aus einem Ordner hinzufügen.

Verfahren

Gehen Sie wie folgt vor, um Beweise in einen Bewertungsbericht aufzunehmen.

Um Beweise zu einem Bewertungsbericht hinzuzufügen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Assessments und anschließend ein Assessment aus.
3. Scrollen Sie auf der Registerkarte Kontrollen nach unten zur Tabelle Kontrollsätze und wählen Sie ein Steuerelement mit Nachweisen aus, das Sie in den Bewertungsbericht aufnehmen möchten.
4. Wählen Sie aus, wie Sie Ihrem Bewertungsbericht Beweise hinzufügen möchten.

    a. Um einen ganzen Beweisordner hinzuzufügen, scrollen Sie nach unten zu den Beweisordnern, wählen Sie den Ordner aus, den Sie hinzufügen möchten, und klicken Sie dann auf Zum Bewertungsbericht hinzufügen.

> **Tip**
>
> Wenn Sie den Ordner, nach dem Sie suchen, nicht sehen können, ändern Sie den Dropdownfilter auf Alle Zeiten. Andernfalls werden standardmäßig die Ordner der letzten sieben Tage angezeigt.
> Wenn Zum Bewertungsbericht hinzufügen ausgegraut ist, wurde der Beweisordner bereits zum Bewertungsbericht hinzugefügt.

b. Um bestimmte Beweise hinzuzufügen, wählen Sie einen Beweisordner aus, um dessen Inhalt zu öffnen. Wählen Sie ein oder mehrere Elemente aus der Liste aus und klicken Sie dann auf Zum Bewertungsbericht hinzufügen.

> **Tip**
>
> Wenn Zum Bewertungsbericht hinzufügen ausgegraut ist, stellen Sie sicher, dass Sie das Kontrollkästchen neben den Beweisen aktiviert haben, und versuchen Sie es dann erneut.

5. Nachdem Sie die Beweise zum Bewertungsbericht hinzugefügt haben, wird ein grünes Erfolgsbanner angezeigt. Wählen Sie Beweise im Bewertungsbericht anzeigen, um die Beweise zu sehen, die in Ihrem Bewertungsbericht enthalten sein werden.
   - Alternativ können Sie sich die Beweise anzeigen lassen, die in Ihrem Bewertungsbericht enthalten sein werden, indem Sie zu Ihrer Bewertung zurückkehren und die Registerkarte Auswahl des Bewertungsberichts auswählen.

Nächste Schritte

Informationen dazu, wie Sie Beweise aus einem Bewertungsbericht entfernen müssen, finden Sie unterBeweise aus einem Bewertungsbericht entfernen.

Wenn Sie bereit sind, einen Bewertungsbericht zu erstellen, finden Sie weitere Informationen unterGenerieren eines Bewertungsberichts.

Weitere Ressourcen

Antworten auf häufig gestellte Fragen und Probleme finden Sie Behebung von Bewertungsberichtfehlern im Abschnitt zur Fehlerbehebung in diesem Handbuch.

Beweise aus einem Bewertungsbericht entfernen

Gehen Sie wie folgt vor, wenn Sie Beweise aus einem Bewertungsbericht entfernen müssen. Sie können entweder einen ganzen Beweisordner entfernen, oder Sie können bestimmte Beweiselemente aus einem Ordner entfernen.

Verfahren

Um Beweise aus einem Bewertungsbericht zu entfernen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Bewertungen und dann den Namen der Bewertung aus, um sie zu öffnen.
3. Scrollen Sie auf der Registerkarte Kontrollen nach unten zur Tabelle Kontrollsätze und wählen Sie den Namen einer Kontrolle aus, um sie zu öffnen.
4. Wählen Sie aus, wie Sie Beweise aus Ihrem Bewertungsbericht entfernen möchten.

   a. Um einen ganzen Beweisordner zu entfernen, scrollen Sie nach unten zu den Beweisordnern, wählen Sie den Ordner aus, den Sie entfernen möchten, und wählen Sie dann Aus Bewertungsbericht entfernen aus.

   > **Tip**
   >
   > Wenn Sie den Ordner, nach dem Sie suchen, nicht sehen können, ändern Sie den Dropdownfilter auf Alle Zeiten. Andernfalls werden standardmäßig die Ordner der letzten sieben Tage angezeigt.
   > Wenn Aus Bewertungsbericht entfernen ausgegraut ist, wurde der Beweisordner bereits aus dem Bewertungsbericht entfernt.

   b. Um bestimmte Beweise zu entfernen, wählen Sie einen Beweisordner aus, um dessen Inhalt zu öffnen. Wählen Sie ein oder mehrere Elemente aus der Liste aus und klicken Sie dann auf Aus dem Bewertungsbericht entfernen.

> **Tip**
>
> Wenn Aus Bewertungsbericht entfernen ausgegraut ist, stellen Sie sicher, dass Sie das Kontrollkästchen neben den Beweisen aktiviert haben, und versuchen Sie es dann erneut.

5. Nachdem Sie die Beweise zum Bewertungsbericht hinzugefügt haben, wird ein grünes Erfolgsbanner angezeigt. Wählen Sie Beweise im Bewertungsbericht anzeigen, um die Beweise zu sehen, die in Ihrem Bewertungsbericht enthalten sein werden.
   - Alternativ können Sie sich die Beweise anzeigen lassen, die in Ihrem Bewertungsbericht enthalten sein werden, indem Sie zu Ihrer Bewertung zurückkehren und die Registerkarte Auswahl des Bewertungsberichts auswählen.

Nächste Schritte

Wenn Sie bereit sind, einen Bewertungsbericht zu erstellen, finden Sie weitere Informationen unterGenerieren eines Bewertungsberichts.

Weitere Ressourcen

Antworten auf häufig gestellte Fragen und Probleme finden Sie Behebung von Bewertungsberichtfehlern im Abschnitt zur Fehlerbehebung in diesem Handbuch.

Generieren eines Bewertungsberichts

Wenn Sie bereit sind, Ihren Bewertungsbericht zu erstellen, gehen Sie wie folgt vor.

Voraussetzungen

Bevor Sie einen Bewertungsbericht erstellen können, müssen Sie Ihrem Bewertungsbericht mindestens einen Beweis hinzufügen. Sie können entweder einen ganzen Beweisordner hinzufügen, oder Sie können einzelne Beweiselemente innerhalb eines Ordners hinzufügen.

Um sicherzustellen, dass Ihr Bewertungsbericht erfolgreich erstellt wurde, lesen Sie unseren Konfigurationstipps für das Ziel Ihres Bewertungsberichts.

Verfahren

Erstellen Sie einen Bewertungsbericht wie folgt:

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Bewertungen aus.
3. Wählen Sie den Namen der Bewertung aus, für die Sie einen Bewertungsbericht erstellen möchten.
4. Wählen Sie die Registerkarte Auswahl des Bewertungsberichts und anschließend Bewertungsbericht erstellen.

   > **Tip**
   >
   > Wenn die Option Bewertungsbericht erstellen ausgegraut ist, bedeutet dies, dass dem Bewertungsbericht noch keine Beweise hinzugefügt wurden.

5. Geben Sie im Popup-Fenster einen Namen und eine Beschreibung für den Bewertungsbericht ein und überprüfen Sie die Details des Bewertungsberichts.
6. Wählen Sie Bewertungsbericht erstellen und warten Sie einige Minuten, bis Ihr Bewertungsbericht generiert ist.
7. Suchen Sie Ihren Bewertungsbericht auf der Seite Download Center der Audit Manager-Konsole und laden Sie ihn herunter.
   - Sie können auch zu Ihrem Ziel-S3-Bucket für den Bewertungsbericht wechseln und den Bewertungsbericht von dort herunterladen.

Nächste Schritte

Nachdem Sie einen Bewertungsbericht erstellt haben, erfahren Sie mehr über Folgendes:

- Finden Sie Ihren Bewertungsbericht und laden Sie ihn herunter – Erfahren Sie, wie Sie Ihren Bewertungsbericht vom Download-Center oder von Amazon S3 herunterladen können.
- Erkunden Sie Ihren Bewertungsbericht – Erfahren Sie, wie Sie sich in einem Bewertungsbericht zurechtfinden und dessen Inhalt erkunden.

- Überprüfen Sie Ihren Bewertungsbericht — Erfahren Sie, wie Sie den ValidateAssessmentReportIntegrityAPI-Vorgang zur Validierung Ihres Bewertungsberichts verwenden können.
- Löschen eines unerwünschten Bewertungsberichts – Erfahren Sie, wie Sie einen unerwünschten Bericht aus dem Download-Center oder aus Amazon S3 löschen können.
- Erstellen Sie Bewertungsberichte mit Evidence Finder — Erfahren Sie, wie Sie anhand Ihrer Evidence Finder-Suchergebnisse Bewertungsberichte erstellen können.

Weitere Ressourcen

Antworten auf häufig gestellte Fragen und Probleme finden Sie Behebung von Bewertungsberichtfehlern im Abschnitt zur Fehlerbehebung in diesem Handbuch.

Den Status einer Bewertungskontrolle ändern in AWS Audit Manager

Sie können den Status einer Bewertungskontrolle innerhalb Ihrer aktiven Bewertung ändern. Wenn Sie den Status einer Kontrolle aktualisieren, können Sie deren Fortschritt verfolgen und angeben, wann Sie sie überprüft haben. So bleibt Ihre Bewertung übersichtlich und übersichtlich up-to-date.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor eine Bewertung erstellt haben und dass ihr aktueller Status aktiv ist.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen für die Verwaltung einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können den Status einer Bewertungskontrolle mithilfe der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) aktualisieren.

> **Note**
>
> Die Änderung eines Kontrollstatus in Überprüft ist endgültig. Nachdem Sie den Status einer Kontrolle auf Überprüft gesetzt haben, können Sie den Status dieser Kontrolle nicht mehr ändern oder zu einem früheren Status zurückkehren.

Audit Manager console

So ändern Sie den Status einer Bewertungskontrolle in der Audit Manager Manager-Konsole

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Bewertungen aus.
3. Wählen Sie den Namen der Bewertung, um sie zu öffnen.
4. Wählen Sie auf der Bewertungsseite die Registerkarte Kontrollen aus, scrollen Sie nach unten zur Tabelle Kontrollsätze und wählen Sie dann den Namen einer Kontrolle aus, um es zu öffnen.
5. Wählen Sie oben rechts auf der Seite die Option Kontrollstatus aktualisieren und wählen Sie dann einen Status aus:

Status	Description
Wird geprüft	Wählen Sie diesen Status, wenn Sie die Kontrolle noch nicht überprüft haben.
Überprüft	Wählen Sie diesen Status, wenn Sie die Überprüfung der Nachweise für diese Kontrolle abgeschlossen haben und mit dem Sammeln oder Hinzufügen von Nachweisen fortfahren möchten.
Inaktiv	Wählen Sie diesen Status, wenn Sie die automatische Erfassung von Nachweisen für diese Kontrolle beenden möchten.

6. Wählen Sie Kontrollstatus aktualisieren, um Ihre Auswahl zu bestätigen.

AWS CLI

Um den Status einer Bewertungskontrolle in der AWS CLI

1. Führen Sie den Befehl list-assessments aus.

```
aws auditmanager list-assessments
```

   Die Antwort gibt eine Liste von Bewertungen zurück. Suchen Sie die Bewertung, die das Steuerelement enthält, das Sie aktualisieren möchten, und notieren Sie sich die Bewertungs-ID.

2. Führen Sie den Befehl get-assessment aus und geben Sie die Bewertungs-ID aus Schritt 1 an.

   Ersetzen Sie im folgenden Beispiel die *placeholder text* durch Ihre eigenen Informationen.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
```

   Suchen Sie in der Antwort das Steuerelement, das Sie aktualisieren möchten, und notieren Sie sich die Steuerelement-ID und die zugehörige Kontrollsatz-ID.

3. Führen Sie den update-assessment-controlBefehl aus und geben Sie die folgenden Parameter an:

   - `--assessment-id`— Die Bewertung, zu der die Kontrolle gehört.
   - `--control-set-id`— Der Kontrollsatz, zu dem das Steuerelement gehört.
   - `--control-id`— Das Steuerelement, das Sie aktualisieren möchten.
   - `--control-status`— Setzen Sie diesen Wert auf`UNDER_REVIEW`,`REVIEWED`, oder`INACTIVE`.

   Ersetzen Sie im folgenden Beispiel die *placeholder text* durch Ihre eigenen Informationen.

```
aws auditmanager update-assessment-control --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --
control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
```

Audit Manager API

Um den Status einer Bewertungskontrolle mithilfe der API zu ändern

1. Verwenden Sie die ListAssessmentsOperation.

   Suchen Sie in der Antwort nach der Bewertung, die das Steuerelement enthält, das Sie aktualisieren möchten, und notieren Sie sich die Bewertungs-ID.

2. Verwenden Sie den GetAssessmentVorgang und geben Sie die Bewertungs-ID aus Schritt 1 an.

   Suchen Sie in der Antwort das Steuerelement, das Sie aktualisieren möchten, und notieren Sie sich die Kontroll-ID und die zugehörige Kontrollsatz-ID.

3. Verwenden Sie die UpdateAssessmentControlOperation und geben Sie die folgenden Parameter an:

   - `assessmentId`— Die Bewertung, zu der die Kontrolle gehört.
   - `controlSetId`— Der Kontrollsatz, zu dem das Steuerelement gehört.
   - `controlId`— Das Steuerelement, das Sie aktualisieren möchten.
   - `controlStatus`— Setzen Sie diesen Wert auf `UNDER_REVIEWREVIEWED`, oder`INACTIVE`.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, indem Sie einen der Links im vorherigen Verfahren auswählen, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Wenn Sie bereit sind, den Status der Bewertung zu ändern, finden Sie unter. Den Status einer Bewertung in inaktiv ändern in AWS Audit Manager

Den Status einer Bewertung in inaktiv ändern in AWS Audit Manager

Wenn Sie für eine Bewertung keine Nachweise mehr erfassen müssen, können Sie den Bewertungsstatus in Inaktiv ändern. Wenn sich der Status einer Bewertung zu inaktiv ändert, werden bei der Bewertung keine Nachweise mehr erfasst. Infolgedessen fallen für diese Bewertung keine Gebühren mehr an.

Audit Manager stoppt nicht nur die Beweiserhebung, sondern nimmt auch die folgenden Änderungen an den Kontrollen vor, die Teil der inaktiven Bewertung sind:

- Alle Kontrollsätze wechseln in den Status Überprüft.
- Alle Kontrollen, die den Status Wird geprüft haben, wechseln in den Status Überprüft.
- Delegierte für die inaktive Bewertung können die zugehörigen Kontrollen und Kontrollsätze nicht mehr anzeigen oder bearbeiten.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor eine Bewertung erstellt haben und dass ihr aktueller Status aktiv ist.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen für die Verwaltung einer Bewertung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können einen Bewertungsstatus mithilfe der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) aktualisieren.

> **Warning**
>
> Diese Aktion ist unumkehrbar. Wir empfehlen Ihnen, vorsichtig vorzugehen und sicherzustellen, dass Sie Ihre Bewertung als inaktiv markieren möchten. Wenn eine Bewertung inaktiv ist, haben Sie schreibgeschützten Zugriff auf ihre Inhalte. Sie können weiterhin zuvor erfasste Nachweise einsehen und Bewertungsberichte erstellen. Sie können die inaktive Bewertung jedoch nicht bearbeiten, Kommentare hinzufügen oder manuelle Nachweise hochladen.

Audit Manager console

So ändern Sie den Status einer Bewertung in der Audit Manager Manager-Konsole auf inaktiv

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Bewertungen aus.
3. Wählen Sie den Namen der Bewertung, um sie zu öffnen.
4. Wählen Sie in der oberen rechten Ecke der Seite die Option Bewertungsstatus aktualisieren und dann Inaktiv aus.
5. Wählen Sie im Popup-Fenster die Option Status aktualisieren aus, um zu bestätigen, dass Sie den Status auf inaktiv ändern möchten.

Die Änderungen an der Bewertung und ihren Kontrollen werden nach etwa einer Minute wirksam.

AWS CLI

Um den Status einer Bewertung in inaktiv zu ändern AWS CLI

1. Identifizieren Sie zunächst die Bewertung, die Sie aktualisieren möchten. Führen Sie dazu den Befehl Bewertungen auflisten aus.

   ```
   aws auditmanager list-assessments
   ```

   Die Antwort gibt eine Liste von Bewertungen zurück. Suchen Sie die Bewertung, die Sie deaktivieren möchten, und notieren Sie sich die Bewertungs-ID.
2. Führen Sie als Nächstes den update-assessment-statusBefehl aus und geben Sie die folgenden Parameter an:

   - `--assessment-id` – Verwenden Sie diesen Parameter, um die Bewertung anzugeben, die Sie deaktivieren möchten.
   - `--status` – Legen Sie diesen Wert auf fest `INACTIVE`.

   Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111 --status INACTIVE
```

Die Änderungen an der Bewertung und ihren Kontrollen werden nach etwa einer Minute wirksam.

Audit Manager API

Um den Status einer Bewertung mithilfe der API in inaktiv zu ändern

1. Gehen Sie wie ListAssessmentsfolgt vor, um die Bewertung zu finden, die Sie deaktivieren möchten, und notieren Sie sich die Bewertungs-ID.
2. Verwenden Sie die UpdateAssessmentStatusOperation und geben Sie die folgenden Parameter an:

   - Bewertungs-ID – Verwenden Sie diesen Parameter, um die Bewertung anzugeben, die Sie deaktivieren möchten.
   - Status – Setzen Sie diesen Wert auf. `INACTIVE`

Die Änderungen an der Bewertung und ihren Kontrollen werden nach etwa einer Minute wirksam.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, indem Sie auf einen der Links im vorherigen Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Wenn Sie sicher sind, dass Sie Ihre inaktive Bewertung nicht mehr benötigen, können Sie Ihre Audit Manager Manager-Umgebung bereinigen, indem Sie die Bewertung löschen. Detaillierte Anweisungen finden Sie unter Löschen einer Bewertung in AWS Audit Manager.

Löschen einer Bewertung in AWS Audit Manager

Wenn Sie eine Bewertung nicht mehr benötigen, können Sie sie aus Ihrer Audit Manager Manager-Umgebung löschen. Auf diese Weise können Sie Ihren Arbeitsbereich aufräumen und sich auf die Bewertungen konzentrieren, die für Ihre aktuellen Aufgaben und Prioritäten relevant sind.

> **Tip**
>
> Wenn Sie die Kosten senken möchten, sollten Sie erwägen, den Bewertungsstatus auf inaktiv zu ändern, anstatt die Bewertung zu löschen. Durch diese Aktion wird die Erfassung von Nachweisen beendet und Ihre Bewertung in einen schreibgeschützten Status versetzt, in dem Sie die zuvor erfassten Nachweise überprüfen können. Für inaktive Bewertungen fallen keine Gebühren an.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor eine Bewertung erstellt haben.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Löschen einer Bewertung in AWS Audit Manager verfügt. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können Bewertungen mit der Audi Manager-Konsole, der Audit Manager-API oder der AWS Command Line Interface (AWS CLI) löschen.

> **Warning**
>
> Durch diese Aktion werden Ihre Bewertung und alle damit erfassten Nachweise dauerhaft gelöscht. Diese Daten können nicht wiederhergestellt werden. Wir empfehlen Ihnen daher, vorsichtig vorzugehen und sicher zu sein, dass Sie Ihre Bewertung löschen möchten.

Audit Manager console

Um eine Bewertung in der Audit Manager Manager-Konsole zu löschen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Bewertungen aus.
3. Wählen Sie die Bewertung, die Sie löschen möchten, und wählen Sie Löschen.

AWS CLI

Um eine Bewertung in der AWS CLI

1. Identifizieren Sie zunächst die Bewertung, die Sie löschen möchten. Führen Sie dazu den Befehl Bewertungen auflisten aus.

   ```
   aws auditmanager list-assessments
   ```

   Die Antwort gibt eine Liste von Bewertungen zurück. Suchen Sie die Bewertung, die Sie löschen möchten, und notieren Sie sich die Bewertungs-ID.

2. Verwenden Sie als Nächstes den Befehl Bewertung löschen und geben Sie den `--assessment-id` der Bewertung an, die Sie löschen möchten.

   Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Um eine Bewertung mithilfe der API zu löschen

1. Verwenden Sie den ListAssessmentsVorgang, um die Bewertung zu finden, die Sie löschen möchten.

   Notieren Sie sich die Bewertungs-ID in der Antwort.

2. Verwenden Sie den DeleteAssessmentVorgang und geben Sie die AssessmentID der Bewertung an, die Sie löschen möchten.

Für weitere Informationen zu API-Befehlen klicken Sie auf einen der vorherigen Links in der AWS Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen. AWS SDKs

Weitere Ressourcen

Informationen zur Datenspeicherung in Audit Manager finden Sie unterLöschung von Audit Manager-Daten.

Delegationen in AWS Audit Manager

Im Laufe des Begutachtungsprozesses kann es vorkommen AWS Audit Manager, dass Sie auf Situationen stoßen, in denen Sie Hilfe von Fachexperten benötigen, um die gesammelten Beweise zu überprüfen und zu validieren. Hier kommt das Konzept der Delegationen ins Spiel.

Wichtige Punkte

Delegationen ermöglichen es den Prüfinhabern, Delegierten — Personen mit Spezialkenntnissen in den entsprechenden Bereichen — bestimmte Kontrollgruppen zuzuweisen. Mithilfe der Delegierungsfunktion können Sie sicherstellen, dass die Nachweise für jede Kontrolle von den entsprechenden Mitarbeitern sorgfältig geprüft werden. Auf diese Weise können Sie den Überprüfungsprozess rationalisieren und die allgemeine Genauigkeit und Zuverlässigkeit Ihrer Bewertungen verbessern. Ganz gleich, ob Sie Unterstützung bei der Interpretation technischer Nachweise, bei der Klärung von Compliance-Anforderungen oder bei der Gewinnung tieferer Einblicke in bestimmte Bereiche benötigen — Delegationen ermöglichen Ihnen eine effektive Zusammenarbeit mit Fachexperten.

Auf hoher Ebene sieht der Delegationsprozess wie folgt aus:

1. Der Audit-Verantwortliche wählt in seiner Bewertung einen Kontrollsatz und delegiert diesen zur Überprüfung.
2. Der Delegierte überprüft diese Kontrollen und ihre Nachweise und gibt den Kontrollsatz nach Abschluss der Prüfung an den Audit-Verantwortlichen zurück.
3. Der Audit-Verantwortliche wird darüber informiert, dass die Prüfung abgeschlossen ist, er überprüft die Kontrollen auf Anmerkungen des Delegierten.

> **Note**
>
> An AWS-Konto kann ein Prüfinhaber oder ein Delegierter in einem anderen AWS-Regionen Bereich sein.

Weitere Ressourcen

In den folgenden Abschnitten dieses Kapitels erfahren Sie mehr über die Verwaltung von Delegierungsaufgaben in AWS Audit Manager.

Grundlegendes zu den verschiedenen Delegierungsaufgaben für Prüfungsverantwortliche

Als Prüfungsverantwortlicher in Ihrer Organisation sind Sie dafür verantwortlich AWS Audit Manager, die Bewertungen zu verwalten und die Einhaltung der Vorschriften sicherzustellen. Sie verfügen zwar über Fachkenntnisse in den Bereichen Unternehmensführung, Risiko und Compliance, aber es kann vorkommen, dass Sie Fragen haben oder Unterstützung von Fachexperten benötigen, um bestimmte technische Nachweise oder Kontrollen zu überprüfen und zu interpretieren. Hier wird die Delegierungsfunktion in Audit Manager nützlich.

Wichtige Punkte

Durch die Erstellung einer Delegation können Sie Kontrollgruppen innerhalb einer Bewertung anderen Audit Manager Manager-Benutzern (sogenannten Delegierten) zuweisen, die über Fachwissen oder technisches Fachwissen in relevanten Bereichen verfügen. Diese Delegierten können dann die zugewiesenen Kontrollsätze überprüfen, die gesammelten Nachweise analysieren, bei Bedarf Kommentare oder zusätzliche Nachweise einreichen und den Status der einzelnen Kontrollen aktualisieren.

Der Delegationsprozess rationalisiert die Überprüfung und Validierung von Kontrollen, indem das kollektive Fachwissen innerhalb Ihrer Organisation genutzt wird. Es stellt sicher, dass jede Kontrolle von den qualifiziertesten Mitarbeitern sorgfältig geprüft wird, wodurch die Genauigkeit und Zuverlässigkeit Ihrer Bewertungen verbessert wird.

Weitere Ressourcen

In den folgenden Abschnitten werden Sie durch die verschiedenen Aufgaben geführt, die mit der Verwaltung von Delegationen als Prüfungsverantwortlicher verbunden sind. Dazu gehört, wie Sie Kontrollgruppen delegieren, den Status von Delegationen verfolgen und abgeschlossene Delegationen verwalten. Durch den effektiven Einsatz von Delegationen können Sie mit Fachexperten zusammenarbeiten, deren Fachwissen nutzen und einen umfassenden und fundierten Prüfprozess innerhalb von Audit Manager aufrechterhalten.

- Delegieren eines Kontrollsatzes zur Überprüfung in AWS Audit Manager
- Suchen und Überprüfen der Delegationen, die Sie eingesendet haben AWS Audit Manager
- Löschen Ihrer abgeschlossenen Delegationen in AWS Audit Manager

Delegieren eines Kontrollsatzes zur Überprüfung in AWS Audit Manager

Wenn Sie Unterstützung von einem Fachexperten benötigen, können Sie den Experten auswählen AWS-Konto , der Ihnen helfen soll, und diesem dann ein Kontrollset zur Überprüfung übertragen.

Delegieren Sie Berechtigungen

Die folgende Richtlinie ist einem Delegierten zugeordnet, an den der Kontrollsatz delegiert wurde.

Audit Manager *placeholder text* ersetzt die durch Ihre Konto- und Ressourcen-IDs, bevor die Richtlinie angehängt wird.

JSON

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

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who is delegated a Control Set of
 the Assessment"
            },
            "Action": [
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder"
            ],
            "Resource": "arn:aws:auditmanager:us-
east-1:123456789012:assessment/assessment_ID/controlSet/control_set_ID"
        }
    ]
}
```

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen zum Erstellen einer Delegierung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie haben die Wahl zwischen den folgenden Verfahren, um einen Kontrollsatz zu delegieren.

Delegieren eines Kontrollsatzes von einer Bewertungsseite

Um einen Kontrollsatz von einer Bewertungsseite aus zu delegieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Bewertungen aus.
3. Wählen Sie den Namen der Bewertung aus, die den Kontrollsatz enthält, den Sie delegieren möchten.

4. Wählen Sie auf der Bewertungsseite die Registerkarte Kontrollen aus. Daraufhin werden eine Zusammenfassung des Kontrollstatus und die Liste der Kontrollen in der Bewertung angezeigt.
5. Markieren Sie einen Kontrollsatz und wählen Sie Kontrollsatz delegieren.
6. Unter Delegiertenauswahl wird eine Liste mit Benutzern und Rollen angezeigt. Wählen Sie einen Benutzer oder eine Rolle aus, oder verwenden Sie die Suchleiste, um nach einem Benutzer oder einer Rolle zu suchen.
7. Überprüfen Sie unter Delegierungsdetails den Namen des Kontrollsatzes und den Namen der Bewertung.
8. (Optional) Fügen Sie unter Kommentare Anweisungen hinzu, um den Delegierten bei der seiner Prüfung zu unterstützen. Geben Sie keine vertraulichen Informationen im Kommentar preis.
9. Wählen Sie Kontrollsatz delegieren.
10. Ein grünes Banner bestätigt die erfolgreiche Delegierung des Kontrollsatzes. Wählen Sie Delegierung anzeigen, um die Delegierungsanfrage zu sehen. Sie können Ihre Delegationen auch jederzeit einsehen, indem Sie im linken Navigationsbereich der AWS Audit Manager Konsole Delegationen auswählen.

Delegieren eines Kontrollsatzes von der Delegationsseite aus

Um einen Kontrollsatz von der Delegationsseite aus zu delegieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Delegierungen.
3. Wählen Sie auf der Delegationsseite die Option Delegierung erstellen.
4. Geben Sie unter Bewertungs- und Kontrollsatz auswählen den Bewertungs- und Kontrollsatz an, den Sie delegieren möchten.
5. Unter Delegiertenauswahl sehen Sie eine Liste mit Benutzern und Rollen. Wählen Sie einen Benutzer oder eine Rolle aus, oder verwenden Sie die Suchleiste, um nach einem Benutzer oder einer Rolle zu suchen.
6. (Optional) Fügen Sie unter Kommentare Anweisungen hinzu, um den Delegierten bei der seiner Prüfung zu unterstützen. Geben Sie keine vertraulichen Informationen im Kommentar preis.
7. Wählen Sie Delegierung erstellen.
8. Ein grünes Banner bestätigt die erfolgreiche Delegierung des Kontrollsatzes. Wählen Sie Delegierung anzeigen, um die Delegierungsanfrage zu sehen. Sie können Ihre Delegationen

auch jederzeit einsehen, indem Sie im linken Navigationsbereich der AWS Audit Manager Konsole Delegationen auswählen.

Nachdem Sie einen Kontrollsatz zur Überprüfung delegiert haben, erhält der Delegierte eine Benachrichtigung und kann dann mit der Überprüfung des Kontrollsatzes beginnen. Der vom Delegierten zu beachtende Prozess wird in Grundlegendes zu den verschiedenen Delegierungsaufgaben für Delegierte beschrieben.

Nächste Schritte

Informationen dazu, wie Sie Ihre Delegierung zu einem späteren Zeitpunkt erneut überprüfen können, finden Sie unter. Suchen und Überprüfen der Delegationen, die Sie eingesendet haben AWS Audit Manager

Suchen und Überprüfen der Delegationen, die Sie eingesendet haben AWS Audit Manager

Sie können jederzeit auf eine Liste Ihrer Delegationen zugreifen, indem Sie im linken Navigationsbereich von Audit Manager Delegationen auswählen. Die Seite Delegationen enthält eine Liste Ihrer aktiven und abgeschlossenen Delegationen.

Wenn eine Delegierung abgeschlossen ist, erhalten Sie eine Benachrichtigung in Audit Manager. Möglicherweise erhalten Sie auch Kommentare mit Anmerkungen vom Delegierten. Das folgende Verfahren erklärt, wie Sie Ihre Delegationen in Audit Manager überprüfen können, nachdem sie abgeschlossen sind, und wie Sie alle Kommentare einsehen können, die der Delegierte möglicherweise für Sie hinterlassen hat.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen verfügt, um eine Delegierung einzusehen. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Gehen Sie wie folgt vor, um die Delegationen zu finden und zu überprüfen, die Sie zuvor erstellt haben.

Anzeige einer abgeschlossenen Delegierung und Suche nach Kommentaren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Delegierungen.
3. Sehen Sie sich die Seite Delegationen an, die eine Tabelle mit den folgenden Informationen enthält:

Name	Description
Delegiert an	Das AWS-Konto , an das Sie den Kontrollsatz delegiert haben.
Date (Datum)	Das Datum, an dem Sie den Kontrollsatz delegiert haben.
Status	Der aktuelle Status der Delegierung.
Bewertung	Der Name der Bewertung mit einem Link zur Bewertung sdetailseite.
Kontrollsatz	Der Name des Kontrollsatzes, der zur Überprüfung delegiert wurde.

4. Suchen Sie den Bewertungs- und Kontrollsatz, den der Delegierte geprüft und übermittelt hat, und wählen Sie den Namen der Bewertung aus, um sie zu öffnen.
5. Scrollen Sie auf der Seite mit den Bewertungsdetails auf der Registerkarte Kontrollen nach unten zur Tabelle Kontrollsätze.
6. Suchen Sie unter Nach Kontrollsatz gruppierte Kontrollen den Namen des Kontrollsatzes, den Sie delegiert haben.
7. Erweitern Sie den Namen des Kontrollsatzes, um die zugehörigen Steuerelemente anzuzeigen, und wählen Sie den Namen eines Steuerelements, um die Kontrolldetailseite zu öffnen.
8. Wählen Sie die Registerkarte Kommentare, um alle Anmerkungen anzuzeigen, die der Delegierte zu dieser bestimmten Kontrolle hinzugefügt hat.
9. Wenn Sie überzeugt sind, dass die Überprüfung eines Kontrollsatzes abgeschlossen ist, wählen Sie den Kontrollsatz aus und wählen Sie Vollständige Überprüfung des Kontrollsatzes aus.

> **Important**
>
> Der Audit Manager sammelt kontinuierlich Beweise. Daher können jederzeit weitere Nachweise erfasst werden, nachdem der Delegierte die Prüfung einer Kontrolle abgeschlossen hat.
> Wenn Sie für Ihre Bewertungsberichte nur überprüfte Nachweise einbeziehen möchten, können Sie anhand des Zeitstempels der Überprüfung feststellen, wann die Nachweise geprüft wurden. Dieser Zeitstempel befindet sich auf Registerkarte „Änderungsprotokoll“ der Seite mit den Kontrolldetails. Anhand dieses Zeitstempels können Sie feststellen, welche Nachweise Sie Ihren Bewertungsberichten hinzufügen.

Nächste Schritte

Informationen zum Löschen einer Delegierung, wenn sie abgeschlossen ist und Sie sie nicht mehr benötigen, finden Sie unterLöschen Ihrer abgeschlossenen Delegationen in AWS Audit Manager.

Löschen Ihrer abgeschlossenen Delegationen in AWS Audit Manager

Es kann vorkommen, dass Sie eine Delegierung erstellen, aber später keine Unterstützung mehr bei der Überprüfung dieses Kontrollsatzes benötigen. In diesem Fall können Sie eine aktive Delegierung in Audit Manager löschen. Sie können auch abgeschlossene Delegationen löschen, die Sie nicht mehr auf der Delegationsseite sehen möchten.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Löschen einer Delegierung verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

So löschen Sie eine Delegierung

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Delegierungen.

3. Wählen Sie auf der Seite Delegierungen die Delegierung aus, die Sie löschen möchten, und klicken Sie dann auf Delegierung entfernen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster zur Bestätigung die Option Entfernen.

Grundlegendes zu den verschiedenen Delegierungsaufgaben für Delegierte

Als Delegierter spielen Sie eine wichtige Rolle bei der Unterstützung der Prüfungsverantwortlichen während des Bewertungsprozesses. AWS Audit Manager Die Prüfungsverantwortlichen sind zwar für die Verwaltung der Bewertungen und die allgemeine Einhaltung der Vorschriften verantwortlich, benötigen jedoch manchmal Unterstützung von Fachexperten bei der Überprüfung und Interpretation bestimmter technischer Nachweise, die nicht in ihren Zuständigkeitsbereich fallen. In solchen Szenarien werden Ihr Wissen und Ihre Fähigkeiten von unschätzbarem Wert.

Wichtige Punkte

Die Delegierungsfunktion ermöglicht es den Prüfinhabern, Ihnen bestimmte Kontrollgruppen zur Überprüfung zuzuweisen und dabei auf Ihr spezialisiertes geschäftliches oder technisches Fachwissen zurückzugreifen. Dieser kollaborative Ansatz verbessert nicht nur die Genauigkeit und Zuverlässigkeit der Bewertungen, sondern optimiert auch den Überprüfungsprozess, sodass sich die Prüfungsverantwortlichen auf ihre Kernaufgaben konzentrieren können, während Sie sich auf die Bereiche konzentrieren können, in denen Ihr Fachwissen am wertvollsten ist.

Als Delegierter erhalten Sie möglicherweise Anfragen von Prüfinhabern, Nachweise zu überprüfen, die mit den zugewiesenen Kontrollsätzen verknüpft sind. Sie können den Audit-Verantwortlichen helfen, indem Sie die Kontrollsätze und die zugehörigen Nachweise überprüfen, Kommentare hinzufügen, zusätzliche Nachweise hochladen und den Status jeder geprüften Kontrolle aktualisieren.

> **Note**
>
> Audit-Verantwortliche delegieren bestimmte Kontrollsätze zur Überprüfung, aber keine ganzen Bewertungen. Aus diesem Grund haben Delegierte nur begrenzten Zugriff auf Bewertungen. Delegierte können Nachweise überprüfen, Kommentare hinzufügen, manuelle Nachweise hochladen und den Kontrollstatus für jede Kontrolle im Kontrollsatz aktualisieren. Weitere Informationen zu Rollen und dazu gehörenden Berechtigungen finden Sie unter Empfohlene Richtlinien für Benutzerrollen in AWS Audit Manager.

Weitere Ressourcen

In den folgenden Abschnitten erfahren Sie mehr über die Aufgaben, die mit der Verwaltung von Delegationen als Delegierter verbunden sind. Dazu gehört, wie Sie eingehende Delegierungsanfragen einsehen, zugewiesene Kontrollsätze überprüfen, Kommentare und zusätzliche Nachweise einreichen und Ihre überprüften Kontrollen an den Prüfungsverantwortlichen zurücksenden.

- Ihre Benachrichtigungen für eingehende Delegierungsanfragen anzeigen
- Überprüfung des delegierten Kontrollsatzes und der zugehörigen Nachweise
- Kommentare zu einem Steuerelement während einer Überprüfung des Kontrollsatzes hinzufügen
- Markieren eines Steuerelements als überprüft in AWS Audit Manager
- Rückgabe eines überprüften Kontrollsatzes an den Audit-Verantwortlichen

Ihre Benachrichtigungen für eingehende Delegierungsanfragen anzeigen

Wenn ein Audit-Verantwortlicher Sie um Unterstützung bei der Überprüfung eines Kontrollsatzes bittet, erhalten Sie eine Benachrichtigung, die Sie über den an Sie delegierten Kontrollsatz informiert.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen von Benachrichtigungen verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

So zeigen Sie Ihre Benachrichtigungen an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen.
3. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze, die Ihnen zur Prüfung delegiert wurden. Die Tabelle enthält die folgenden Informationen:

Name	Description
Date (Datum)	Das Datum, an dem der Kontrollsatz delegiert wurde.
Bewertung	Der Name der Bewertung, die dem Kontrollsatz zugeordnet ist.
Kontrollsatz	Der Name des Kontrollsatzes.
Quelle	Der Benutzer oder die Rolle, die den Kontrollsatz an Sie delegiert hat.
Beschreibung	Anweisungen, die vom Prüfungsverantwortlichen bereitgestellt werden.

> **Tip**
>
> Sie können auch ein SNS-Thema abonnieren, um E-Mails zu erhalten, wenn ein Kontrollsatz zur Überprüfung an Sie delegiert wurde. Weitere Informationen finden Sie unter Benachrichtigungen in AWS Audit Manager.

Nächste Schritte

Wenn Sie bereit sind, mit der Überprüfung der Kontrollen zu beginnen, die an Sie delegiert wurden, finden Sie unterÜberprüfung des delegierten Kontrollsatzes und der zugehörigen Nachweise.

Überprüfung des delegierten Kontrollsatzes und der zugehörigen Nachweise

Sie können die Audit-Verantwortlichen unterstützen, indem Sie die Kontrollsätze überprüfen, die sie an Sie delegiert haben.

Sie können diese Kontrollen und die damit verbundenen Nachweise überprüfen, um festzustellen, ob zusätzliche Maßnahmen erforderlich sind. Zu diesen zusätzlichen Maßnahmen können das manuelle Hochladen zusätzlicher Nachweise für die Einhaltung der Compliance oder das Hinterlassen eines Kommentars gehören, in dem die von Ihnen ergriffenen Abhilfemaßnahmen detailliert beschrieben werden.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen zum Anzeigen eines Kontrollsatzes verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Um einen Kontrollsatz zu prüfen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Benachrichtigungen.
3. Auf der Seite Benachrichtigungen sehen Sie eine Liste der Kontrollsätze, die an Sie delegiert wurden. Legen Sie fest, welchen Kontrollsatz Sie überprüfen möchten, und wählen Sie den Namen der zugehörigen Bewertung, um die Seite mit den Bewertungsdetails zu öffnen.
4. Scrollen Sie auf der Seite mit den Bewertungsdetails auf der Registerkarte Kontrollen nach unten zur Tabelle Kontrollsätze.
5. Erweitern Sie in der Spalte Nach Kontrollsatz gruppierte Kontrollsätze den Namen eines Kontrollsatzes, um dessen Steuerelemente anzuzeigen.
6. Wählen Sie den Namen einer Kontrolle, um die Kontrolldetailseite zu öffnen.
7. (Optional) Wählen Sie Kontrollstatus aktualisieren, um den Status der Kontrolle zu ändern. Während Ihre Überprüfung in Bearbeitung ist, können Sie den Status als in Prüfung markieren.
8. Informationen über das Steuerelement finden Sie in den Ordnern „Beweise“, „Details“, „Datenquellen“, „Kommentare“ und „Changelog“.

    - Weitere Informationen zu den einzelnen Registerkarten und zum besseren Verständnis der darin enthaltenen Daten finden Sie unterÜberprüfung einer Bewertungskontrolle in AWS Audit Manager.

So überprüfen Sie die Nachweise für eine Kontrolle

1. Wählen Sie auf der Kontrollseite die Registerkarte Beweisordner aus.

2. Navigieren Sie zur Tabelle Nachweisordner, um eine Liste der Ordner zu sehen, die Beweise für dieses Steuerelement enthalten. Diese Ordner sind nach dem Datum geordnet, an dem die Nachweise erfasst wurden.
3. Wählen Sie den Namen eines Beweisordners, um ihn zu öffnen. Sie sehen dann eine Zusammenfassung aller an diesem Datum gesammelten Nachweise.

   - Diese Zusammenfassung enthält die Gesamtzahl der Probleme bei der Konformitätsprüfung, die direkt von AWS Security Hub CSPM AWS Config, oder beiden gemeldet wurden.
   - Weitere Informationen zu diesen Informationen finden Sie unterÜberprüfung eines Beweisordners in AWS Audit Manager.
4. Navigieren Sie auf der Übersichtsseite der Beweisordner zur Tabelle Nachweise. Wählen Sie in der Spalte Zeit ein Beweisstück aus, das geöffnet werden soll.
5. Überprüfen Sie die Einzelheiten der Beweise.

   - Weitere Informationen zu diesen Informationen finden Sie unterÜberprüfung von Nachweisen in AWS Audit Manager.

Nächste Schritte

In einigen Fällen müssen Sie möglicherweise zusätzliche Nachweise vorlegen, um die Einhaltung der Vorschriften nachzuweisen. In diesen Fällen können Sie manuell Nachweise hochladen. Detaillierte Anweisungen finden Sie unter Manuelle Nachweise hinzufügen in AWS Audit Manager.

Wenn Sie Kommentare zu einer oder mehreren der Kontrollen hinterlassen möchten, die an Sie delegiert wurden, finden Sie weitere Informationen unterKommentare zu einem Steuerelement während einer Überprüfung des Kontrollsatzes hinzufügen.

Kommentare zu einem Steuerelement während einer Überprüfung des Kontrollsatzes hinzufügen

Sie können Kommentare zu allen Kontrollelementen hinzufügen, die Sie überprüfen. Diese Kommentare sind für den Audit-Verantwortlichen sichtbar.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen verfügt, um Kommentare zu einer Bewertungskontrolle in AWS Audit Manager hinzuzufügen. Zwei

vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Um einen Kommentar zu einem Kontrollelement hinzufügen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen.
3. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze an, die Ihnen zur Prüfung delegiert wurden.
4. Suchen Sie den Kontrollsatz, der die Kontrolle enthält, zu der Sie einen Kommentar hinterlassen möchten, und wählen Sie dann den Namen der zugehörigen Bewertung aus, um die Bewertung zu öffnen.
5. Wählen Sie die Registerkarte Kontrolle, scrollen Sie nach unten zu Kontrollsätze, und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.
6. Wählen Sie die Registerkarte Kommentare.
7. Geben Sie unter Kommentare senden Ihren Kommentar in das Textfeld ein.
8. Wählen Sie Kommentar abgeben aus, um Ihren Kommentar hinzuzufügen. Ihr Kommentar wird dann zusammen mit allen anderen Kommentaren zu diesem Steuerelement im Bereich „Frühere Kommentare“ der Seite angezeigt.

Nächste Schritte

Wenn Sie mit der Überprüfung des Steuerelements fertig sind, folgen Sie den Schritten unterMarkieren eines Steuerelements als überprüft in AWS Audit Manager.

Markieren eines Steuerelements als überprüft in AWS Audit Manager

Sie können den Fortschritt Ihrer Überprüfung anzeigen, indem Sie den Status einzelner Kontrollen innerhalb eines Kontrollsatzes aktualisieren.

Das Ändern des Status einer Kontrolle ist optional. Wir empfehlen jedoch, dass Sie den Status jeder Kontrolle auf Überprüft ändern, wenn Sie Ihre Überprüfung für diese Kontrolle abgeschlossen haben.

Unabhängig vom Status der einzelnen Kontrollen können Sie die Kontrollen zurück an den Audit-Verantwortlichen weiterleiten.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen verfügt, um den Status einer Bewertungskontrolle in AWS Audit Manager zu aktualisieren. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Um eine Kontrolle als überprüft zu markieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen.
3. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze an, die Ihnen zur Prüfung delegiert wurden.
4. Suchen Sie den Kontrollsatz, den Sie als geprüft markieren möchten, und wählen Sie dann den Namen der zugehörigen Bewertung aus, um die Bewertung zu öffnen.
5. Scrollen Sie auf der Seite mit den Bewertungsdetails auf der Registerkarte Kontrollen nach unten zur Tabelle Kontrollsätze.
6. Erweitern Sie in der Spalte Nach Kontrollsatz gruppierte Kontrollsätze den Namen eines Kontrollsatzes, um dessen Steuerelemente anzuzeigen.
7. Wählen Sie den Namen einer Kontrolle, um die Kontrolldetailseite zu öffnen.
8. Wählen Sie Kontrollstatus aktualisieren und ändern Sie den Status zu Überprüft.
9. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option Kontrollstatus aktualisieren, um zu bestätigen, dass Sie die Überprüfung der Kontrolle abgeschlossen haben.

Nächste Schritte

Informationen zum Abschließen des Delegierungsvorgangs finden Sie unterRückgabe eines überprüften Kontrollsatzes an den Audit-Verantwortlichen.

Rückgabe eines überprüften Kontrollsatzes an den Audit-Verantwortlichen

Nachdem Sie den Kontrollsatz überprüft, Kommentare oder zusätzliche Nachweise hinzugefügt und den Status der einzelnen Kontrollen aktualisiert haben, gelangen Sie zu einem wichtigen Schritt: der Rückgabe des überprüften Kontrollsatzes an den Prüfungsverantwortlichen. Das Einreichen des überprüften Kontrollsatzes markiert den Abschluss Ihrer delegierten Aufgaben und ermöglicht es dem Prüfungsverantwortlichen, Ihre Erkenntnisse und Empfehlungen in die Gesamtbeurteilung einfließen zu lassen.

Voraussetzungen

Vergewissern Sie sich, dass Ihre IAM-Identität über die erforderlichen Berechtigungen verfügt, um den überprüften Kontrollsatz an den Prüfungsverantwortlichen in zu senden. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben undErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Gehen Sie wie folgt vor, um den Kontrollsatz an den für die Prüfung Verantwortlichen weiterzuleiten.

Zur Rückgabe eines überprüften Kontrollsatzes an den Audit-Verantwortlichen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen.
3. Prüfung der Liste der Kontrollsätze, die an Sie zur Prüfung delegiert wurden. Suchen Sie nach dem Kontrollsatz, den Sie dem Audit-Verantwortlichen zurücksenden möchten, und wählen Sie den Namen der zugehörigen Bewertung.
4. Scrollen Sie nach unten zur Tabelle Kontrollsätze, wählen Sie den Kontrollsatz aus, den Sie dem Audit-Verantwortlichen vorlegen möchten, und wählen Sie dann Zur Prüfung einreichen aus.
5. In dem daraufhin angezeigten Popup-Fenster können Sie Kommentare hinzufügen, bevor Sie Zur Überprüfung einreichen wählen.

Bewertungsberichte

Ein Bewertungsbericht fasst die ausgewählten Nachweise zusammen, die für eine Bewertung gesammelt wurden. Er enthält auch Links zu PDF-Dateien mit Einzelheiten zu den einzelnen Nachweisen. Der konkrete Inhalt, das Unternehmen und die Benennungskonvention eines Bewertungsberichts hängen von den Parametern ab, die Sie bei der Erstellung des Berichts auswählen.

Bewertungsberichte helfen Ihnen bei der Auswahl und Zusammenstellung der Nachweise, die für Ihr Audit relevant sind. Sie bewerten jedoch nicht die Richtigkeit der Nachweise selbst. Stattdessen stellt Audit Manager einfach die ausgewählten Nachweisdetails als Ausgabe bereit, die Sie mit Ihrem Prüfer teilen können.

Inhalt

Grundlegendes zur Ordnerstruktur des Bewertungsberichts

Wenn Sie einen Bewertungsbericht herunterladen, erstellt Audit Manager einen ZIP-Ordner. Dieser enthält Ihren Bewertungsbericht und die zugehörigen Nachweisdateien in verschachtelten Unterordnern.

Der Zip-Ordner ist wie folgt aufgebaut:

- Bewertungsordner (Beispiel: `myAssessmentName-a1b2c3d4`) – Der Stammordner.
  - Ordner für Bewertungsberichte (Beispiel:`reportName-a1b2c3d4e5f6g7`) — Ein Unterordner, in dem Sie die AssessmentReportSummary Dateien .pdf, digest.txt und README.txt finden.
    - Ordner „Nachweise nach Kontrolle“ (Beispiel: `controlName-a1b2c3d4e5f6g`) – Ein Unterordner, in dem die Nachweisdateien nach der zugehörigen Kontrolle gruppiert werden.
      - Ordner „Nachweise nach Datenquellen“ (Beispiel: `CloudTrail`,`Security Hub CSPM`) – Ein Unterordner, der Nachweisdateien nach dem Datenquellentyp gruppiert.
        - Ordner „Nachweise nach Datum“ (Beispiel: `2022-07-01`) – Ein Unterordner, der Nachweisdateien nach dem Datum der Nachweissammlung gruppiert.
          - Nachweisdateien – Die Dateien, die Details zu einzelnen Nachweisen enthalten.

In einem Bewertungsbericht navigieren

Öffnen Sie zunächst den ZIP-Ordner und navigieren Sie eine Ebene nach unten zum Ordner für den Bewertungsbericht. Hier finden Sie das PDF des Bewertungsberichts und die Datei README.txt.

Sie können sich die Datei README.txt ansehen, um die Struktur und den Inhalt des ZIP-Ordners zu verstehen. Sie enthält auch Bezugsinformationen zu den Namenskonventionen für jede Datei. Diese Informationen können Ihnen helfen, direkt zu einem Unterordner oder einer Nachweisdatei zu navigieren, wenn Sie nach einem bestimmten Objekt suchen.

Andernfalls öffnen Sie die PDF-Datei des Bewertungsberichts, um nach den Nachweisen zu suchen und die benötigten Informationen zu finden. Auf diese Weise erhalten Sie eine allgemeine Übersicht über den Bericht und eine Zusammenfassung der Bewertung, auf welcher der Bericht basiert.

Verwenden Sie als Nächstes das Inhaltsverzeichnis (Table of Contents, TOC), um den Bericht zu untersuchen. Sie können ein beliebiges mit einem Hyperlink verknüpftes Steuerelement im Inhaltsverzeichnis auswählen, um direkt zu einer Zusammenfassung dieser Kontrolle zu gelangen.

Wenn Sie bereit sind, die Nachweisdetails für eine Kontrolle zu überprüfen, können Sie dies tun, indem Sie den Namen des mit einem Hyperlink verknüpften Nachweises auswählen. Bei automatisierten Nachweisen öffnet der Hyperlink eine neue PDF-Datei mit Details zu diesen Nachweisen. Bei manuellen Nachweisen gelangen Sie über den Hyperlink zum S3-Bucket, der die Nachweise enthält.

> **Tip**
>
> In der Breadcrumb-Navigation oben auf jeder Seite wird Ihre aktuelle Position im Bewertungsbericht angezeigt, wenn Sie nach Kontrollen und Nachweisen suchen. Wählen Sie das mit einem Hyperlink verknüpfte Inhaltsverzeichnis aus, um jederzeit zum Inhaltsverzeichnis zurückzukehren.

Überprüfung der Abschnitte eines Bewertungsberichts

Anhand der folgenden Informationen erfahren Sie mehr über die einzelnen Abschnitte eines Bewertungsberichts.

> **Note**
>
> Wenn Sie in den folgenden Abschnitten neben einem der Attribute einen Bindestrich (-) sehen, bedeutet dies, dass der Wert dieses Attributs Null ist oder kein Wert existiert.

Deckblatt

Das Deckblatt enthält den Namen des Bewertungsberichts. Außerdem werden Datum und Uhrzeit der Erstellung des Berichts sowie die Konto-ID des Benutzers angezeigt, der den Bericht erstellt hat.

Das Deckblatt ist wie folgt formatiert. Audit Manager *placeholders* ersetzt das durch die Informationen, die für Ihren Bericht relevant sind.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Übersichtsseite

Die Übersichtsseite besteht aus zwei Teilen: einer Zusammenfassung des Berichts selbst und einer Zusammenfassung der Bewertung, über die berichtet wird.

Zusammenfassungsbericht

In diesem Abschnitt wird der Bewertungsbericht zusammengefasst.

Name	Description
Name des Berichts	Der Name des Berichts.
Beschreibung	Die Beschreibung, die vom Prüfungsverantwortlichen bei der Erstellung des Berichts eingegeben wurde.
Datum der Generierung	Das Datum, an dem der Bericht generiert wurde. Die Zeit wird im UTC-Format (Coordinated Universal Time) dargestellt.
Kontrollen insgesamt enthalten	Die Anzahl der Kontrollen, die im Bericht enthalten sind und für die Beweise gesammelt wurden. Dies ist eine Teilmenge der Gesamtzahl der Kontrollen in der Bewertung.
AWS-Konten enthalten	Die Anzahl derer AWS-Konten , die im Bericht enthalten sind und Beweise gesammelt haben. Dies ist ein Teil der Gesamtzahl der AWS-Konten in der Bewertung enthaltenen.
Auswahl des Bewertung sberichts	Die Anzahl der Nachweise, die für die Aufnahme in den Bericht ausgewählt wurden. Dies beinhaltet die Gesamtzahl der im Bericht festgestellten Probleme bei der Konformitätsprüfung.

Zusammenfassung der Bewertung

In diesem Abschnitt wird der Bewertungsbericht zusammengefasst.

Name	Description
Name der Bewertung	Der Name der Bewertung, anhand derer der Bericht erstellt wurde.
Status	Der Status der Bewertung zum Zeitpunkt der Erstellung des Berichts.
Region der Bewertung	Die AWS-Region , in der die Bewertung erstellt wurde.
AWS-Konten im Geltungsbereich	Die Liste AWS-Konten davon ist Teil der Bewertung.
Name des Frameworks	Der Name des Frameworks, aus dem die Bewertung erstellt wurde.
Inhaber des Audits	Der Benutzer oder die Rolle der Prüfungsverantwortlichen der Bewertung.
Letzte Aktualisierung	Das Datum, an dem die Bewertung zuletzt aktualisiert wurde. Die Uhrzeit wird in UTC dargestellt.

Seite mit dem Inhaltsverzeichnis

Das Inhaltsverzeichnis zeigt den vollständigen Inhalt des Bewertungsberichts. Die Inhalte werden auf der Grundlage der Kontrollsätze, die in der Bewertung enthalten sind, gruppiert und organisiert. Die Kontrollen sind unter dem jeweiligen Kontrollsatz aufgeführt.

Wählen Sie ein beliebiges Element im Inhaltsverzeichnis aus, um direkt zu diesem Abschnitt des Berichts zu gelangen. Sie können entweder einen Kontrollsatz auswählen oder direkt zu einer Kontrolle wechseln.

Kontrollseite

Die Kontrollseite besteht aus zwei Teilen: einer Zusammenfassung der Kontrolle selbst und einer Zusammenfassung der Nachweise, die für die Kontrolle gesammelt wurden.

Zusammenfassung der Kontrolle

Dieser Abschnitt enthält folgende Informationen.

Name	Description
Name des Steuerelements	Der Name des Steuerelements.
Beschreibung	Die Beschreibung des Steuerelements.
Steuersatz	Der Name des Kontrollsatzes, zu dem das Steuerelement gehört.
Informationen werden getestet	Die empfohlenen Testverfahren für diese Kontrolle.
Aktionsplan	Die empfohlenen Maßnahmen, die durchgeführt werden müssen, wenn die Kontrolle nicht erfüllt ist.
Auswahl des Bewertung sberichts	Die Anzahl der Nachweise im Zusammenhang mit dieser Kontrolle , die in den Bewertungsbericht aufgenommen wurden. Dies beinhaltet die Anzahl der Probleme bei der Konformitätsprüfung, die bei den Nachweisen dieser Kontrolle festgestellt wurden.

Gesammelte Nachweise

In diesem Abschnitt werden die Nachweise aufgeführt, die für die Kontrolle gesammelt wurden. Die Beweise sind nach Ordnern gruppiert, die nach dem Datum der Beweiserhebung geordnet und benannt sind. Neben dem Namen jedes Beweisordners steht die Gesamtzahl der Probleme mit der Konformitätsprüfung für diesen Ordner.

Unter dem Namen jedes Beweisordners befindet sich eine Liste aus Hyperlinks mit Nachweisnamen.

- Namen automatisierter Beweise beginnen mit einem Zeitstempel für die Beweiserhebung, gefolgt vom Servicecode, dem Ereignisnamen (bis zu 20 Zeichen), der Konto-ID und einer eindeutigen 12-stelligen eindeutigen ID.

  Beispiel: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  Bei automatisierten Nachweisen öffnet der Name mit dem Hyperlink eine neue PDF-Datei mit einer Zusammenfassung und weiteren Details.

- Namen manueller Nachweise beginnen mit einem Zeitstempel für das Hochladen von Nachweisen, gefolgt von der Bezeichnung `manual`, der Konto-ID und einer 12-stelligen eindeutigen ID. Sie enthalten auch die ersten 10 Zeichen des Dateinamens und die Dateierweiterung (bis zu 10 Zeichen).

  Beispiel: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  Bei manuellen Nachweisen gelangen Sie über den Hyperlinknamen zu dem S3-Bucket, der diese Nachweise enthält.

Neben dem Namen jedes Nachweises steht das Ergebnis der Konformitätsprüfung für dieses Element.

- Bei automatisierten Nachweisen, die von AWS Security Hub CSPM oder gesammelt wurden AWS Config, wird ein konformes, nicht konformes oder nicht schlüssiges Ergebnis gemeldet.
- Bei automatisierten Nachweisen, die anhand von AWS CloudTrail API-Aufrufen gesammelt wurden, und bei allen manuellen Nachweisen wird das Ergebnis „Nicht eindeutig“ angezeigt.

Nachweisübersichtsseite

Die Seite mit der Zusammenfassung der Beweise enthält die folgenden Informationen.

Name	Description
ID (ID)	Die eindeutige Kennung für die Beweise.
Datum der Erfassung	Das Datum, an dem die Beweise erstellt oder hochgeladen wurden.
Beschreibung	Eine Beschreibung der Beweise, einschließlich der Konto-ID und des Datenquellentyps.
Name der Bewertung	Der Name der Bewertung, anhand derer der Bericht erstellt wurde.
Name des Frameworks	Der Name des Frameworks, aus dem die Bewertung erstellt wurde.
Name des Steuerelements	Der Name der Kontrolle, die durch die Beweise gestützt wird.

Name	Description
Name des Kontrollsatzes	Der Name des Kontrollsatzes, zu dem das zugehörige Steuerelement gehört.
Beschreibung des Steuerelements	Die Beschreibung der Kontrolle, die durch die Beweise gestützt wird.
Informationen zum Testen	Die empfohlenen Testverfahren für die Kontrolle.
Aktionsplan	Die empfohlenen Maßnahmen, die durchgeführt werden müssen, wenn die Kontrolle nicht erfüllt ist.
AWS-Region	Der Name der Region, die mit den Beweisen verknüpft ist.
ICH BIN ID	Der ARN des Benutzers oder der Rolle, die mit den Nachweisen verknüpft ist.
AWS-Konto	Die AWS-Konto ID, die den Beweisen zugeordnet ist.
AWS-Service	Der Name der Person AWS-Service , die mit den Beweisen verknüpft ist.
Ereignisname	Der Name des Beweisereignisses.
Ereigniszeit	Der Zeitpunkt, zu dem das Beweisereignis eingetreten ist.
Datenquelle	Von wo aus die Beweise gesammelt oder hochgeladen wurden. Der Datenquellentyp kann entweder AWS Config Security Hub CSPM, AWS API-Aufrufe oder Manuell sein. CloudTrail

Name	Description
Nachweise nach Typ	Die Kategorie der Beweise • Nachweise zur Konformitätsprüfung werden von unserem AWS Config Security Hub CSPM gesammelt. • Nachweise zu Benutzeraktivitäten werden anhand von CloudTrail Protokollen gesammelt. • Der Nachweis von Konfigurationsdaten wird anhand von Schnappschüssen anderer AWS-Services Daten gesammelt. • Manuelle Beweise sind Beweise, die Sie manuell hochladen.
Status der Konformitätsprüfung	Der Status der Bewertung von Nachweisen, die unter die Kategorie Konformitätsprüfung fallen. • Bei automatisierten Nachweisen, die anhand von AWS Security Hub CSPM oder gesammelt wurden AWS Config, wird ein konformes, nicht konformes oder nicht schlüssiges Ergebnis gemeldet. • Bei automatisierten Nachweisen, die anhand von AWS CloudTrail API-Aufrufen gesammelt wurden, und bei allen manuellen Nachweisen wird das Ergebnis „Nicht eindeutig“ angezeigt.

Seite mit den Nachweisdetails

Auf der Seite mit den Nachweisdetails werden der Name der Nachweise und eine Tabelle mit den Nachweisdetails angezeigt. Diese Tabelle enthält eine detaillierte Aufschlüsselung der einzelnen Nachweiselemente, sodass Sie die Daten verstehen und überprüfen können, ob sie korrekt sind. Je nach Datenquelle der Nachweise variiert der Inhalt der Seite mit den Nachweisdetails.

> **Tip**
>
> Die Breadcrumb-Navigation oben auf jeder Seite zeigt Ihren aktuellen Standort an, wenn Sie die Details zu den Nachweisen durchsuchen. Wählen Sie Zusammenfassung der Nachweise aus, um jederzeit zur Zusammenfassung der Nachweise zurückzukehren.

Validierung eines Bewertungsberichts

Wenn Sie einen Bewertungsbericht generieren, erstellt Audit Manager eine Prüfsumme für die Berichtsdatei mit dem Namen `digest.txt`. Sie können diese Datei verwenden, um die Integrität des Berichts zu überprüfen und sicherzustellen, dass nach der Erstellung des Berichts keine Nachweise mehr geändert wurden. Sie enthält ein JSON-Objekt mit Signaturen und Hashes, die ungültig werden, wenn ein Teil des Berichtsarchivs geändert wird.

Verwenden Sie die von Audit Manager bereitgestellte ValidateAssessmentReportIntegrityAPI, um die Integrität eines Bewertungsberichts zu überprüfen.

Weitere Ressourcen

Antworten auf häufig gestellte Fragen und Probleme finden Sie Behebung von Bewertungsberichtfehlern im Abschnitt zur Fehlerbehebung in diesem Handbuch.

Beweissuche

Die Beweissuche bietet eine leistungsstarke Methode zur Suche nach Beweisen in Audit Manager. Anstatt tief verschachtelte Beweisordner zu durchsuchen, um das Gesuchte zu finden, können Sie jetzt die Beweissuche verwenden, um Ihre Beweise schnell abzufragen. Wenn Sie ein delegierter Administrator für Audit Manager sind, aktivieren Sie die Beweissuche, um nach Beweisen für alle Mitgliedskonten in Ihrem Unternehmen zu suchen.

Mithilfe einer Kombination aus Filtern und Gruppierungen können Sie den Umfang Ihrer Suchabfrage schrittweise einschränken. Wenn Sie sich beispielsweise einen umfassenden Überblick über den Zustand Ihres Systems verschaffen möchten, führen Sie eine umfassende Suche durch und filtern Sie nach Bewertung, Datumsbereich und Ressourcen-Compliance. Wenn Sie eine bestimmte Ressource korrigieren wollen, können Sie eine eingeschränkte Suche durchführen, um gezielt nach Beweisen für eine bestimmte Kontrollelement- oder Ressourcen-ID zu suchen. Nachdem Sie Ihre Filter definiert haben, können Sie die entsprechenden Suchergebnisse gruppieren und anschließend per Vorschau anzeigen, bevor Sie einen Bewertungsbericht erstellen.

Um die Beweissuche zu verwenden, müssen Sie dieses Feature in Ihren Audit Manager-Einstellungen aktivieren.

Wichtige Punkte

Verstehen Sie, wie Evidence Finder mit CloudTrail Lake funktioniert

Die Beweissuche verwendet die Abfrage- und Speicherfunktionen von AWS CloudTrail Lake. Bevor Sie Evidence Finder verwenden, ist es hilfreich, etwas mehr über die Funktionsweise von CloudTrail Lake zu erfahren.

CloudTrail Lake aggregiert Daten in einem einzigen, durchsuchbaren Ereignisdatenspeicher, der leistungsstarke SQL-Abfragen unterstützt. Das bedeutet, dass Sie in Ihrem gesamten Unternehmen und innerhalb benutzerdefinierter Zeiträume nach Daten suchen können. Mit der Beweissuche können Sie diese Suchfunktion direkt in der Audit-Manager-Konsole verwenden.

Wenn Sie die Aktivierung der Beweissuche anfragen, erstellt Audit Manager in Ihrem Namen einen Ereignisdatenspeicher. Nachdem die Beweissuche aktiviert wurde, werden alle Ihre künftigen Audit-Manager-Beweise in den Ereignisdatenspeicher aufgenommen, wo sie für Suchanfragen in der Beweissuche zur Verfügung stehen. Wenn die Beweissuche aktiviert wurde, füllen wir den neu

erstellten Ereignisdatenspeicher mit Ihren bisherigen Beweisen aus bis zu zwei Jahren auf. Wenn Sie die Beweissuche als delegierter Administrator aktivieren, füllen wir die Daten für alle Mitgliederkonten in Ihrem Unternehmen auf.

Alle Beweisdaten, unabhängig davon, ob sie aufgefüllt oder neu sind, werden 2 Jahre lang im Ereignisdatenspeicher aufbewahrt. Sie können die standardmäßige Aufbewahrungsfrist jederzeit ändern. Anweisungen dazu finden Sie im AWS CloudTrail -Benutzerhandbuch unter Aktualisieren eines Ereignisdatenspeichers. Ereignisdaten können bis zu sieben Jahre bzw. 2.555 Tage in einem Ereignisdatenspeicher aufbewahrt werden.

> **Note**
>
> Wenn dem Ereignisdatenspeicher neue Beweisdaten hinzugefügt werden, fallen CloudTrail Lake-Gebühren für die Datenspeicherung und Datenaufnahme an.
> Bei CloudTrail Lake-Abfragen zahlen Sie nutzungsabhängig. Das bedeutet, dass Ihnen für jede Suchanfrage, die Sie mit der Beweissuche ausführen, die durchsuchten Daten in Rechnung gestellt werden.
> Weitere Informationen zu den Preisen von CloudTrail Lake finden Sie unter AWS CloudTrail Preise.

Nächste Schritte

Um zu beginnen, aktivieren Sie den Evidence Finder in Ihren Audit Manager Manager-Einstellungen. Detaillierte Anweisungen finden Sie unter Beweissuche aktivieren.

Weitere Ressourcen

- Im Evidence Finder nach Beweisen suchen
- Ergebnisse in der Beweissuche anzeigen
- Filter- und Gruppierungsoptionen für den Evidence Finder
- Beispielhafte Anwendungsfälle für Evidence Finder
- Behebung von Problemen mit der Beweiserhebung

Im Evidence Finder nach Beweisen suchen

Mit dem Evidence Finder können Sie gezielte Suchen durchführen und schnell relevante Beweise zur Überprüfung finden.

Auf dieser Seite erfahren Sie, wie Sie Ihre Suchanfragen nach Kriterien wie Bewertung, Zeitraum, Compliance-Status der Ressourcen und weiteren Attributen filtern können. Durch die Anwendung dieser Filter wird Ihr Suchbereich auf die von Ihnen benötigten Nachweise eingegrenzt. Sie können Ihre Ergebnisse auch nach bestimmten Feldern gruppieren, um Muster besser analysieren zu können.

Voraussetzungen

Stellen Sie sicher, dass Sie die Schritte zur Aktivierung der Evidence Finder in Ihren Audit Manager Manager-Einstellungen abgeschlossen haben. Detaillierte Anweisungen finden Sie unter Beweissuche aktivieren.

Stellen Sie außerdem sicher, dass Sie berechtigt sind, Suchanfragen im Evidence Finder durchzuführen. Ein Beispiel für eine Berechtigungsrichtlinie, die Sie verwenden können, finden Sie unterErlauben Sie Benutzern, Suchanfragen in der Beweissuche durchzuführen.

Verfahren

Gehen Sie wie folgt vor, um über die Audit Manager-Konsole Beweise zu suchen.

1. Führen Sie eine Suchabfrage durch
2. Beenden Sie eine laufende Suchabfrage (optional)
3. Bearbeiten Sie die Filter für Ihre Suchabfrage (optional)

> **Note**
>
> Sie können die CloudTrail API auch verwenden, um Ihre Beweisdaten abzufragen. Weitere Informationen finden Sie unter StartQuery in der AWS CloudTrail -API-Referenz. Wenn Sie lieber die verwenden möchten AWS CLI, finden Sie weitere Informationen unter Eine Abfrage starten im AWS CloudTrail Benutzerhandbuch.

Durchführen einer Suchabfrage

Gehen Sie wie folgt vor, um eine Suchabfrage in der Beweissuche durchzuführen.

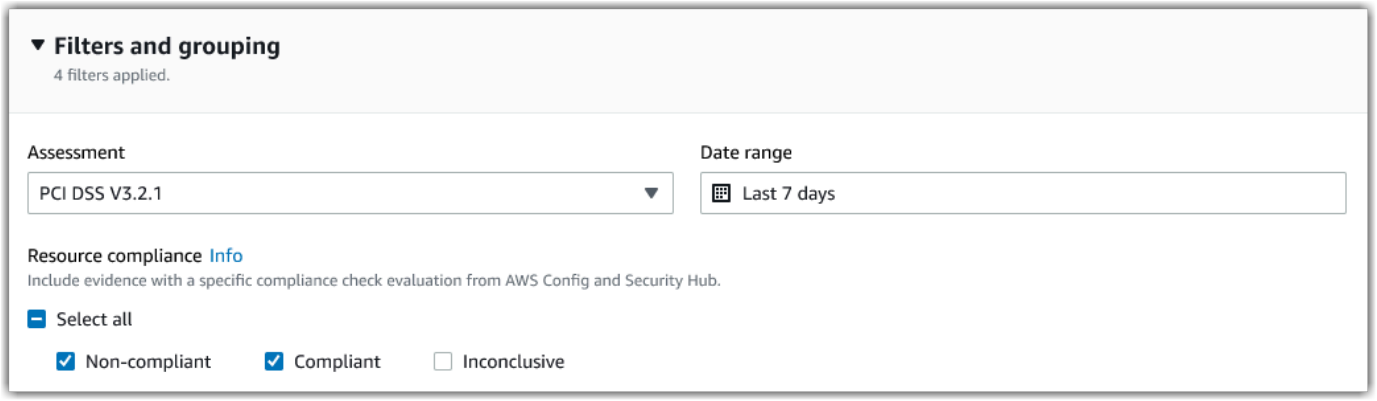
Um nach Beweisen zu suchen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Beweissuche.
3. Wenden Sie als Nächstes Filter an, um den Suchumfang einzuschränken.

   a. Wählen Sie unter Bewertung eine Bewertung aus.

   b. Wählen Sie für Datumsbereich einen Bereich aus.

   c. Für Ressourcen-Compliance wählen einen Bewertungsstatus.

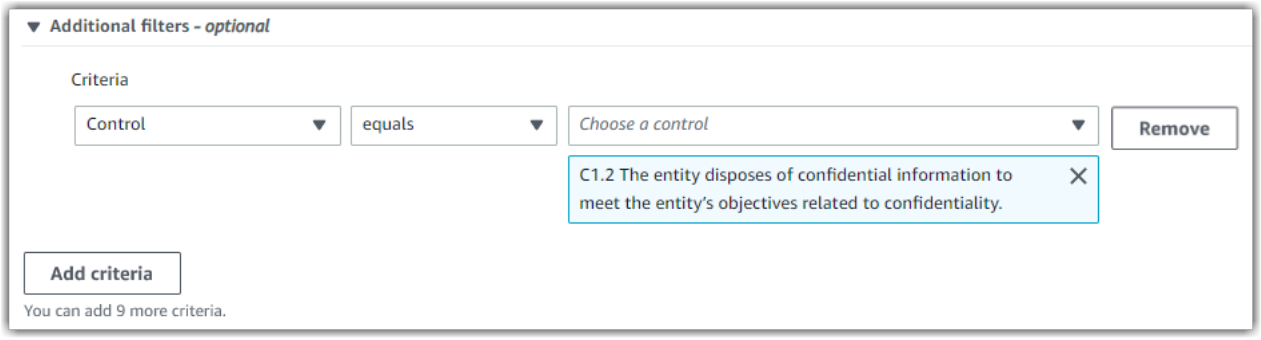


4. (Optional) Wählen Sie Zusätzliche Filter – optional, um die Suche noch weiter einzuschränken.

   a. Wählen Sie Kriterien hinzufügen, wählen Sie ein Kriterium und dann einen oder mehrere Werte für dieses Kriterium aus.

   b. Erstellen Sie weitere Filter auf die gleiche Weise.

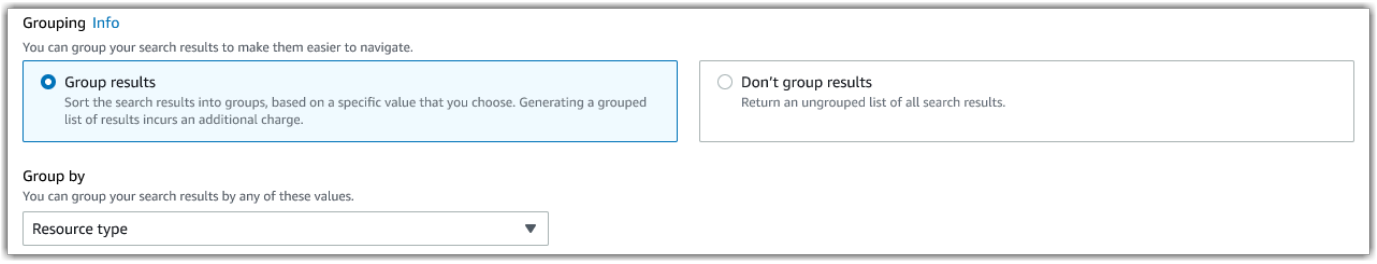
   c. Um einen Filter zu entfernen, wählen Sie Entfernen.



5. Geben Sie bei Gruppierung an, ob Sie die Suchergebnisse gruppieren möchten.

a. Wenn Sie die Ergebnisse gruppieren möchten, wählen Sie einen Wert aus.

b. Wenn Sie die Ergebnisse nicht gruppieren möchten, fahren Sie mit Schritt 6 fort.



6. Wählen Sie Search (Suchen) aus.

Ihre Suche kann einige Minuten dauern, abhängig von der Menge an Beweisdaten, über die Sie verfügen. Sie können die Beweissuche jederzeit verlassen, während die Suche läuft. Eine Flash-Leiste benachrichtigt Sie, wenn die Suchergebnisse fertig sind.

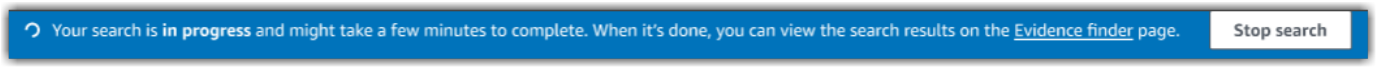
Eine Suchabfrage anhalten

Wenn Sie eine Suchabfrage aus irgendeinem Grund stoppen möchten, gehen Sie folgendermaßen vor.

> **Note**
>
> Das Stoppen einer Suchabfrage kann weiterhin Gebühren verursachen. Ihnen wird nur die Menge an Beweisdaten in Rechnung gestellt, die durchsucht wurde, bis Sie die Suchabfrage beendet haben. Nach dem Beenden können Sie die erfassten Teilergebnisse einsehen.

Stoppen einer laufenden Suchabfrage

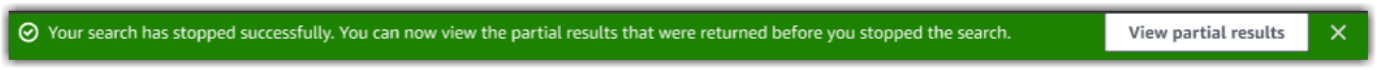
1. Wählen Sie in der blauen Flash-Leiste oben auf dem Bildschirm Suche stoppen aus.



2. (Optional) Überprüfen Sie die Teilergebnisse, die ausgegeben wurden, bevor Sie die Suchabfrage beendet haben.

a. Wenn Sie sich auf der Seite der Beweissuche befinden, werden die Teilergebnisse auf dem Bildschirm angezeigt.

b. Wenn Sie die Beweissuche verlassen haben, wählen Sie in der grünen Bestätigungs-Leiste die Option Teilergebnisse anzeigen aus.



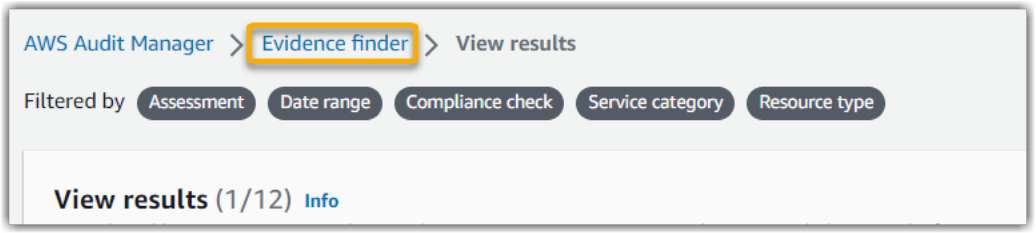
Bearbeiten von Suchfiltern

Gehen Sie wie folgt vor, um zu Ihrer letzten Suchanfrage zurückzukehren, und passen Sie die Filter nach Bedarf an.

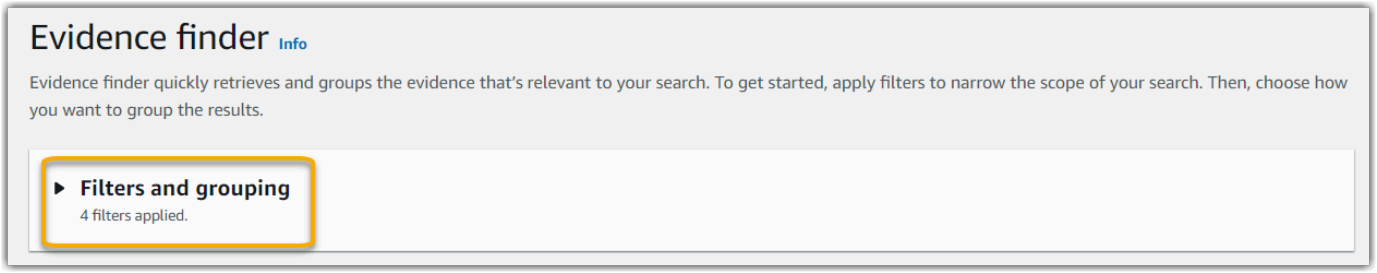
> **Note**
>
> Wenn Sie Ihre Filter bearbeiten und Suchen wählen, wird eine neue Suchabfrage gestartet.

So bearbeiten Sie eine aktuelle Suchabfrage

1. Wählen Sie auf der Seite Ergebnisse anzeigen im Breadcrumb-Navigationsmenü die Option Beweissuche aus.



2. Wählen Sie Filter und Gruppierung, um die Filterauswahl zu erweitern.



3. Bearbeiten Sie als Nächstes Ihre Filter oder starten Sie eine neue Suche.

a. Um Filter zu bearbeiten, passen Sie die aktuelle Auswahl für Filter und Gruppierung an oder entfernen Sie sie.

b. Um von vorn zu beginnen, wählen Sie Filter löschen und wenden Sie die Filter- und Gruppierungsauswahl Ihrer Wahl an.

4. Wählen Sie Suchen, wenn Sie damit fertig sind.

Nächste Schritte

Nachdem Ihre Suche abgeschlossen ist, können Sie sich die Ergebnisse ansehen, die Ihren Suchkriterien entsprechen. Detaillierte Anweisungen finden Sie unter Ergebnisse in der Beweissuche anzeigen.

Weitere Ressourcen

- Filter- und Gruppierungsoptionen für den Evidence Finder
- Beispielhafte Anwendungsfälle für Evidence Finder
- Behebung von Problemen mit der Beweiserhebung

Ergebnisse in der Beweissuche anzeigen

Nachdem Ihre Suche abgeschlossen ist, können Sie sich die Ergebnisse ansehen, die Ihren Suchkriterien entsprechen.

Denken Sie daran, dass bei der Beweiserhebung möglicherweise mehrere Ressourcen geprüft werden. Infolgedessen können Beweise eine oder mehrere verwandte Ressourcen enthalten. In der Beweissuche werden die Ergebnisse auf Ressourcenebene angezeigt, mit einer Zeile für jede Ressource. Sie können eine Vorschau der Zusammenfassung jeder Ressource anzeigen, ohne die Seite verlassen zu müssen.

Nachdem Sie die Suchergebnisse überprüft haben, können Sie einen Bewertungsbericht erstellen, der diese Beweise enthält. Sie können Ihre Suchergebnisse auch in eine CSV-Datei exportieren.

> **Important**
>
> Wir empfehlen Ihnen, die Beweissuche so lange geöffnet zu lassen, bis Sie die Untersuchung Ihrer Suchergebnisse abgeschlossen haben. Ihre Suchergebnisse werden verworfen, wenn Sie die Tabelle Ergebnisse anzeigen verlassen. Bei Bedarf können Sie Ihre aktuellen Ergebnisse in der CloudTrail Konsole unter einsehen https://console.aws.amazon.com/cloudtrail/. Hier werden die Ergebnisse Ihrer Suchanfragen sieben Tage lang aufbewahrt. Beachten Sie jedoch, dass Sie aus Ihren Suchergebnissen in der CloudTrail Konsole keinen Bewertungsbericht erstellen können.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie die Schritte zur Durchführung einer Suche im Evidence Finder bereits befolgt haben.

Verfahren

Gehen Sie wie folgt vor, um Ihre Suchergebnisse im Evidence Finder anzuzeigen.

Aufgaben

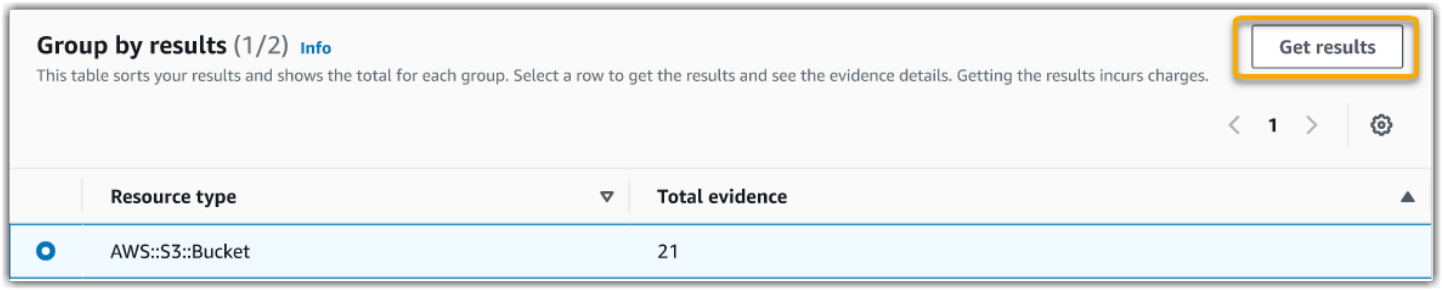
- Schritt 1. Anzeigen der gruppierten Ergebnisse
- Schritt 2. Anzeigen der Ergebnisse
  - Verwaltung Ihrer Anzeigeeinstellungen
  - Vorschau von Ressourcenzusammenfassungen anzeigen

Schritt 1. Anzeigen der gruppierten Ergebnisse

Wenn Sie Ihre Ergebnisse gruppiert haben, können Sie die Gruppierungen überprüfen, bevor Sie sich eingehender mit den Beweisen befassen.

> **Note**
>
> Wenn Sie die Ergebnisse nicht gruppiert haben, zeigt die Beweissuche die Tabelle Gruppieren nach Ergebnissen nicht an. Stattdessen werden Sie direkt zur Tabelle Ergebnisse anzeigen weitergeleitet.

Verwenden Sie die Tabelle Nach Ergebnissen gruppieren, um zu erfahren, wie umfangreich die passenden Beweise sind und wie sie innerhalb einer bestimmten Dimension verteilt sind. Die Ergebnisse werden nach dem von Ihnen ausgewählten Wert gruppiert. Wenn Sie beispielsweise nach Ressourcentyp gruppiert haben, zeigt die Tabelle eine Liste von AWS Ressourcentypen. In der Spalte Gesamte Beweise wird die Anzahl der übereinstimmenden Ergebnisse für jeden Ressourcentyp angezeigt.



Um die Ergebnisse für eine Gruppe zu erhalten

1. Wählen Sie in der Tabelle Gruppieren nach Ergebnissen die Zeile für die Ergebnisse aus, die Sie abrufen möchten.
2. Wählen Sie Ergebnisse abrufen aus. Dadurch wird eine neue Suchabfrage gestartet und Sie werden zur Tabelle Ergebnisse anzeigen weitergeleitet, in der Sie die Ergebnisse für diese Gruppe sehen können.

Schritt 2. Anzeigen der Ergebnisse

In der Tabelle Ergebnissen anzeigen werden Ihre Suchergebnisse angezeigt. Von hier aus können Sie Ihre Anzeigeeinstellungen verwalten und eine Vorschau der Ressourcenzusammenfassungen anzeigen.

Verwaltung Ihrer Anzeigeeinstellungen

Ihre Anzeigeeinstellungen bestimmen, was Sie auf der Ergebnisseite sehen.

Um Ihre Anzeigeeinstellungen zu verwalten

1. Wählen Sie das Einstellungssymbol (#) oben in der Tabelle Ergebnisse anzeigen.
2. Überprüfen und ändern Sie nach Bedarf die folgenden Einstellungen:

Einstellung	Description
Wählen Sie sichtbare Tabellenspalten aus	Verwenden Sie die Umschaltoption, um zu ändern, welche Spalten angezeigt werden.
Größe der Seite	Wählen Sie ein Optionsfeld aus, um festzulegen, wie viele Ergebnisse auf jeder Seite angezeigt werden.
Wrap Text	Aktivieren Sie das Kontrollkästchen, um lange Textzeilen zur besseren Lesbarkeit umzubrechen.

3. Wählen Sie Bestätigen, um Ihre Einstellungen zu speichern.

Vorschau von Ressourcenzusammenfassungen anzeigen

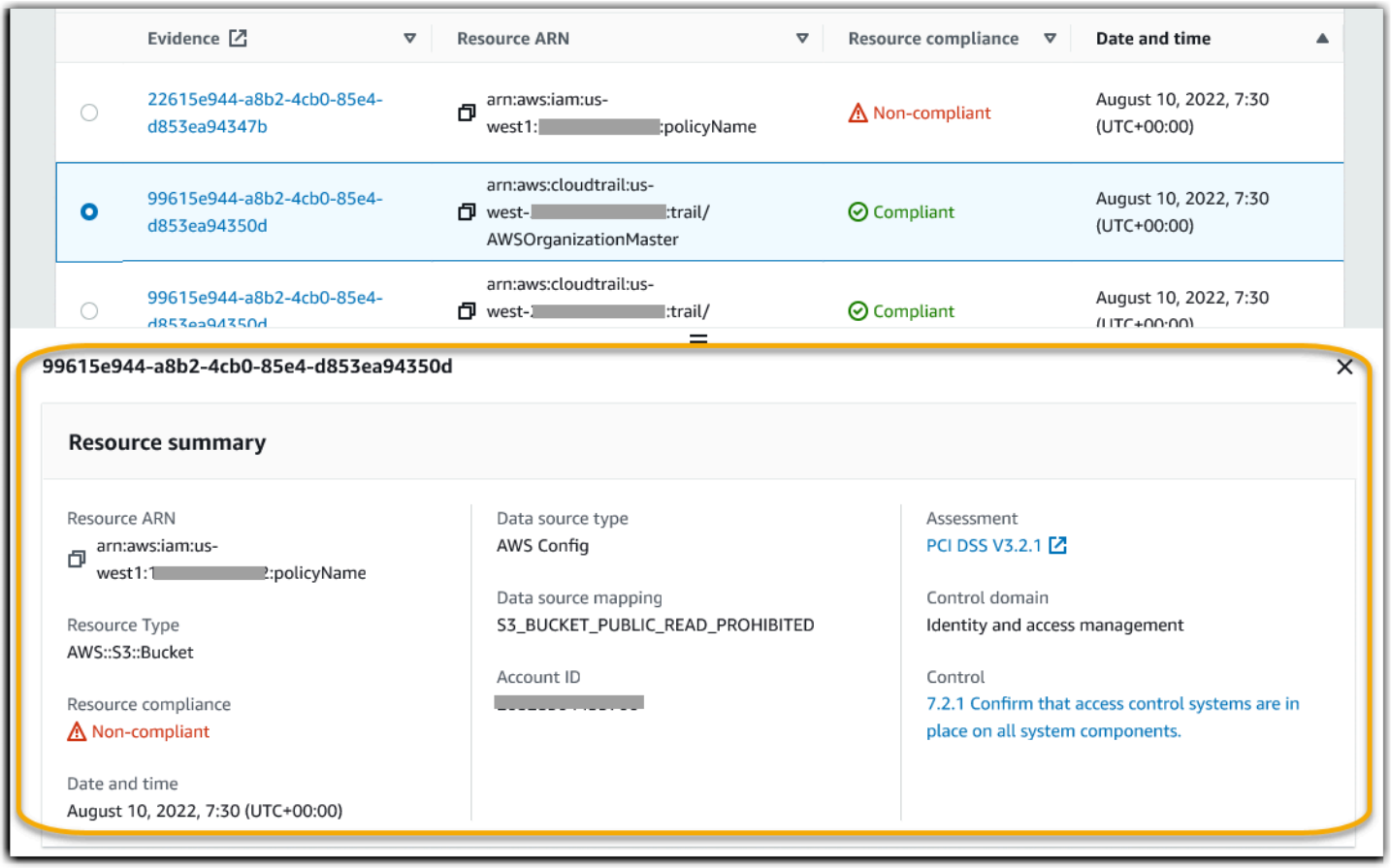
Sie können eine Vorschau der zugehörigen Ressourcen anzeigen, um die Beweise zu finden, die Ihrer Suchabfrage entsprechen. Auf diese Weise können Sie feststellen, ob die Suchabfrage die gewünschten Ergebnisse geliefert hat oder ob Sie Ihre Filter anpassen und die Suchabfrage erneut ausführen müssen.

Denken Sie daran, dass Beweise eine oder mehrere verwandte Ressourcen enthalten können. Die Beweissuche zeigt Ergebnisse auf Ressourcenebene an (mit einer Zeile für jede Ressource).

> **Note**
>
> Die Beweissuche gibt Ergebnisse für automatisierte und manuelle Beweise zurück. Sie können jedoch nur eine Vorschau der Ressourcenübersichten für automatisierte Beweise anzeigen. Dies liegt daran, dass Audit Manager keine Ressourcenbewertungen für manuelle Beweise durchführt und daher keine Ressourcenübersicht verfügbar ist.
> Um Details zu manuellen Beweisen zusehen, wählen Sie den Namen des Beweises aus, um die Seite mit den Beweisdetails zu öffnen. Wenn Sie anhand der Ergebnisse Ihrer Beweissuche einen Bewertungsbericht erstellen, sind die Einzelheiten der manuellen Beweise im Bewertungsbericht enthalten.

Um eine Vorschau der Ressourcen-Zusammenfassungen anzuzeigen

1. Aktivieren Sie das Kontrollkästchen neben einem Ergebnis. Dadurch wird auf der aktuellen Seite ein Bereich mit der Zusammenfassung der Ressourcen geöffnet.
2. (Optional) Um die vollständigen Details der zugehörigen Beweise zu sehen, wählen Sie den Namen des Beweises aus.
3. (Optional) Verwenden Sie die horizontalen Linien (=), um den Bereich mit der Ressourcenzusammenfassung und seine Größe zu ändern.
4. Wählen Sie (x), um den Bereich mit der Ressourcenzusammenfassung zu schließen.



Nächste Schritte

Nachdem Sie Ihre Suchergebnisse überprüft haben, können Sie daraus einen Bewertungsbericht erstellen oder sie als CSV-Datei exportieren. Detaillierte Anweisungen finden Sie unter Exportieren Sie Ihre Suchergebnisse aus dem Evidence Finder.

Weitere Ressourcen

- Filter- und Gruppierungsoptionen für den Evidence Finder
- Beispielhafte Anwendungsfälle für Evidence Finder
- Behebung von Problemen mit der Beweiserhebung

Exportieren Sie Ihre Suchergebnisse aus dem Evidence Finder

Nachdem Sie Ihre Suchergebnisse überprüft haben, können Sie auf der Grundlage dieser Ergebnisse einen Bewertungsbericht erstellen. Alternativ können Sie Ihre Evidence Finder-Suchergebnisse in eine CSV-Datei exportieren.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie die Schritte zum Durchführen einer Suche und zum Überprüfen Ihrer Suchergebnisse im Evidence Finder bereits befolgt haben.

Verfahren

Inhalt

Generieren eines Bewertungsberichts anhand Ihrer Suchergebnisse

Wenn Sie mit den Suchergebnissen zufrieden sind, können Sie einen Bewertungsbericht erstellen.

Zur Generierung eines Bewertungsberichts aus Ihren Suchergebnissen

1. Wählen Sie oben in der Tabelle mit Ergebnisse anzeigen die Option Bewertungsbericht erstellen.
2. Geben Sie einen Namen und eine Beschreibung für Ihren Bewertungsbericht ein und überprüfen Sie die Details des Bewertungsberichts.
3. Wählen Sie Bewertungsbericht erstellen.

Es dauert einige Minuten, bis Ihr Bewertungsbericht erstellt ist. Sie können währenddessen die Beweissuche verlassen. Eine grüne Erfolgsmeldung bestätigt, dass der Bericht fertig ist. Sie können dann zum Audit Manager Downloadcenter gehen und Ihren Bewertungsbericht herunterladen.

> **Note**
>
> Audit Manager generiert einen einmaligen Bericht, der nur die Beweise aus den Suchergebnissen verwendet. Dieser Bericht enthält keine Nachweise, die manuell von der Bewertungsseite aus zu einem Bericht hinzugefügt wurden.
> Es gelten Beschränkungen dafür, wie viele Beweise in einen Bewertungsbericht aufgenommen werden können. Weitere Informationen finden Sie unter Behebung von Problemen mit der Beweiserhebung.

Exportieren Sie Ihre Suchergebnisse in eine CSV-Datei

Möglicherweise benötigen Sie eine portable Version der Ergebnisse Ihrer Beweissuche. In diesem Fall können Sie Ihre Suchergebnisse in eine CSV-Datei exportieren.

Nachdem Sie Ihre Suchergebnisse exportiert haben, ist die CSV-Datei sieben Tage lang im Audit Manager-Downloadcenter verfügbar. Eine Kopie der CSV-Datei wird auch an Ihren bevorzugten S3-Bucket gesendet, der als Exportziel bezeichnet wird. Ihre CSV-Datei bleibt in diesem Bucket verfügbar, bis Sie diese Datei löschen.

Audit Manager verwendet CloudTrail Lake-Funktionen, um CSV-Dateien aus dem Evidence Finder zu exportieren und bereitzustellen. Die folgenden Faktoren definieren, wie der CSV-Exportprozess funktioniert:

- Ihre Suchergebnisse sind in der CSV-Datei enthalten. Wenn Sie nur bestimmte Suchergebnisse aufnehmen möchten, empfehlen wir, Ihre aktuellen Suchfilter zu bearbeiten. Auf diese Weise können Sie Ihre Ergebnisse einschränken, sodass nur die Beweise angezeigt werden, die Sie exportieren möchten.
- CSV-Dateien werden im komprimierten GZIP-Format exportiert. Der standardmäßige CSV-Dateiname lautet `queryID/result.csv.gz`, wobei `queryID` die ID Ihrer Suchabfrage ist.
- Die maximale Dateigröße für einen CSV-Export beträgt 1 TB. Wenn Sie mehr als 1 TB an Daten exportieren, werden Ihre Ergebnisse in mehr als eine Datei aufgeteilt. Jede CSV-Datei ist mit `result_number.csv.gz` benannt. Die Anzahl der CSV-Dateien, die Sie erhalten, hängt von

der Gesamtgröße Ihrer Suchergebnisse ab. Wenn Sie beispielsweise 2 TB an Daten exportieren, erhalten Sie zwei Dateien mit Abfrageergebnissen: `result_1.csv.gz` und`result_2.csv.gz`.

- Zusätzlich zur CSV-Datei wird eine JSON-Signaturdatei an Ihren S3-Bucket übermittelt. Diese Datei dient als Prüfsumme, um zu überprüfen, ob die Informationen in der CSV-Datei korrekt sind. Weitere Informationen finden Sie im AWS CloudTrail Entwicklerhandbuch unter Struktur CloudTrail signieren. Mithilfe der Integritätsprüfung der Abfrageergebnisse können Sie feststellen, ob die CloudTrail Abfrageergebnisse nach ihrer Übermittlung geändert, gelöscht oder unverändert geblieben sind. Anweisungen finden Sie im AWS CloudTrail -Entwicklerhandbuch unter Überprüfen von gespeicherten Abfrageergebnissen.

> **Note**
>
> Manuelle Beweise mit Textantworten sind derzeit nicht in der Vorschau oder in CSV-Exporten enthalten. Um Textbeantworten zu sehen, wählen Sie in den Ergebnissen Ihrer Beweissuche den Namen der manuellen Beweise aus, um die Seite mit den Nachweisdetails zu öffnen. Wenn Sie Textantworten außerhalb der Audit Manager Konsole anzeigen müssen, empfehlen wir Ihnen, anhand der Ergebnisse Ihrer Beweissuche einen Bewertungsbericht zu erstellen. Alle manuellen Beweisdetails, einschließlich Textantworten, sind in den Bewertungsberichten enthalten.

Erstmaligerer Export von Ergebnissen

Führen Sie die folgenden Schritte aus, wenn Sie Ihre Suchergebnisse zum ersten Mal exportieren. Dieses Verfahren gibt Ihnen die Möglichkeit, ein Standardexportziel für alle künftigen Exporte anzugeben. Wenn Sie derzeit kein Standard-Exportziel speichern möchten, können Sie dies später tun, indem Sie Ihre Exportzieleinstellungen aktualisieren.

> **Important**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie über einen S3-Bucket verfügen, den Sie als Exportziel verwenden können. Sie können einen Ihrer vorhandenen S3-Buckets verwenden oder einen neuen Bucket in Amazon S3 erstellen. Für optimale Sicherheit und Leistung empfehlen wir, einen S3-Bucket zu verwenden, der sich in demselben AWS Konto und in derselben Region wie bei Ihrer Bewertung befindet. Darüber hinaus muss Ihr S3-Bucket über die erforderlichen Berechtigungsrichtlinien verfügen, CloudTrail damit die Exportdateien in ihn geschrieben werden können. Insbesondere muss die Bucket-Richtlinie eine `s3:PutObject`

Aktion und den Bucket-ARN enthalten und CloudTrail als Dienstprinzipal auflisten. Wir stellen Ihnen ein Beispiel für eine Berechtigungsrichtlinie zur Verfügung, die Sie befolgen können. Anweisungen zum Anhängen dieser Richtlinie an Ihren S3-Bucket finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3-Konsole.
Weitere Tipps finden Sie unterKonfigurationstipps für Ihr Exportziel. Falls beim Exportieren einer CSV-Datei Probleme auftreten, finden Sie weitere Informationen untercsv-exports.

So exportieren Sie Ihre Suchergebnisse (erstmalige Ausführung)

1. Wählen Sie oben in der Tabelle Ergebnisse anzeigen die Option Export CSV.
2. Geben Sie den S3-Bucket an, an den die Datei exportiert werden soll.
   - Wählen Sie S3 durchsuchen, um aus einer Liste Ihrer Buckets auszuwählen.
   - Alternativ können Sie den Bucket-URI in diesem Format eingeben: **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Um Ihren Ziel-Bucket zu organisieren, können Sie einen optionalen Ordner für Ihre CSV-Exporte erstellen. Hängen Sie dazu einen Schrägstrich (**`/`**) und ein Präfix an den Wert im Feld Ressourcen-URI an (z. B. **`/evidenceFinderExports`**). Audit Manager fügt dann dieses Präfix hinzu, wenn es die CSV-Datei zum Bucket hinzufügt, und Amazon S3 generiert den durch das Präfix angegebenen Pfad. Weitere Informationen zu Präfixen in Amazon S3 finden Sie unter Organisieren von Objekten in der Amazon S3-Konsole im Amazon Simple Storage Service-Benutzerhandbuch.
3. (Optional) Wenn Sie diesen Bucket nicht als Standard-Exportziel speichern möchten, deaktivieren Sie unter meine Beweissuche-Einstellungen das Kontrollkästchen Diesen Bucket als Standardexportziel speichern.
4. Wählen Sie Export aus.

Exportieren Sie Ihre Ergebnisse, nachdem Sie ein Exportziel festgelegt haben

Nachdem Sie einen Standard-S3-Bucket als Standardexportziel gespeichert haben, können Sie in Zukunft die folgenden Schritte ausführen.

Um Ihre Suchergebnisse zu exportieren (nachdem Sie ein Standard-Exportziel gespeichert haben)

1. Wählen Sie oben in der Tabelle Ergebnisse anzeigen die Option Export CSV.
2. Überprüfen Sie in der angezeigten Eingabeaufforderung den Standard-S3-Bucket, in dem Ihre exportierte Datei gespeichert werden soll.

   a. (Optional) Um diesen Bucket weiterhin zu verwenden und diese Meldung in Zukunft auszublenden, aktivieren Sie das Kontrollkästchen Nicht mehr erinnern.

   b. (Optional) Um diesen Bucket zu ändern, gehen Sie wie folgt vor, um Ihre Exportzieleinstellungen zu aktualisieren.
3. Wählen Sie Bestätigen aus.

Je nachdem, wie viele Daten Sie exportieren, kann es einige Minuten dauern, bis der Exportvorgang abgeschlossen ist. Sie können die Beweissuche jederzeit verlassen, während der Export läuft. Wenn Sie die Beweissuche verlassen, wird Ihre Suche gestoppt und Ihre Suchergebnisse werden in der Konsole verworfen. Der CSV-Exportprozess wird jedoch im Hintergrund fortgesetzt. Die CSV-Datei enthält alle Suchergebnisse, die Ihrer Anfrage entsprachen.

Anzeige Ihrer Ergebnisse nach dem Export

Gehen Sie zum Audit Manager, um Ihre CSV-Datei zu finden und ihren Status zu überprüfenAudit Manager Download-Center. Wenn die exportierte Datei fertig ist, können Sie Ihre CSV-Datei aus dem Downloadcenter herunterladen.

Sie können die CSV-Datei auch in Ihrem S3-Bucket Ihres Exportziels suchen und herunterladen.

So suchen Sie die CSV-Datei und Sign-Datei in der Amazon S3-Konsole

1. Öffnen Sie die Amazon S3-Konsole.
2. Wählen Sie den Export-Bucket aus, den Sie beim Export Ihrer CSV-Datei angegeben haben.
3. Navigieren Sie durch die Objekthierarchie, bis Sie die CSV- und Sign-Dateien finden. Die CSV-Datei hat eine Erweiterung `.csv.gz` und die Sign-Datei hat die Erweiterung `.json`.

Sie navigieren dabei durch eine Objekthierarchie, die dem folgenden Beispiel ähnelt, Name des Exportzielort-Bucket, Konto-ID, Datum und Abfrage-ID sind jedoch anders.

```
All Buckets
```

```
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

Weitere Ressourcen

- Behebung von Problemen mit der Beweiserhebung
- Konfiguration Ihres Standardexportziels für Evidence Finder

Filter- und Gruppierungsoptionen für den Evidence Finder

Auf dieser Seite finden Sie eine Liste der Filter- und Gruppierungsoptionen, die Sie in Evidence Finder verwenden können.

Referenz filtern

Sie können die folgenden Filter verwenden, um Beweise zu finden, die bestimmten Kriterien entsprechen, z. B. einer Bewertung, Kontrolle oder AWS-Service.

Topics

- Erforderliche Filter
- Zusätzliche Filter (optional)
- Kombinieren von Filtern

Erforderliche Filter

Verwenden Sie diese Filter, wenn Sie einen allgemeinen Überblick zu den Beweisen zu einer Bewertung wünschen.

Name des Filters	Description	Hinweise
Bewertung	Gibt Beweise für eine bestimmte Bewertung zurück.	Sie können nur nach einer Bewertung filtern.
Datumsbereich	Gibt Beweise für einen bestimmten Zeitraum zurück.	Sie können entweder einen relativen Bereich verwenden, um einen Bereich zu definieren, der sich auf das heutige Datum bezieht (z. B. **`Last 30 days`**). Oder Sie können einen absoluten Bereich verwenden, um einen bestimmten Datumsbereich anzugeben (z. B. **`June 27th - July 4th`**).
Ressourcen-Compliance	Gibt Ressourcen zurück, für die eine bestimmte Compliance-Überprüfung durchgeführt wurde.	Audit Manager sammelt Nachweise zur Konformitätsprüfung für Kontrollen, die Security Hub CSPM als Datenquellentyp verwenden AWS Config . Bei dieser Beweissuche können mehrere Ressourcen bewertet werden. Daher kann ein einziger Beweis für die Compliance-Überprüfung eine oder mehrere Ressourcen umfassen. Sie können diesen Filter verwenden, um den Compliance-Status auf Ressourcenebene zu untersuchen. Sie können eine oder mehrere der folgenden Optionen wählen: • Nicht konform – Dieser Filter findet Ressourcen mit Problemen bei der Compliance-Überprüfung. Dies passiert, wenn Security Hub ein Fehlerergebnis oder ein nicht konformes Ergebnis AWS Config meldet. • Konform – Dieser Filter findet Ressourcen, bei denen keine Probleme mit der Compliance-Überprüfung aufgetreten sind. Dies passiert, wenn Security Hub CSPM ein Pass-Ergebnis

Name des Filters	Description	Hinweise
		oder ein Compliance-Ergebnis AWS Config meldet. • Nicht eindeutig – Dieser Filter findet Ressourcen, für die keine Compliance-Überprüfung verfügbar oder anwendbar ist. Dies passiert, wenn eine AWS Config Ressource Security Hub CSPM als zugrunde liegenden Datenquellentyp verwendet , diese Dienste jedoch nicht aktiviert sind. Dies ist auch der Fall, wenn die Ressource einen zugrunde liegenden Datenquellentyp verwendet , der keine Konformitätsprüfungen unterstützt (z. B. manuelle Nachweise, AWS API-Aufrufe oder CloudTrail).

Zusätzliche Filter (optional)

Verwenden Sie diese Filter, um den Umfang Ihrer Suchabfrage einzugrenzen. Verwenden Sie beispielsweise Service, um alle Beweise zu sehen, die sich auf Amazon S3 beziehen. Verwenden Sie den Ressourcentyp, um sich nur auf S3-Buckets zu konzentrieren. Oder verwenden Sie Ressource ARN, um auf einen bestimmten S3-Bucket abzuzielen.

Sie können zusätzliche Filter mit einem oder mehreren der folgenden Kriterien erstellen.

Name des Kriteriums	Description	Wann sollten diese Kriterien verwendet werden
Konto-ID	Drilldown nach AWS-Konto.	Verwenden Sie diese Kriterien, um Beweise zu finden, die sich auf ein bestimmtes AWS-Konto beziehen.
Kontrolle	Aufschlüsselung nach Namen der Kontrolle.	Verwenden Sie diese Kriterien, um Beweise zu finden, die sich auf eine bestimmte Kontrolle beziehen.

Name des Kriteriums	Description	Wann sollten diese Kriterien verwendet werden
Kontrolldomaine	Aufschlüsselung nach Kontrolldomäne.	Verwenden Sie diese Kriterien, um sich bei der Vorbereitung auf ein Audit auf einen bestimmten Themenbereich zu konzentrieren. Sie können nach Kontrolldomäne filtern, wenn Sie eine Bewertung abfragen, die auf Basis eines Standard-Frameworks erstellt wurde. Zu den Kontrolldomänen gehören beispielsweise Netzwerksicherheit, Identitäts- und Zugriffsmanagement sowie Datenschutz. Einige Kontrolldomänen werden möglicherweise als veraltet markiert, nachdem Audit Manager auf eine neue Gruppe von Kontrolldomänen umgestellt hat, die von AWS Control Catalog bereitgestellt werden. Weitere Informationen finden Sie unter Ich sehe, dass eine Kontrolldomäne als „veraltet“ markiert ist. Was bedeutet das?.
Data source type (Datenquellentyp)	Aufschlüsselung nach Datenquellentyp.	Verwenden Sie diese Kriterien, um sich auf eine bestimmte Datenquelle zu konzentrieren. Legen Sie den Wert auf `Manual` fest, um Beweise zu finden, die Sie manuell hochgeladen haben. Andernfalls können Sie automatisierte Beweise danach filtern, woher sie stammen (z. B. `AWS Config`, `CloudTrail` , `Security Hub CSPM` oder`AWS API calls`).

Name des Kriteriums	Description	Wann sollten diese Kriterien verwendet werden
Ereignisname	Aufschlüsselung nach Ereignisnamen.	Verwenden Sie diese Kriterien, um sich auf ein bestimmtes Ereignis zu konzentrieren, auf das sich die Beweise beziehen. Ein Ereignis ist der Datensatz zu einer Aktivität in einem AWS-Konto-Konto. Sie können beispielsweise nach dem Namen eines API-Aufrufs suchen, z. B. nach dem `AttachRolePolicy` - IAM-Vorgang, der zur Konfiguration von Berechtigungen verwendet wird. Oder suchen Sie nach einem CloudTrail Schlüsselwort, z. B. nach dem `ConsoleLogin` Ereignis, das protokolliert wird, CloudTrail wenn sich ein Benutzer bei Ihrem Konto anmeldet.
ARN-Ressourcen	Aufschlüsselung nach Amazon-Ressourcenname (ARN).	Verwenden Sie diese Kriterien, um Beweise zu finden, die sich auf eine bestimmte AWS -Ressource beziehen.
Ressourcentyp	Aufschlüsselung nach Ressourcentyp.	Verwenden Sie diese Kriterien, um sich auf die Art der Ressource zu konzentrieren, die bewertet wird, z. B. eine EC2 Amazon-Instance oder ein S3-Bucket.
Service	Gehen Sie nach AWS-Service Namen genauer vor.	Verwenden Sie diese Kriterien, um Beweise zu finden, die sich auf ein bestimmtes Objekt beziehen AWS-Service, z. B. Amazon EC2, Amazon S3 oder AWS Config.
Servicekategorie	Nach AWS-Service Kategorien aufschlüsseln.	Verwenden Sie diese Kriterien, um sich auf eine bestimmte Kategorie von zu konzentrieren AWS-Service. Zu den Beispielen gehören Sicherheit, Identität und Compliance, Datenbank und Speicher.

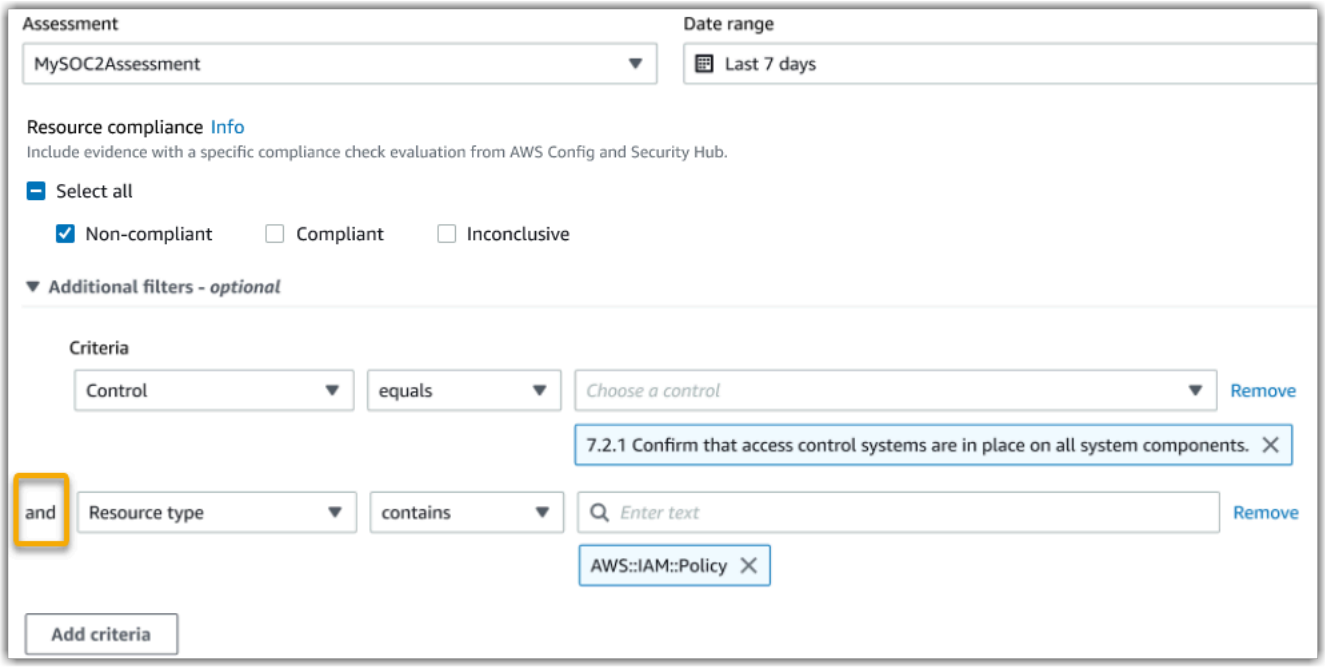
Kombinieren von Filtern

Verhalten der Kriterien

Wenn Sie mehr als ein Kriterium angeben, wendet Audit Manager den AND-Operator auf Ihre Auswahl an. Das bedeutet, dass alle Kriterien in einer einzigen Abfrage zusammengefasst sind und die Ergebnisse allen kombinierten Kriterien entsprechen müssen.

Beispiel

In der folgenden Filtereinstellung gibt die Beweissuche nicht-konforme Ressourcen aus den letzten 7 Tagen für die Beurteilung mit dem Namen **`MySOC2Assessment`** zurück. Darüber hinaus beziehen sich die Ergebnisse sowohl auf eine IAM-Richtlinie als auch auf die angegebene Kontrolle.

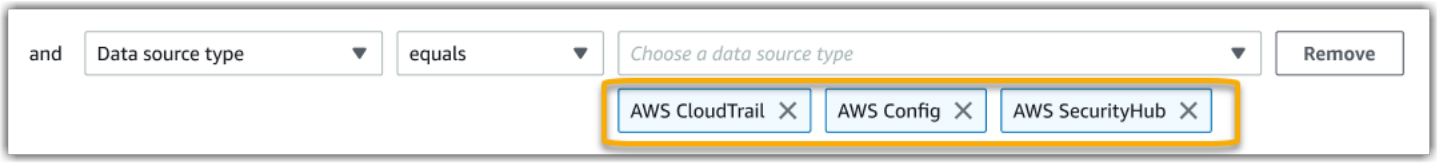


Verhalten des Kriterienwerts

Wenn Sie mehr als einen Kriterienwert angeben, werden die Werte mit einem OR-Operator verknüpft. Die Beweissuche gibt Ergebnisse aus, die einem dieser Kriterienwerte entsprechen.

Beispiel

In der folgenden Filterkonfiguration gibt Evidence Finder Suchergebnisse zurück, die entweder von AWS CloudTrail AWS Config, oder stammen AWS Security Hub CSPM.



Referenz zur Gruppierung

Sie können Ihre Suchergebnisse für eine schnellere Navigation gruppieren. Die Gruppierung zeigt Ihnen, wie breit Ihre Suchergebnisse sind und wie sie über eine bestimmte Dimension verteilt sind.

Sie können einen der folgenden Gruppierungswerte verwenden.

Gruppierung nach	Description
Konto-ID	Gruppieren Sie die Ergebnisse nach AWS-Konto.
Kontrolle	Ergebnisse nach dem Namen der Kontrolle gruppieren.
Data source type (Datenquellentyp)	Gruppieren Sie die Ergebnisse nach der Art der Datenquelle, aus der die Beweise stammen.
Ereignisname	Gruppieren Sie die Ergebnisse nach einem Ereignisnamen.
ARN-Ressourcen	Gruppieren Sie die Ergebnisse nach dem Amazon-Ressourcenname (ARN).
Ressourcentyp	Gruppieren Sie die Ergebnisse nach Ressourcentyp.
Service	Gruppieren Sie die Ergebnisse nach AWS-Service Namen.
Servicekategorie	Gruppieren Sie die Ergebnisse nach AWS-Service Kategorien.

Beispielhafte Anwendungsfälle für Evidence Finder

Der Beweissuche kann Ihnen bei verschiedenen Anwendungsfällen helfen. Diese Seite enthält einige Beispiele und schlägt die Suchfilter vor, die Sie in jedem Szenario verwenden können.

Themen

Anwendungsfall 1: Finden Sie nicht-konforme Beweise und organisieren Sie Delegationen.

Dieser Anwendungsfall ist ideal, wenn Sie als Compliance-Beauftragter, Datenschutzbeauftragter oder GRC-Experte für die Audit-Vorbereitung zuständig sind.

Bei der Überwachung des Compliance-Status in Ihrem Unternehmen können Sie die Hilfe von Partnerteams bei der Behebung von Problemen in Anspruch nehmen. Sie können die Beweissuche verwenden, um Ihre Arbeit für Ihre Partnerteams zu organisieren.

Durch die Anwendung von Filtern können Sie sich jeweils auf die Beweise für einen Bereich konzentrieren. Darüber hinaus können Sie auch die Zuständigkeiten und den Umfang der einzelnen Partnerteams, mit denen Sie zusammenarbeiten, überwachen. Wenn Sie auf diese Weise eine gezielte Suche durchführen, können Sie anhand der Suchergebnisse ermitteln, was in den einzelnen Themenbereichen genau behoben werden muss. Sie können diese nicht-konformen Beweise dann zur Behebung an das entsprechende Partnerteam delegieren.

Folgen Sie für diesen Workflow den Schritten zur Suche nach Beweisen. Verwenden Sie die folgenden Filter, um nicht-konforme Beweise zu finden.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Wenden Sie als Nächstes zusätzliche Filter für den Bereich an, auf den Sie sich konzentrieren. Verwenden Sie beispielsweise den Filter Servicekategorie, um nach nicht-konformen Ressourcen zu suchen, die sich auf IAM beziehen. Teilen Sie diese Ergebnisse dann mit dem Team, das die IAM-Ressourcen für Ihr Unternehmen besitzt. Oder, wenn Sie eine Bewertung abfragen, die anhand eines Standard-Frameworks erstellt wurde, können Sie den Filter für die Kontrolldomäne verwenden, um nach nicht-konformen Beweisen zu suchen, die sich auf die Identitäts- und Zugriffsverwaltungsdomäne beziehen.

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS-Service category that you're focusing on>
```

Nachdem Sie die benötigten Nachweise gefunden haben, folgen Sie den Schritten, um anhand Ihrer Suchergebnisse einen Bewertungsbericht zu erstellen. Detaillierte Anweisungen finden Sie unter

Generieren eines Bewertungsberichts anhand Ihrer Suchergebnisse. Sie können diesen Bericht an Ihr Partnerteam weitergeben, das ihn als Checkliste zur Fehlerbehebung verwenden kann.

Anwendungsfall 2: Identifizieren Sie konforme Beweise

Dieser Anwendungsfall ist ideal SecOps, wenn Sie in einer IT-Abteilung oder einer anderen Rolle arbeitenDevOps, die Cloud-Ressourcen besitzt und verwaltet.

Im Rahmen eines Audits werden Sie möglicherweise gebeten, Probleme mit den Ressourcen, die Sie besitzen, zu beheben. Nachdem Sie dies erledigt haben, können Sie die Beweissuche verwenden, um zu überprüfen, ob Ihre Ressourcen konform sind.

Folgen Sie für diesen Workflow den Schritten zur Suche nach Beweisen. Verwenden Sie die folgenden Filter, um konforme Beweise zu finden.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Wenden Sie als Nächstes zusätzliche Filter an, um nur die Beweise anzuzeigen, für die Sie verantwortlich sind. Je nach Umfang Ihrer Eigentümer-Rolle sollten Sie die Suche so zielgerichtet wie nötig durchführen. Die folgenden Filterbeispiele sind von weit bis eng sortiert. Wählen Sie die für Sie geeigneten Optionen aus und ersetzen Sie sie durch Ihre eigenen Werte. *<placeholder text>*

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS-Services that you own>
Service | <a specific AWS-Service that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

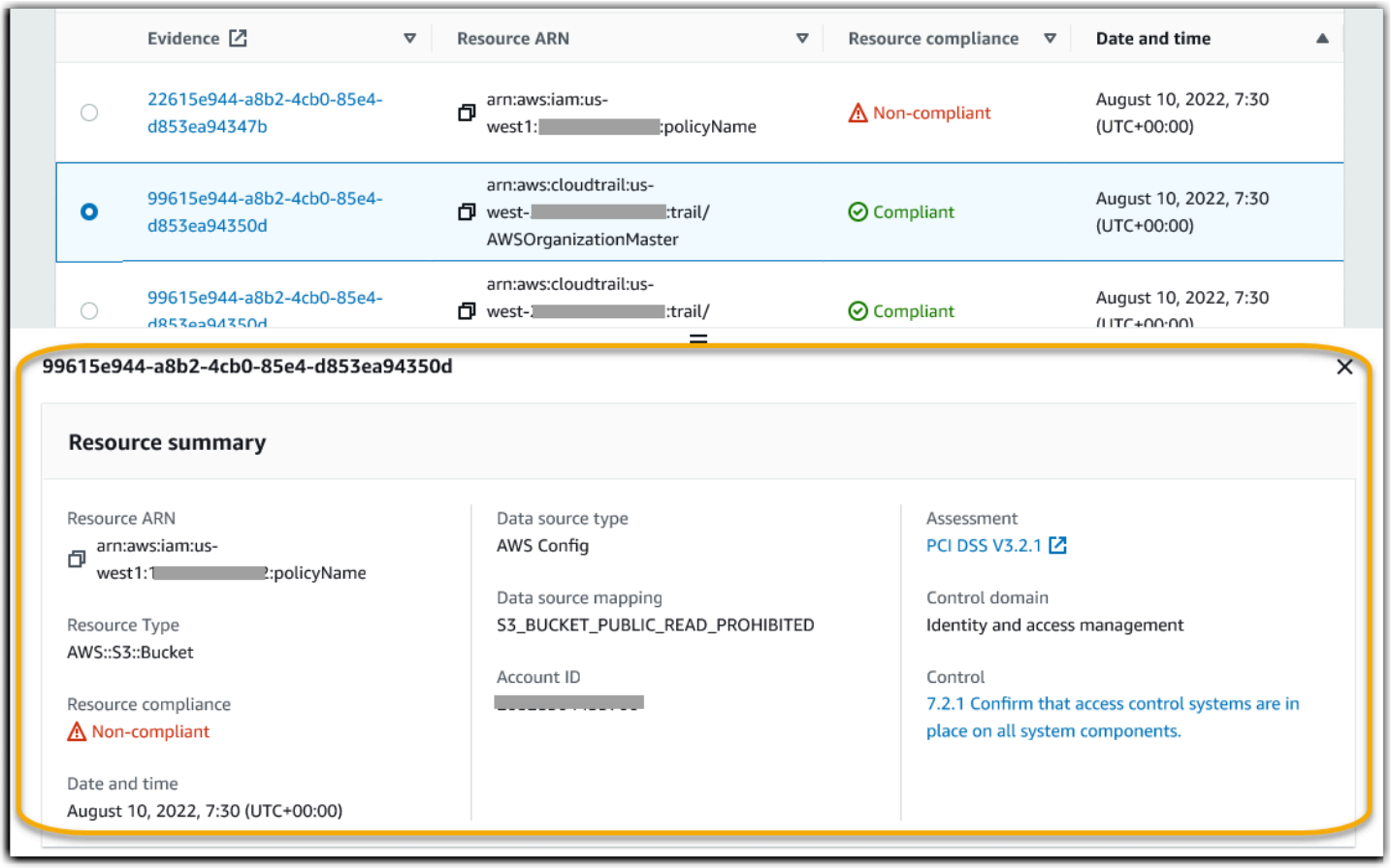
Wenn Sie für mehrere Instanzen derselben Kriterien verantwortlich sind (wenn Sie beispielsweise mehrere besitzen AWS-Services), können Sie Ihre Ergebnisse nach diesem Wert gruppieren. Sie erhalten so die Gesamtzahl der passenden Beweise für jeden AWS-Service. Sie können dann die Ergebnisse für die Dienste abrufen, die Sie besitzen.

Anwendungsfall 3: Führen Sie eine kurze Vorschau der Ressourcen zu den Beweisen durch

Dieser Anwendungsfall ist ideal für alle Audit Manager-Kunden.

Bisher war es sehr zeitaufwändig, einzelne Beweisdetails zu überprüfen. Wenn Sie eine Vorschau der Beweise anzeigen wollten, mussten Sie direkt zu dieser Bewertung gehen und dann durch tief verschachtelte Beweisordner navigieren. Die Beweissuche bietet jetzt eine bequeme Möglichkeit, eine Vorschau dieser Informationen anzuzeigen. Für jedes Beweiselement zu Ihrer Suchanfrage können Sie eine Vorschau der einzelnen Ressourcen anzeigen.

Folgen Sie zunächst den Schritten zur Suche nach Beweisen. Aktivieren Sie anschließend die Optionsschaltfläche neben einem Ergebnis, um eine Ressourcen-Zusammenfassung auf der aktuellen Seite anzuzeigen. Sie können jede einzelne Ressource, die sich auf ein Beweisstück bezieht, in der Vorschau anzeigen. Um die vollständigen Beweisdetails für eine Ressource zu sehen, wählen Sie den Namen des Beweises aus. Weitere Informationen finden Sie unter Vorschau von Ressourcenzusammenfassungen anzeigen.



Audit Manager Download-Center

Im Download-Center können Sie all Ihre herunterladbaren Audit Manager-Dateien finden und verwalten. Wenn Sie einen Bewertungsbericht erstellen oder Suchergebnisse aus Evidence Finder exportieren, werden die Dateien im Download-Center angezeigt.

Inhalt

Das Download-Center durchsuchen

Gehen Sie wie folgt vor, um Ihre Dateien im Download-Center zu durchsuchen.

Um Dateien im Download-Center zu finden

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich die Option Download-Center aus.
3. Wählen Sie die Registerkarte Bewertungsberichte, um die Bewertungsberichte anzuzeigen, die zum Herunterladen zur Verfügung stehen.

    - Auf dieser Registerkarte werden die Bewertungsberichte angezeigt, die Sie erstellt haben. Bewertungsberichte bleiben im Download-Center verfügbar, bis Sie sie löschen.
    - Um den aktuellen Status Ihres Bewertungsberichts zu sehen, klicken Sie auf das Aktualisierungssymbol (#), um die Tabelle neu zu laden. Jede Zeile in der Tabelle mit den Bewertungsberichten enthält den Namen des Berichts, sein Erstellungsdatum und einen der folgenden Status:

Status	Description
In Bearbeitung	Audit Manager generiert den Bewertungsbericht.

Status	Description
Bereit	Der Bewertungsbericht steht Ihnen zum Herunterladen zur Verfügung.
Fehler	Der Bewertungsbericht konnte nicht generiert werden. In diesem Fall zeigt Audit Manager eine Meldung an, die den Fehler beschreibt. Informationen zur Behebung dieser Fehler finden Sie unterBehebung von Bewertungsberichtfehlern.

4. Wählen Sie die Registerkarte Exporte, um die CSV-Exporte anzuzeigen, die zum Herunterladen verfügbar sind.

   - Auf dieser Registerkarte werden die Evidence Finder-Suchergebnisse angezeigt, die Sie in den letzten sieben Tagen exportiert haben. CSV-Dateien werden nach sieben Tagen aus dem Download-Center entfernt, sie sind jedoch weiterhin in Ihrem Exportziel S3-Bucket verfügbar. Anweisungen, wie Sie einen CSV-Export aus der Beweissuche in Ihrem S3-Zielort-Bucket finden, finden Sie unter Anzeige Ihrer Ergebnisse nach dem Export.
   - Um den aktuellen Status Ihrer CSV-Exporte zu sehen, wählen Sie das Aktualisierungssymbol (#), um die Tabelle neu zu laden. Jede Zeile in der Exporttabelle zeigt den Dateinamen, das Exportdatum und einen der folgenden Status:

Status	Description
In Bearbeitung	Audit Manager bereitet die CSV-Datei vor.
Bereit	Der Export war erfolgreich und die Datei steht Ihnen zum Herunterladen zur Verfügung.
Fehler	Der Export ist fehlgeschlagen. In diesem Fall zeigt Audit Manager eine Meldung an, die den Fehler beschreibt. Informationen zur Behebung dieser Fehler finden Sie untercsv-exports.

> **Note**
>
> Beachten Sie, dass auf der Registerkarte „Exporte“ möglicherweise auch CSV-Dateien für Abfragen angezeigt werden, die Sie direkt in AWS CloudTrail Lake ausgeführt haben. Dies schließt Abfragen ein, die in der CloudTrail Konsole oder mithilfe der CloudTrail API gestellt wurden. CloudTrail Exporte werden auf dieser Registerkarte angezeigt, wenn Sie den Audit Manager Manager-Ereignisdatenspeicher abgefragt haben und sich dafür entschieden haben, die Ergebnisse in Amazon S3 zu speichern.

Herunterladen einer Datei

Gehen Sie wie folgt vor, um eine Datei aus dem Download-Center herunterzuladen.

So laden Sie eine Datei herunter

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich die Option Download-Center aus.
3. Wählen Sie entweder die Registerkarte Bewertungsberichte oder die Registerkarte Exporte.
4. Wählen Sie die Datei aus, die Sie herunterladen möchten, und klicken Sie dann auf Herunterladen.

Anweisungen zum direkten Herunterladen einer Datei aus Ihrem S3-Ziel-Bucket finden Sie unter Objekt herunterladen im Amazon Simple Storage Service (Amazon S3) -Benutzerhandbuch.

Löschen einer Datei

Gehen Sie wie folgt vor, um alle Bewertungsberichte, die Sie nicht mehr benötigen, im Download-Center zu löschen.

> **Note**
>
> Löschen von CSV-Exporten aus dem Download-Center wird derzeit nicht unterstützt. CSV-Exporte werden nach sieben Tagen automatisch aus dem Download-Center entfernt.

So löschen Sie einen Bewertungsbericht

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich die Option Download-Center aus.
3. Wählen Sie die Registerkarte Bewertungsberichte aus.
4. Wählen Sie den Bericht, den Sie löschen möchten, und klicken Sie auf Löschen.

Wenn Sie einen Bewertungsbericht oder einen CSV-Export aus Ihrem S3-Zielort-Bucket löschen möchten, empfehlen wir Ihnen, diese Aufgabe direkt in Amazon S3 auszuführen. Anweisungen finden Sie unter Löschen von Amazon S3-Objekten im Amazon Simple Storage Service (Amazon S3)-Benutzerhandbuch.

Weitere Ressourcen

- Konfiguration Ihres Standardexportziels für Evidence Finder
- Konfiguration Ihres Standardziels für Bewertungsberichte
- Behebung von Bewertungsberichtfehlern
- Behebung von Problemen beim CSV-Export
- Ein Objekt von Amazon S3 herunterladen
- Löschen von Amazon S3 S3-Objekten

Verwendung der Framework-Bibliothek zur Verwaltung von Frameworks in AWS Audit Manager

Sie können Frameworks in der Framework-Bibliothek unter finden und verwalten AWS Audit Manager.

Ein Framework bestimmt, welche Kontrollen über einen bestimmten Zeitraum in einer Umgebung getestet werden. Es definiert die Kontrollen und ihre Datenquellenzuordnungen für einen bestimmten Compliance-Standard oder eine bestimmte Vorschrift. Es wird auch zur Strukturierung und Automatisierung von Audit Manager-Bewertungen verwendet. Sie können Frameworks als Ausgangspunkt verwenden, um Ihre AWS-Service Nutzung zu überprüfen und mit der Automatisierung der Beweiserhebung zu beginnen.

Wichtige Punkte

In der Framework-Bibliothek sind Frameworks in die folgenden Kategorien unterteilt.

- Standard-Frameworks sind vorgefertigte Frameworks, die AWS bietet: Diese Frameworks basieren auf AWS bewährten Verfahren für verschiedene Compliance-Standards und -Vorschriften wie GDPR und HIPAA. Zu den Standard-Frameworks gehören Kontrollen, die in Kontrollgruppen organisiert sind, die auf dem Compliance-Standard oder den Vorschriften basieren, die das Framework unterstützt.

  Sie können den Inhalt von Standard-Frameworks anzeigen, aber nicht bearbeiten oder löschen. Sie können jedoch eine bearbeitbare Kopie eines beliebigen Standard-Frameworks erstellen, um ein neues Framework zu erstellen, das Ihren spezifischen Anforderungen entspricht.
- Benutzerdefinierte Frameworks sind Frameworks, die Sie erstellen. Sie können ein benutzerdefiniertes Framework von Grund auf neu erstellen oder indem Sie eine bearbeitbare Kopie eines vorhandenen Frameworks erstellen. Sie können benutzerdefinierte Frameworks verwenden, um Kontrollsätze so zu organisieren, dass sie Ihren spezifischen Anforderungen entsprechen.

Sie können eine Bewertung anhand eines Standard-Frameworks oder eines benutzerdefinierten Frameworks erstellen.

> **Note**
>
> AWS Audit Manager hilft beim Sammeln von Nachweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Standards und -Vorschriften relevant sind. Ihre Einhaltung wird jedoch nicht bewertet. Die auf diese Weise gesammelten Nachweise enthalten AWS Audit Manager daher möglicherweise nicht alle Informationen über Ihre AWS Nutzung, die für Audits erforderlich sind. AWS Audit Manager ist kein Ersatz für Rechtsbeistand oder Compliance-Experten.

Weitere Ressourcen

Um Frameworks in Audit Manager zu erstellen und zu verwalten, folgen Sie den hier beschriebenen Verfahren.

- Die verfügbaren Frameworks finden Sie in AWS Audit Manager
- Überprüfung eines Frameworks in AWS Audit Manager
- Erstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager
  - Ein benutzerdefiniertes Framework von Grund auf neu erstellen in AWS Audit Manager
  - Erstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager
- Bearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager
- Löschen eines benutzerdefinierten Frameworks in AWS Audit Manager
- Teilen eines benutzerdefinierten Frameworks in AWS Audit Manager
  - Framework-Konzepte und -Terminologie freigeben
  - Senden Sie eine Anfrage zum Teilen eines benutzerdefinierten Frameworks in AWS Audit Manager
  - Antworten auf Anfragen zum Teilen in AWS Audit Manager
  - Löschen von Anfragen zum Teilen in AWS Audit Manager
- Unterstützte Frameworks in AWS Audit Manager

Die verfügbaren Frameworks finden Sie in AWS Audit Manager

Sie finden alle verfügbaren Frameworks auf der Framework-Bibliotheksseite in der Audit Manager Manager-Konsole.

Sie können auch alle verfügbaren Frameworks mithilfe der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) anzeigen.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen von Frameworks verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Audit Manager console

So zeigen Sie verfügbare Frameworks in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek aus.
3. Wählen Sie die Registerkarte Standard-Frameworks oder Benutzerdefinierte Frameworks, um die verfügbaren Standard- und benutzerdefinierten Frameworks zu durchsuchen.

AWS CLI

Um die verfügbaren Frameworks einzusehen, finden Sie im AWS CLI

Um Frameworks in Audit Manager anzuzeigen, verwenden Sie den list-assessment-frameworksBefehl und geben Sie a an`--framework-type`. Sie können entweder eine Liste der Standard-Frameworks oder auch eine Liste der benutzerdefinierten Frameworks abrufen.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Um verfügbare Frameworks mithilfe der API anzuzeigen

Verwenden Sie den ListAssessmentFrameworksVorgang und geben Sie einen FrameworkType an. Sie können entweder eine Liste der Standard-Frameworks oder auch eine Liste der benutzerdefinierten Frameworks zurückzusenden.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr in der AWS Audit Manager API-Referenz zu erfahren. Dies beinhaltet Informationen zur Verwendung der `ListAssessmentFrameworks` Operation und der Parameter in einer der sprachspezifischen Sprachen. AWS SDKs

Nächste Schritte

Wenn Sie bereit sind, sich mit den Details eines Frameworks vertraut zu machen, folgen Sie den Schritten unter. Überprüfung eines Frameworks in AWS Audit Manager Diese Seite führt Sie durch die Einzelheiten des Frameworks und erklärt die Informationen, die Sie dort sehen.

Auf der Seite mit der Framework-Bibliothek können Sie auch ein benutzerdefiniertes Framework erstellen, bearbeiten, löschen oder teilen.

Weitere Ressourcen

Lösungen für Framework-Probleme in Audit Manager finden Sie unterBehebung von Framework-Problemen.

Überprüfung eines Frameworks in AWS Audit Manager

Sie können die Details eines Frameworks mithilfe der Audit Manager-Konsole, der Audit Manager-API oder der AWS Command Line Interface (AWS CLI) überprüfen.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen von Frameworks verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Audit Manager console

So zeigen Sie Framework-Details in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek, um eine Liste der verfügbaren Frameworks anzuzeigen.
3. Wählen Sie die Registerkarte Standard-Frameworks oder Benutzerdefinierte Frameworks, um die verfügbaren Frameworks zu durchsuchen.
4. Wählen Sie den Namen des Frameworks, um es zu öffnen.
5. Überprüfen Sie die Framework-Details anhand der folgenden Informationen als Referenz.

Abschnitt Framework-Details

Dieser Abschnitt zeigt die Frameworks im Überblick. In diesem Abschnitt können Sie die folgenden Informationen überprüfen:

Name	Beschreibung
Beschreibung	Eine Beschreibung des Frameworks, falls eine bereitgestellt wurde.
Typ des Frameworks	Gibt an, ob es sich bei dem Framework um ein Standard-Framework oder ein benutzerdefiniertes Framework handelt.
Art der Konformität	Der Compliance-Standard oder die Verordnung, die das Framework unterstützt.

Wenn Sie sich ein benutzerdefiniertes Framework ansehen, können Sie auch die folgenden Details sehen:

Name	Beschreibung
Erstellt von	Das Konto, mit dem das benutzerdefinierte Framework erstellt wurde.
Erstellungsdatum	Das Datum, an dem das benutzerdefinierte Framework erstellt wurde.
Letzte Aktualisierung	Das Datum, an dem dieses Framework zuletzt bearbeitet wurde.

Registerkarte „Kontrollen“

Auf dieser Registerkarte werden die Kontrollen im Framework aufgeführt, eingeteilt in Kontrollsätze. Auf dieser Registerkarte können Sie die folgenden Informationen überprüfen:

Name	Beschreibung
Steuerelemente, gruppiert nach Steuersatz	Wählen Sie das Symbol für die Strukturansicht, um die Steuerelemente anzuzeigen, die zu den einzelnen Steuersätzen gehören.
Typ	Gibt an, ob es sich bei dem Steuerelement um ein Standardsteuerelement oder ein benutzerdefiniertes Steuerelement handelt.
Datenquellen	Gibt die Datenquelle an, aus der Audit Manager Beweise für diese Framework-Steuerung sammelt.

Registerkarte „Tags“

Diese Registerkarte listet die Tags auf, die dem Framework zugeordnet sind. Auf dieser Registerkarte können Sie die folgenden Informationen überprüfen:

Name	Beschreibung
Schlüssel	Der Tag-Schlüssel (z. B. ein Konformitätsstandard, eine Vorschrift oder eine Kategorie).
Wert	Der Tag-Wert.

AWS CLI

Um die Details des Frameworks einzusehen, finden Sie AWS CLI

1. Um das Framework zu identifizieren, das Sie überprüfen möchten, führen Sie den list-assessment-frameworksBefehl aus und geben Sie a an`--framework-type`. Sie können entweder eine Liste der Standard-Frameworks oder auch eine Liste der benutzerdefinierten Frameworks abrufen.

   Im folgenden Beispiel ersetzen Sie das entweder *`placeholder text`* durch `Custom` oder`Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   Als Antwort wird eine Liste von Frameworks zurückgegeben. Suchen Sie nach dem zu überprüfenden Framework und notieren Sie sich die Framework-ID und den Amazon-Ressourcenname (ARN).

2. Um die Framework-Details abzurufen, führen Sie den get-assessment-frameworkBefehl aus und geben Sie den an`--framework-id`.

   Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

> **Tip**
>
> Die Framework-Details werden im JSON-Format zurückgesandt. Informationen zu diesen Daten finden Sie in der AWS CLI Befehlsreferenz unter get-assessment-framework Ausgabe.

3. Um die Tags für ein Framework zu sehen, verwenden Sie den list-tags-for-resourceBefehl und geben Sie die `--resource-arn` für das Framework an.

   Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen:

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Weitere Informationen zur Verwendung von Tags in Audit Manager finden Sie unter Markieren von AWS Audit Manager -Ressourcen.

Audit Manager API

Um Framework-Details mithilfe der API anzuzeigen

1. Um das Framework zu identifizieren, das Sie überprüfen möchten, verwenden Sie den ListAssessmentFrameworksVorgang und geben Sie einen FrameworkType an. Sie können entweder eine Liste der Standard-Frameworks oder auch eine Liste der benutzerdefinierten Frameworks zurückzusenden.

   Suchen Sie in der Antwort nach dem zu überprüfenden Framework und notieren Sie sich die Framework-ID und den Amazon-Ressourcenname (ARN).

2. Verwenden Sie den Vorgang, um die Framework-Details abzurufen. GetAssessmentFramework Geben Sie in der Anfrage die FrameworkID aus Schritt 1 an.

> **Tip**
>
> Die Framework-Details werden im JSON-Format zurückgesandt. Informationen zu diesen Daten finden Sie unter GetAssessmentFramework Response Elements in der AWS Audit Manager API-Referenz.

3. Verwenden Sie die ListTagsForResourceOperation, um Tags für das Framework anzuzeigen. Geben Sie in der Anfrage die resourceArn aus Schritt 1 an.

Weitere Informationen zu Tags in Audit Manager finden Sie unter AWS Audit Manager Ressourcen kennzeichnen.

Weitere Informationen zu diesen API-Vorgängen finden Sie unter einem der Links im vorherigen Verfahren, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Auf der Seite mit den Framework-Details können Sie eine Bewertung anhand des Frameworks erstellen oder eine bearbeitbare Kopie des Frameworks erstellen.

Wenn Sie ein benutzerdefiniertes Framework überprüfen, können Sie das Framework auch bearbeiten, löschen oder teilen.

Weitere Ressourcen

- Auf der Detailseite meines benutzerdefinierten Frameworks werde ich aufgefordert, mein benutzerdefiniertes Framework neu zu erstellen
- Ich kann keine Kopie meines benutzerdefinierten Frameworks erstellen

Erstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager

Sie können benutzerdefinierte Frameworks verwenden, um Kontrollsätze so zu organisieren, dass sie Ihren spezifischen Anforderungen entsprechen.

Wichtige Punkte

Wenn es darum geht, benutzerdefinierte Frameworks in Audit Manager zu erstellen, stehen Ihnen zwei Methoden zur Auswahl:

1. Ein benutzerdefiniertes Framework von Grund auf neu erstellen — Dies gibt Ihnen die Flexibilität, mit einem Neuanfang zu beginnen und jeden Aspekt des Frameworks gemäß Ihren Spezifikationen zu definieren. Dieser Ansatz ist besonders vorteilhaft, wenn Ihre Anforderungen erheblich von bestehenden Standard-Frameworks abweichen oder wenn Sie firmenspezifische Kontrollsätze integrieren müssen.
2. Erstellen einer bearbeitbaren Kopie eines vorhandenen Frameworks — Dieser Ansatz ermöglicht es Ihnen, die Struktur und den Inhalt eines vorhandenen Frameworks zu nutzen und bietet Ihnen gleichzeitig die Freiheit, es an Ihre spezifischen Bedürfnisse anzupassen. Wenn Sie mit einer etablierten Grundlage beginnen, können Sie den Prozess der Erstellung Ihres benutzerdefinierten Frameworks rationalisieren und sich darauf konzentrieren, es an die individuellen Anforderungen Ihres Unternehmens anzupassen.

Unabhängig vom gewählten Ansatz umfasst die Erstellung eines benutzerdefinierten Frameworks eine Reihe von Schritten, z. B. die Angabe von Framework-Details, die Definition von Kontrollsätzen und die Überprüfung des Frameworks, bevor seine Erstellung abgeschlossen wird. Während dieses Prozesses können Sie die spezifischen Kontrollsätze Ihres Unternehmens einbeziehen und so sicherstellen, dass das benutzerdefinierte Framework Ihre GRC-Anforderungen genau widerspiegelt.

Weitere Ressourcen

Anweisungen zum Erstellen eines benutzerdefinierten Frameworks finden Sie in den folgenden Ressourcen.

- Ein benutzerdefiniertes Framework von Grund auf neu erstellen in AWS Audit Manager
- Erstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager

Ein benutzerdefiniertes Framework von Grund auf neu erstellen in AWS Audit Manager

Wenn die Compliance-Anforderungen Ihres Unternehmens nicht mit den vorgefertigten Standard-Frameworks übereinstimmen, die in verfügbar sind AWS Audit Manager, können Sie stattdessen Ihr eigenes benutzerdefiniertes Framework von Grund auf neu erstellen.

Auf dieser Seite werden die Schritte zur Erstellung eines benutzerdefinierten Frameworks beschrieben, das auf Ihre spezifischen Bedürfnisse zugeschnitten ist.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Erstellen eines benutzerdefinierten Frameworks verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Aufgaben

- Schritt 1: Framework-Details angeben
- Schritt 2: Geben Sie Kontrollsätze an
- Schritt 3: Überprüfen und Erstellen des Frameworks

Schritt 1: Framework-Details angeben

Geben Sie zunächst Details zu Ihrem benutzerdefinierten Framework an.

Framework-Details spezifizieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek und dann Benutzerdefiniertes Framework erstellen aus.
3. Geben Sie unter Framework-Details einen Namen, einen Konformitätstyp (optional) und eine Beschreibung für Ihr Framework (ebenfalls optional) ein. Wenn Sie einen Compliance-Typ wie PCI_DSS oder GDPR eingeben, können Sie dieses Schlüsselwort verwenden, um später nach Ihrem Framework zu suchen.
4. Wählen Sie unter Tags die Option Neuen Tag hinzufügen, um Ihrer Framework einen Tag zuzuordnen. Sie können für jedes Tag einen Schlüssel und einen Wert angeben. Der Tag-Schlüssel ist eine Pflichtangabe. Sie können es als Suchkriterien verwenden, wenn Sie in der Framework-Bibliothek nach diesem Framework suchen.
5. Wählen Sie Weiter aus.

Schritt 2: Geben Sie Kontrollsätze an

Als Nächstes geben Sie an, welche Kontrollen Sie zu Ihrem Framework hinzufügen und wie Sie sie organisieren möchten. Fügen Sie zunächst Kontrollsätze zum Framework und dann Kontrollen zu den Kontrollsätzen hinzu.

> **Note**
>
> Wenn Sie die AWS Audit Manager Konsole verwenden, um ein benutzerdefiniertes Framework zu erstellen, können Sie bis zu 10 Kontrollsätze für jedes Framework hinzufügen. Wenn Sie die Audit Manager-API verwenden, um ein benutzerdefiniertes Framework zu erstellen, können Sie mehr als 10 Kontrollsätze erstellen. Verwenden Sie die von Audit Manager bereitgestellte CreateAssessmentFrameworkAPI, um mehr Kontrollsätze hinzuzufügen, als die Konsole derzeit zulässt.

Um einen Kontrollsatz anzugeben

1. Geben Sie unter Name des Kontrollsatzes eine Bezeichnung ein.
2. Verwenden Sie unter Steuerelemente hinzufügen die Dropdownliste Steuerelementtyp, um einen der beiden Steuerungstypen auszuwählen: Standardsteuerelemente oder Benutzerdefinierte Steuerelemente.
3. Basierend auf der Option, die Sie im vorherigen Schritt ausgewählt haben, wird eine Liste mit Standard- oder benutzerdefinierten Kontrollen angezeigt. Wählen Sie ein oder mehrere Steuerelemente aus und wählen Sie Zum Steuersatz hinzufügen aus.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option „Zum Kontrollsatz hinzufügen“.
5. Prüfen Sie die Steuerelemente, die in der Liste Ausgewählte Steuerelemente angezeigt werden.
   - Um weitere Steuerelemente hinzuzufügen, wiederholen Sie die Schritte 2—4.
   - Um unerwünschte Steuerelemente zu entfernen, wählen Sie ein oder mehrere Steuerelemente aus und wählen Sie Steuerung entfernen.
6. Um einen neuen Kontrollsatz hinzuzufügen, wählen Sie Kontrollsatz hinzufügen.
7. Um einen unerwünschten Kontrollsatz zu entfernen, wählen Sie Kontrollsatz entfernen.
8. Nach dem Hinzufügen von Kontrollen und Kontrollsätzen wählen Sie Weiter.

Schritt 3: Überprüfen und Erstellen des Frameworks

Überprüfen Sie die Informationen für Ihr Framework. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten.

Wenn Sie fertig sind, wählen Sie Benutzerdefiniertes Framework erstellen aus.

Nächste Schritte

Nachdem Sie Ihr neues benutzerdefiniertes Framework erstellt haben, können Sie anhand Ihres Frameworks eine Bewertung erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Informationen dazu, wie Sie Ihr benutzerdefiniertes Framework zu einem späteren Zeitpunkt erneut aufrufen können, finden Sie unterDie verfügbaren Frameworks finden Sie in AWS Audit Manager. Gehen Sie wie folgt vor, um Ihr benutzerdefiniertes Framework zu finden, sodass Sie es anzeigen, bearbeiten, teilen oder löschen können.

Weitere Ressourcen

Lösungen für Framework-Probleme in Audit Manager finden Sie unterBehebung von Framework-Problemen.

Erstellen einer editierbaren Kopie eines vorhandenen Frameworks in AWS Audit Manager

Anstatt ein benutzerdefiniertes Framework von Grund auf neu zu erstellen, können Sie ein vorhandenes Framework als Ausgangspunkt verwenden und eine bearbeitbare Kopie erstellen. Wenn Sie dies tun, verbleibt das vorhandene Framework in der Framework-Bibliothek, und ein neues benutzerdefiniertes Framework wird mit Ihren spezifischen Einstellungen erstellt.

Sie können eine bearbeitbare Kopie jedes vorhandenen Frameworks erstellen. Es kann entweder ein Standard- oder ein benutzerdefiniertes Framework sein.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Erstellen eines benutzerdefinierten Frameworks verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Aufgaben

- Schritt 1: Framework-Details angeben
- Schritt 2: Geben Sie die Kontrollsätze an
- Schritt 3: Überprüfen und Erstellen des Frameworks

Schritt 1: Framework-Details angeben

Alle Framework-Details, mit Ausnahme von Tags, werden aus dem ursprünglichen Framework übernommen. Überprüfen und ändern dieser Details nach Bedarf.

Framework-Details spezifizieren

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek aus.
3. Wählen Sie das Framework aus, das Sie als Ausgangspunkt verwenden möchten, wählen Sie Benutzerdefiniertes Framework erstellen und dann Kopie erstellen aus.
4. Geben Sie im daraufhin angezeigten Popup-Fenster einen Namen für das neue benutzerdefinierte Framework ein und wählen Sie Weiter.
5. Überprüfen Sie unter Framework-Details den Namen, den Konformitätstyp und die Beschreibung für Ihr Framework und ändern Sie sie nach Bedarf. Der Konformitätstyp sollte den Konformitätsstandard oder die Vorschrift angeben, die mit Ihrem Framework verknüpft ist. Sie können mit diesem Schlüsselwort nach Ihrem Framework suchen.
6. Wählen Sie unter Tags die Option Neuen Tag hinzufügen, um Ihrer Framework einen Tag zuzuordnen. Sie können für jedes Tag einen Schlüssel und einen Wert angeben. Der Tag-Schlüssel ist obligatorisch und kann als Suchkriterium verwendet werden, wenn Sie in der Framework-Bibliothek nach diesem Framework suchen.
7. Wählen Sie Weiter aus.

Schritt 2: Geben Sie die Kontrollsätze an

Die Kontrollsätze wurden aus dem ursprünglichen Framework übernommen. Ändern Sie die aktuelle Konfiguration, indem Sie nach Bedarf weitere Steuerelemente hinzufügen oder vorhandene Steuerelemente entfernen.

> **Note**
>
> Wenn Sie die Audit Manager Manager-Konsole verwenden, um ein benutzerdefiniertes Framework zu erstellen, können Sie bis zu 10 Kontrollsätze für jedes Framework hinzufügen. Wenn Sie die Audit Manager-API verwenden, um ein benutzerdefiniertes Framework zu erstellen, können Sie mehr als 10 Kontrollsätze hinzufügen. Verwenden Sie die von Audit Manager bereitgestellte CreateAssessmentFrameworkAPI, um mehr Kontrollsätze hinzuzufügen, als die Konsole derzeit zulässt.

Um einen Kontrollsatz anzugeben

1. Ändern Sie unter Name des Kontrollsatzes den Namen des Kontrollsatzes nach Bedarf.
2. Fügen Sie unter Steuerelemente hinzufügen ein neues Steuerelement hinzu, indem Sie in der Dropdownliste einen der beiden Steuerelementtypen auswählen: Standardsteuerelemente oder Benutzerdefinierte Steuerelemente.
3. Basierend auf der Option, die Sie im vorherigen Schritt ausgewählt haben, wird eine Liste mit Standard- oder benutzerdefinierten Kontrollen angezeigt. Wählen Sie ein oder mehrere Steuerelemente aus und klicken Sie dann auf Zum Kontrollsatz hinzufügen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option „Zum Kontrollsatz hinzufügen“.
5. Prüfen Sie die Steuerelemente, die in der Liste Ausgewählte Steuerelemente angezeigt werden.
   - Um weitere Steuerelemente hinzuzufügen, wiederholen Sie die Schritte 2—4.
   - Um unerwünschte Steuerelemente zu entfernen, wählen Sie ein oder mehrere Steuerelemente aus und wählen Sie Steuerung entfernen.
6. Um dem Framework einen neuen Kontrollsatz hinzuzufügen, wählen Sie Kontrollsatz hinzufügen.
7. Um einen unerwünschten Kontrollsatz zu entfernen, wählen Sie Kontrollsatz entfernen.
8. Nach dem Hinzufügen von Kontrollen und Kontrollsätzen wählen Sie Weiter.

Schritt 3: Überprüfen und Erstellen des Frameworks

Überprüfen Sie die Informationen für Ihr Framework. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten.

Wenn Sie fertig sind, wählen Sie Benutzerdefiniertes Framework erstellen aus.

Nächste Schritte

Nachdem Sie Ihr neues benutzerdefiniertes Framework erstellt haben, können Sie anhand Ihres Frameworks eine Bewertung erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Informationen dazu, wie Sie Ihr benutzerdefiniertes Framework zu einem späteren Zeitpunkt erneut aufrufen können, finden Sie unterDie verfügbaren Frameworks finden Sie in AWS Audit Manager. Gehen Sie wie folgt vor, um Ihr benutzerdefiniertes Framework zu finden, sodass Sie es anzeigen, bearbeiten, teilen oder löschen können.

Weitere Ressourcen

Lösungen für Framework-Probleme in Audit Manager finden Sie unterBehebung von Framework-Problemen.

Bearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager

Möglicherweise müssen Sie Ihre benutzerdefinierten Frameworks ändern, wenn AWS Audit Manager sich Ihre Compliance-Anforderungen ändern.

Auf dieser Seite werden die Schritte zur Bearbeitung der Details und Kontrollsätze eines benutzerdefinierten Frameworks beschrieben.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor ein benutzerdefiniertes Framework erstellt haben.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Bearbeiten eines benutzerdefinierten Frameworks verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Aufgaben

- Schritt 1: Framework-Details bearbeiten

- Schritt 2: Bearbeiten Sie die Kontrollsätze
- Schritt 3. Überprüfen und speichern

Schritt 1: Framework-Details bearbeiten

Überprüfen und bearbeiten Sie zunächst die vorhandenen Framework-Details.

So bearbeiten Sie Framework-Details

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek und dann Benutzerdefiniertes Framework aus.
3. Wählen Sie das zu bearbeitende Framework aus, klicken Sie auf Aktionen und dann auf Bearbeiten.
   - Sie können auch ein benutzerdefiniertes Framework öffnen und oben rechts auf der Seite mit den Framework-Details die Option Bearbeiten auswählen.
4. Überprüfen Sie unter Framework-Details den Namen, den Konformitätstyp und die Beschreibung für Ihr Framework und nehmen Sie alle erforderlichen Änderungen vor.
5. Wählen Sie Weiter aus.

> **Tip**
>
> Um die Tags für ein Framework zu bearbeiten, öffnen Sie das Framework und wählen Sie die Registerkarte Framework-Tags. Dort können Sie die mit dem Framework verknüpften Tags anzeigen und bearbeiten.

Schritt 2: Bearbeiten Sie die Kontrollsätze

Überprüfen und bearbeiten Sie als Nächstes die Kontrollen und Kontrollsätze im Framework.

> **Note**
>
> Wenn Sie die AWS Audit Manager Konsole verwenden, um ein benutzerdefiniertes Framework zu bearbeiten, können Sie bis zu 10 Kontrollsätze für jedes Framework hinzufügen.

Wenn Sie die Audit-Manager-API verwenden, um ein benutzerdefiniertes Framework zu bearbeiten, können Sie mehr als 10 Kontrollsätze hinzufügen. Verwenden Sie die von Audit Manager bereitgestellte UpdateAssessmentFrameworkAPI, um mehr Kontrollsätze hinzuzufügen, als die Konsole derzeit zulässt.

Um einen Kontrollsatz zu bearbeiten

1. Überprüfen und bearbeiten Sie unter Name des Kontrollsatzes nach Bedarf die Bezeichnung.
2. Verwenden Sie unter Steuerelemente hinzufügen die Dropdownliste Steuerelementtyp, um einen der beiden Steuerungstypen auszuwählen: Standardsteuerelemente oder Benutzerdefinierte Steuerelemente.
3. Basierend auf der Option, die Sie im vorherigen Schritt ausgewählt haben, wird eine Tabelle mit Standard- oder benutzerdefinierten Kontrollen angezeigt. Wählen Sie ein oder mehrere Steuerelemente aus und wählen Sie Zum Steuersatz hinzufügen aus.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster „Hinzufügen“.
5. Überprüfen und bearbeiten Sie die Steuerelemente, die in der Liste Ausgewählte Steuerelemente angezeigt werden.
   - Um weitere Steuerelemente hinzuzufügen, wiederholen Sie die Schritte 2—4.
   - Um unerwünschte Steuerelemente zu entfernen, wählen Sie ein oder mehrere Steuerelemente aus und wählen Sie „Aus Steuersatz entfernen“.
6. Um dem Framework einen neuen Kontrollsatz hinzuzufügen, wählen Sie Kontrollsatz hinzufügen.
7. Um einen unerwünschten Kontrollsatz zu entfernen, wählen Sie Kontrollsatz entfernen.
8. Nach dem Hinzufügen von Kontrollen und Kontrollsätzen wählen Sie Weiter.

Schritt 3. Überprüfen und speichern

Überprüfen Sie die Informationen für Ihr Framework. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten.

Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.

Nächste Schritte

Wenn Sie sicher sind, dass Sie kein benutzerdefiniertes Framework mehr benötigen, können Sie Ihre Audit Manager Manager-Umgebung bereinigen, indem Sie das Framework löschen. Detaillierte

Anweisungen finden Sie unter Löschen eines benutzerdefinierten Frameworks in AWS Audit Manager.

Weitere Ressourcen

Lösungen für Framework-Probleme in Audit Manager finden Sie unterBehebung von Framework-Problemen.

Teilen eines benutzerdefinierten Frameworks in AWS Audit Manager

Sie können die Framework-Sharing-Funktion von verwenden AWS Audit Manager , um die von Ihnen erstellten benutzerdefinierten Frameworks schnell zu replizieren. Sie können Ihre benutzerdefinierten Frameworks mit anderen AWS-Konto teilen oder Ihre Frameworks AWS-Region unter Ihrem eigenen Konto in ein anderes replizieren. Der Empfänger kann dann auf Ihr benutzerdefiniertes Framework zugreifen und es zur Erstellung von Bewertungen verwenden. Dies ist möglich, ohne Ihre Konfiguration für dieses Framework wiederholen zu müssen.

Wichtige Punkte

Um ein benutzerdefiniertes Framework gemeinsam zu nutzen, erstellen Sie eine Freigabeanfrage. Der Empfänger der Freigabeanfrage hat dann 120 Tage Zeit, um die Anfrage anzunehmen oder abzulehnen. Wird die Freigabeanfrage angenommen, repliziert Audit Manager das geteilte, benutzerdefinierte Framework in ihre Framework-Bibliothek. Audit Manager repliziert nicht nur das benutzerdefinierte Framework, sondern auch alle benutzerdefinierten Kontrollsätze und benutzerdefinierten Kontrollen, die Teil dieses Frameworks sind. Diese benutzerdefinierten Kontrollen werden dann der Kontrollbibliothek des Empfängers hinzugefügt. Audit Manager repliziert keine Standard-Frameworks oder -Kontrollen. Standardmäßig sind diese in allen AWS-Konten und Regionen verfügbar, in denen Audit Manager aktiviert ist.

Die Framework-Freigabefunktion ist nur in der kostenpflichtigen Version verfügbar. Es fallen jedoch keine zusätzlichen Gebühren für die gemeinsame Nutzung eines benutzerdefinierten Frameworks oder die Annahme einer Freigabeanfrage an. Weitere Informationen zu den Preisen für AWS Audit Manager finden Sie auf der Seite mit den AWS Audit Manager Preisen.

> **Important**
>
> Sie dürfen ein benutzerdefiniertes Framework, das von einem Standard-Framework abgeleitet ist, nicht teilen, wenn das Standard-Framework als nicht für die gemeinsame Nutzung in Frage kommt AWS, es sei denn, Sie haben vom Eigentümer des Standard-Frameworks die Genehmigung dazu eingeholt. Weitere Informationen darüber, welche Standard-Frameworks nicht für die gemeinsame Nutzung infrage kommen, und weitere Informationen finden Sie unter Voraussetzungen für die gemeinsame Nutzung von Frameworks.

Weitere Ressourcen

Weitere Informationen zur gemeinsamen Nutzung benutzerdefinierter Frameworks in Audit Manager finden Sie in den folgenden Ressourcen.

- Framework-Konzepte und -Terminologie freigeben
- Senden Sie eine Anfrage zum Teilen eines benutzerdefinierten Frameworks in AWS Audit Manager
- Antworten auf Anfragen zum Teilen in AWS Audit Manager
- Löschen von Anfragen zum Teilen in AWS Audit Manager

Framework-Konzepte und -Terminologie freigeben

Wenn Sie sich mit den folgenden Schlüsselkonzepten vertraut machen, können Sie mehr aus dem Feature zur gemeinsamen Nutzung von AWS Audit Manager benutzerdefinierten Frameworks herausholen.

Wichtige Punkte

Absender

Dies ist der Ersteller einer Freigabeanfrage und der AWS-Konto Ort, an dem das benutzerdefinierte Framework existiert. Absender können benutzerdefinierte Frameworks mit jedem AWS-Konto teilen. Oder sie replizieren ein benutzerdefiniertes Framework auf jedes unterstützte Framework, das AWS-Region unter ihrem eigenen Konto unterstützt wird.

Empfänger

Dies ist der Nutzer des gemeinsamen Frameworks. Empfänger können eine Freigabeanfrage eines Absenders entweder annehmen oder ablehnen.

> **Note**
>
> Ein Empfänger kann ein delegiertes Administratorkontos sein. Sie können benutzerdefinierte Frameworks jedoch nicht mit einem AWS Organizations Verwaltungskonto teilen.

Voraussetzungen für Frameworks

Sie können nur benutzerdefinierte Frameworks freigeben. Standardmäßig sind Standard-Frameworks bereits in allen vorhanden AWS-Konten und AWS-Regionen wo AWS Audit Manager ist sie aktiviert. Darüber hinaus dürfen die freigegebenen, benutzerdefinierten Frameworks keine sensiblen Daten enthalten. Dazu gehören Daten, die sich im Framework selbst, seinen Kontrollsätzen und allen benutzerdefinierten Kontrollen befinden, die Teil des benutzerdefinierten Frameworks sind.

> **Important**
>
> Einige der von angebotenen Standard-Frameworks AWS Audit Manager enthalten urheberrechtlich geschütztes Material, das Lizenzvereinbarungen unterliegt. Benutzerdefinierte Frameworks können Inhalte enthalten, die von diesen Frameworks abgeleitet sind. Sie dürfen ein benutzerdefiniertes Framework, das von einem Standard-Framework abgeleitet ist, nicht weitergeben, wenn das Standard-Framework als nicht für die gemeinsame Nutzung in Frage kommt AWS, es sei denn, Sie haben vom Eigentümer des Standard-Frameworks die Genehmigung dazu eingeholt.
> Der folgenden Tabelle entnehmen Sie, welche Standard-Frameworks für die gemeinsame Nutzung infrage kommen.

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
Essential Eight des australischen Cybersicherheitszentrums (ACSC)	 Ja
Handbuch zur Informationssicherheit (ISM) des Australian Cyber Security Center (ACSC) 02. März 2023	 Ja
Amazon Web Services (AWS) Audit Manager Manager-Beispielframework	 Ja
AWS Control Tower -Leitlinien	 Ja
AWS generatives Framework für bewährte KI-Methoden v2	 Ja
AWS License Manager	 Ja
AWS Bewährte grundlegende Sicherheitsverfahren	 Ja
AWS Bewährte Verfahren für den Betrieb	 Ja

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	 Ja
Kanadisches Zentrum für Cybersicherheit (CCCS) Medium Cloud Control	 Nein
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Stufe 1	 Nein
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Stufe 1 und 2	 Nein
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Stufe 1	 Nein
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Stufe 1 und 2	 Nein
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Stufe 1	 Nein
Zentrum für Internetsicherheit (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Stufe 1 und 2	 Nein

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
Zentrum für Internetsicherheit (CIS) v7.1, IG1	 Ja
CIS Critical Security Controls Version 8.0 (CIS v8.0), IG1	 Nein
Sicherheitsbasiskontrollen des Federal Risk and Authorization Management Program (FedRAMP) r4, moderat	 Ja
Allgemeine Datenschutzverordnung (DSGVO) 2016	 Ja
Gramm-Leach-Bliley Gesetz (GLBA)	 Ja
Titel 21 Bundesgesetzbuch (CFR) Teil 11, Elektronische Aufzeichnungen; elektronische Signaturen — Geltungsbereich und Anwendung 24. Mai 2023	 Ja
EudraLex - Die Vorschriften für Arzneimittel in der Europäischen Union (EU) - Band 4: Gute Herstellungspraxis (GMP) Arzneimittel für Human- und Tierarzneimittel - Anhang 11	 Ja
Sicherheitsregel des Health Insurance Portability and Accountability Act (HIPAA): Februar 2003	 Ja

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
Endgültige Omnibus-Regel des Gesetzes über die Portabilität und Rechenschaftspflicht von Krankenversicherungen (HIPAA)	Ja
Internationale Organisation für Normung (ISO) / Internationale Elektrotechnische Kommission (IEC) 27001:2013 Anhang A	Nein
NIST 800-53 Rev 5: Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organizations	Ja
NIST Cybersecurity Framework (CSF) v1.1	Ja
NIST 800-171 Revision 2: Schutz kontrollierter, nicht klassifizierter Informationen in nichtföderalen Systemen und Organizations	Ja
Datensicherheitsstandard der Zahlungskartenindustrie (PCI DSS) v3.2.1	Nein
Datensicherheitsstandard für die Zahlungskartenindustrie (PCI DSS) v4.0	Nein
Erklärung zu Standards for Attestations Engagement (SSAE) Nr. 18, Service Organizations Controls (SOC) Report 2	Nein

Anfrage freigeben

Um ein benutzerdefiniertes Framework gemeinsam zu nutzen, erstellen Sie eine Freigabeanfrage. In der Freigabeanfrage wird ein Empfänger angegeben und dieser darüber informiert, dass ein benutzerdefiniertes Framework verfügbar ist. Die Empfänger haben 120 Tage Zeit, um auf eine Freigabeanfrage zu antworten, indem sie sie annehmen oder ablehnen. Wenn innerhalb von 120 Tagen keine Maßnahmen ergriffen werden, läuft die Freigabeanfrage ab und der Empfänger kann das benutzerdefinierte Framework nicht mehr zu seiner Framework-Bibliothek hinzufügen. Absender und Empfänger können auf der Freigabeseite in der Framework-Bibliothek Freigabeanfragen einsehen und entsprechende Maßnahmen ergreifen.

Status der Freigabeanfrage

Freigabeanfragen können einen der folgenden Status haben.

Status	Description
Aktiv	Dies weist auf eine Freigabeanfrage hin, die erfolgreich an den Empfänger gesendet wurde und auf dessen Antwort wartet.
Läuft ab	Dies weist auf eine Share-Anfrage hin, die innerhalb der nächsten 30 Tage abläuft.
Geteilt	Dies weist auf eine Teilungsanfrage hin, die der Empfänger akzeptiert hat.
Inaktiv	Dies weist auf eine Freigabeanfrage hin, die widerrufe n, abgelehnt oder abgelaufen ist, bevor der Empfänger Maßnahmen ergriffen hat.
Replizieren	Dies weist auf eine akzeptierte Freigabeanfrage hin, die in die Framework-Bibliothek des Empfängers repliziert wird.
Fehlgeschlagen	Dies weist auf eine Freigabeanfrage hin, die nicht erfolgreich an den Empfänger gesendet wurde.

Benachrichtigungen über Anfragen freigeben

Audit Manager benachrichtigt die Empfänger, wenn sie eine Freigabeanfrage erhalten. Sowohl Empfänger als auch Absender erhalten eine Benachrichtigung, wenn eine Freigabeanfrage in den nächsten 30 Tagen abläuft.

- Für Empfänger wird neben eingegangenen Anfragen mit dem Status Aktiv oder Läuft ab ein blauer Statuspunkt angezeigt. Der Empfänger kann auf die Benachrichtigung antworten, indem er/sie die Freigabeanfrage annimmt oder ablehnt.
- Für Empfänger wird neben eingegangenen Anfragen mit dem Status Läuft ab ein blauer Statuspunkt angezeigt. Die Benachrichtigung gilt als beantwortet, wenn der Empfänger die Anfrage annimmt oder ablehnt. Andernfalls ist sie beantwortet, wenn die Anfrage abläuft. Darüber hinaus kann der Absender die Benachrichtigung beantworten, indem er/sie die Freigabeanfrage widerruft.

Eigentumsrecht beim Absender

Die Absender behalten vollen Zugriff auf die von ihnen freigegebenen benutzerdefinierten Frameworks. Sie können aktive Freigabeanfragen jederzeit stornieren, indem sie die Freigabeanfrage vor ihrem Ablauf zurückziehen. Nachdem ein Empfänger eine Freigabeanfrage akzeptiert hat, kann der Absender dem Empfänger jedoch den Zugriff auf dieses benutzerdefinierte Framework nicht mehr entziehen. Dies liegt daran, dass Audit Manager, wenn der Empfänger die Anfrage akzeptiert, unabhängig davon eine Kopie des benutzerdefinierten Frameworks in der Framework-Bibliothek des Empfängers erstellt.

Audit Manager repliziert nicht nur das benutzerdefinierte Framework des Absenders, sondern auch alle benutzerdefinierten Kontrollen und benutzerdefinierten Kontrollen, die Teil dieses Frameworks sind. Audit Manager repliziert jedoch keine Tags, die an das benutzerdefinierte Framework angehängt sind.

Eigentumsrecht beim Empfänger

Die Empfänger haben vollen Zugriff auf die von ihnen akzeptierten benutzerdefinierten Frameworks. Wenn der Empfänger die Anfrage akzeptiert, repliziert Audit Manager das benutzerdefinierte Framework auf die Registerkarte „Benutzerdefinierte Frameworks“ seiner Framework-Bibliothek. Die Empfänger können das freigegebene benutzerdefinierte Framework dann genauso verwalten wie jedes andere benutzerdefinierte Framework. Empfänger können die benutzerdefinierten Frameworks, die sie von anderen Absendern erhalten, gemeinsam nutzen. Empfänger können Absender nicht daran hindern, Freigabeanfrage zu senden.

Ablauf des freigegebenen Frameworks

Wenn ein Absender eine Freigabeanfrage erstellt, legt Audit Manager fest, dass die Anfrage nach 120 Tagen abläuft. Empfänger können das gemeinsame Framework annehmen und darauf zugreifen, bevor die Anfrage abläuft. Wenn ein Empfänger während dieser Zeit nicht zustimmt, läuft die Freigabeanfrage ab. Nach diesem Zeitpunkt verbleibt eine Aufzeichnung der abgelaufenen Freigabeanfrage im Verlauf. Snapshots der abgelaufenen freigegebenen Frameworks werden zu Prüfungszwecken in einem S3-Bucket mit einer einjährigen TTL archiviert.

Absender können sich dafür entscheiden, eine Freigabeanfrage jederzeit zu widerrufen, bevor sie abläuft.

Speicherung und Sicherung von freigegebenen Framework-Daten

Wenn Sie eine Freigabeanfrage erstellen, speichert Audit Manager eine Momentaufnahme Ihres benutzerdefinierten Frameworks im Osten der USA (Nord-Virginia) AWS-Region. Audit Manager speichert auch eine Sicherungskopie desselben Snapshots in den USA West (Oregon) AWS-Region.

Audit Manager löscht den Snapshot und den Backup-Snapshot, wenn eines der folgenden Ereignisse eintritt:

- Der Absender widerruft die Freigabeanfrage.
- Der Empfänger lehnt die Freigabeanfrage ab.
- Beim Empfänger tritt ein Fehler auf und er konnte die Freigabeanfrage nicht erfolgreich akzeptieren.
- Die Freigabeanfrage läuft ab, bevor der Empfänger auf die Anfrage reagiert.

Wenn ein Absender eine Freigabeanfrage erneut sendet, wird der Snapshot durch eine aktualisierte Version ersetzt, die der neuesten Version des benutzerdefinierten Frameworks entspricht.

Wenn ein Empfänger eine Freigabeanfrage annimmt, wird der Snapshot in den Ordner repliziert AWS-Konto AWS-Region , der in der Freigabeanforderung angegeben wurde.

Versionsverwaltung des freigegebenen Frameworks

Wenn Sie ein benutzerdefiniertes Framework gemeinsam nutzen, erstellt Audit Manager eine unabhängige Kopie dieses Frameworks in der angegebenen AWS-Konto Region. Dies bedeutet, dass Sie die folgenden Punkte beachten sollten:

- Das freigegebene Framework, das ein Empfänger akzeptiert, ist eine Momentaufnahme des Frameworks zum Zeitpunkt der Erstellung der Freigabeanfrage. Wenn Sie das ursprüngliche benutzerdefinierte Framework nach dem Senden einer Freigabeanfrage aktualisieren, wird die Anfrage nicht automatisch aktualisiert. Um die neueste Version des aktualisierten Frameworks zu teilen, können Sie die Freigabeanfrage erneut senden. Das Ablaufdatum dieses neuen Snapshots liegt 120 Tage nach dem Datum der erneuten Freigabe.
- Wenn Sie ein benutzerdefiniertes Framework mit einem anderen teilen AWS-Konto und es dann aus Ihrer Framework-Bibliothek löschen, verbleibt das gemeinsam genutzte benutzerdefinierte Framework in der Framework-Bibliothek des Empfängers.
- Wenn Sie ein benutzerdefiniertes Framework mit einem anderen AWS-Region unter Ihrem Konto teilen und dann dieses benutzerdefinierte Framework in der ersten Region löschen AWS-Region, verbleibt das benutzerdefinierte Framework in der zweiten Region.
- Löschen Sie ein freigegebenes benutzerdefiniertes Framework, nachdem Sie es akzeptiert haben, verbleiben alle benutzerdefinierten Kontrollen, die als Teil des benutzerdefinierten Frameworks repliziert wurden, in Ihrer Kontrollbibliothek.

Weitere Ressourcen

- Senden Sie eine Anfrage zum Teilen eines benutzerdefinierten Frameworks in AWS Audit Manager
- Antworten auf Anfragen zum Teilen in AWS Audit Manager
- Löschen von Anfragen zum Teilen in AWS Audit Manager
- Behebung von Framework-Problemen

Senden Sie eine Anfrage zum Teilen eines benutzerdefinierten Frameworks in AWS Audit Manager

In diesem Tutorial wird beschrieben, wie Sie Ihre benutzerdefinierten Frameworks für AWS-Konten und gemeinsam nutzen können AWS-Regionen.

Wenn Sie ein benutzerdefiniertes Framework freigeben, erstellt Audit Manager einen Snapshot Ihres Frameworks und sendet eine Freigabeanfrage an den Empfänger. Der Empfänger hat 120 Tage Zeit, um das gemeinsame Framework zu akzeptieren. Wird die Freigabeanfrage angenommen, repliziert Audit Manager das freigegebene, benutzerdefinierte Framework in der festgelegten AWS-Region ihrer Framework-Bibliothek. Wenn Sie ein benutzerdefiniertes Framework unter Ihrem eigenen Konto

in eine andere Region replizieren möchten, verwenden Sie das folgende Tutorial und geben Sie Ihre eigene AWS-Konto ID als Empfängerkonto-ID ein.

Voraussetzungen

Stellen Sie vor Beginn dieses Tutorial sicher, dass folgenden Bedingungen erfüllt sind:

- Sie sind mit den Konzepten und der Terminologie des Audit Manager-Frameworks vertraut.
- Das freizugebende benutzerdefinierte Framework ist für die gemeinsame Nutzung geeignet und befindet sich in der Framework-Bibliothek Ihrer AWS Audit Manager -Umgebung.
- Der Empfänger hat es bereits AWS Audit Manager in dem Bereich aktiviert, in AWS-Region dem Sie das benutzerdefinierte Framework teilen möchten.
- Der Empfänger ist kein AWS Organizations Verwaltungskonto.
- Ihre IAM-Identität verfügt über die entsprechenden Berechtigungen, um ein benutzerdefiniertes Framework gemeinsam zu nutzen. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

> **Tip**
>
> Bevor Sie beginnen, notieren Sie sich die AWS-Konto ID, mit der Sie Ihr benutzerdefiniertes Framework teilen möchten. Dies kann Ihre eigene Konto-ID sein, wenn Sie das Framework auf ein anderes AWS-Region unter Ihrem Konto replizieren möchten. Diese Informationen sind für den zweiten Schritt des Tutorials erforderlich.

Verfahren

Aufgaben

- Schritt 1: Identifizieren Sie das benutzerdefinierte Framework, das Sie freigeben möchten
- Schritt 2: Senden einer Freigabeanfrage
- Schritt 3: Anzeige Ihrer gesendeten Anfragen
- Schritt 4 (optional): Widerrufen der Freigabeanfrage

Schritt 1: Identifizieren Sie das benutzerdefinierte Framework, das Sie freigeben möchten

Identifizieren Sie zunächst das benutzerdefinierte Framework, das Sie freigeben möchten. Sie finden alle verfügbaren benutzerdefinierten Frameworks auf der Seite Framework-Bibliothek im Audit Manager.

> **Important**
>
> Geben Sie keine benutzerdefinierten Frameworks frei, die vertrauliche Daten enthalten. Dazu gehören Daten, die sich im Framework selbst, seinen Kontrollsets und allen benutzerdefinierten Kontrollen befinden, die das benutzerdefinierte Framework beeinträchtigen. Weitere Informationen finden Sie unter Framework-Berechtigung.

Ihre verfügbaren benutzerdefinierten Frameworks aufrufen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Framework-Bibliothek aus.
3. Wählen Sie die Registerkarte Benutzerdefinierte Frameworks. Eine Liste Ihrer verfügbaren benutzerdefinierten Frameworks wird angezeigt. Sie können einen beliebigen Framework-Namen wählen, um die Details dieses benutzerdefinierten Frameworks anzuzeigen.

Schritt 2: Senden einer Freigabeanfrage

Geben Sie als Nächstes einen Empfänger an und senden Sie ihm eine Freigabeanfrage für das benutzerdefinierte Framework. Der Empfänger hat 120 Tage Zeit, um auf die Freigabeanfrage zu antworten, bevor sie abläuft.

Eine Freigabeanfrage senden

1. Wählen Sie unter der Registerkarte Benutzerdefinierte Frameworks der Framework-Bibliothek den Namen eines Frameworks aus, um die Seite mit den Details zu öffnen. Wählen Sie von hier aus Aktionen und dann Benutzerdefiniertes Framework freigeben.
   - Wählen Sie alternativ ein benutzerdefiniertes Framework aus der Liste in der Framework-Bibliothek, anschließend Aktionen und Benutzerdefiniertes Framework freigeben. Abhängig von der Größe des benutzerdefinierten Frameworks kann diese Methode einige Sekunden dauern, bis Audit Manager die Freigabeanfrage vorbereitet.

2. Lesen Sie den im Dialogfeld angezeigten Hinweis.

   - Wenn Sie sich nicht sicher sind, ob Sie Ihr benutzerdefiniertes Framework freigeben dürfen, finden Sie weitere Informationen unter Voraussetzungen für Frameworks.
   - Wenn Ihr Framework über Steuerelemente verfügt, die benutzerdefinierte AWS Config Regeln als Datenquelle verwenden, empfehlen wir Ihnen, den Empfänger zu kontaktieren, um ihn darüber zu informieren. Der Empfänger kann dann dieselben AWS Config Regeln in seiner Instanz von erstellen und aktivieren AWS Config. Weitere Informationen finden Sie unter Mein gemeinsames Framework verfügt über Steuerelemente, die benutzerdefinierte AWS Config Regeln als Datenquelle verwenden. Kann der Empfänger Beweise für diese Kontrollen sammeln?.

3. Geben Sie **`agree`** ein und wählen Sie dann Zustimmen, um fortzufahren.
4. Befolgen Sie in der nächsten Ansicht diese Schritte:

   - Geben Sie unter AWS-Konto die Konto-ID des Empfängers ein. Dies kann Ihre eigene Konto-ID sein.
   - Wählen Sie unter AWS-Region die Region des Empfängers aus der Dropdown-Liste aus.
   - (Optional) geben Sie unter Nachricht an den Empfänger einen Kommentar zu dem benutzerdefinierten Framework ein, das Sie freigeben.
   - Überprüfen Sie unter Details zum benutzerdefinierten Framework die Details, um die Freigabe dieses Frameworks zu bestätigen.

5. Wählen Sie Freigeben.

> **Note**
>
> Beachten Sie folgende Punkte:
>
> - Wenn Sie ein benutzerdefiniertes Framework mit einem anderen teilen AWS-Konto, wird das Framework nur auf das angegebene AWS-Region Framework repliziert. Nachdem der Empfänger die Freigabeanfrage akzeptiert hat, kann er das Framework nach Bedarf regionsübergreifend replizieren.
> - Wenn Sie benutzerdefinierte Frameworks gemeinsam nutzen AWS-Regionen, kann es bis zu 10 Minuten dauern, bis Aktionen zur gemeinsamen Nutzung bearbeitet sind. Wir empfehlen Ihnen, nach dem Senden einer regionsübergreifenden Freigabeanfrage später zu überprüfen, ob der Versand erfolgreich war.

- Wenn Sie eine Freigabeanfrage senden, erstellt Audit Manager eine Momentaufnahme des benutzerdefinierten Frameworks zum Zeitpunkt der Erstellung. Wenn Sie das benutzerdefinierte Framework nach dem Senden einer Freigabeanfrage aktualisieren, wird die Anfrage nicht automatisch aktualisiert. Um die neueste Version eines aktualisierten Frameworks zu teilen, können Sie die Freigabeanfrage erneut senden. Das Ablaufdatum dieses neuen Snapshots liegt 120 Tage nach dem Datum der erneuten Freigabe.

Schritt 3: Anzeige Ihrer gesendeten Anfragen

Sie können die Registerkarte Gesendete Anfragen auswählen, um eine Liste aller von Ihnen gesendeten Freigabeanfragen zu sehen. Sie können diese Liste nach Bedarf filtern. Sie können beispielsweise Filter anwenden, um nur Anfragen anzuzeigen, die innerhalb der nächsten 30 Tage ablaufen.

Ihre gesendeten Anfragen ansehen und filtern

1. Wählen Sie im Navigationsbereich Freigabeanfragen aus.
2. Wählen Sie die Registerkarte Gesendete Anfragen.
3. (Optional) wenden Sie Filter an, um genau festzulegen, welche gesendeten Anfragen sichtbar sind. Suchen Sie hierzu in der Dropdownliste Alle Status und ändern den Filter auf einen der folgenden Werte.

Status	Description
Aktiv	Dieser Filter zeigt Anfragen zum Teilen an, die noch auf eine Antwort vom Empfänger warten.
Läuft ab	Dieser Filter zeigt Share-Anfragen an, die in den nächsten 30 Tagen ablaufen.
Geteilt	Dieser Filter zeigt Anfragen zum Teilen an, die vom Empfänger akzeptiert wurden. Das freigegebene, benutzerdefinierte Framework ist jetzt in der Framework-Bibliothek des Empfänger s vorhanden.
Inaktiv	Dieser Filter zeigt Freigabeanfragen an, die abgelehnt, widerrufe n oder abgelaufen sind, bevor der Empfänger Maßnahmen

Status	Description
	ergriffen hat. Wählen Sie die Option Inaktiv aus, um weitere Details anzuzeigen.
Replizieren	Dies weist auf eine akzeptierte Freigabeanfrage hin, die in die Framework-Bibliothek des Empfängers repliziert wird.
Fehlgeschlagen	Dieser Filter zeigt die Freigabeanfragen an, die nicht erfolgrei ch an den Empfänger gesendet wurden. Wählen Sie die Option Fehlgeschlagen, um weitere Details anzuzeigen.

> **Note**
>
> Die Bearbeitung einer Freigabeanforderung kann bis zu 15 Minuten dauern. Wenn also beim Senden Ihrer Freigabeanfrage an den Empfänger ein Fehler aufgetreten ist, wird der Status Fehlgeschlagen möglicherweise nicht sofort angezeigt. Wir empfehlen Ihnen, später zu überprüfen, ob der Versand erfolgreich war.

Schritt 4 (optional): Widerrufen der Freigabeanfrage

Wenn Sie eine aktive Freigabeanfrage stornieren müssen, bevor sie abläuft, können Sie die Anfrage jederzeit widerrufen. Dieser Schritt ist optional. Unternehmen Sie nichts, kann der Empfänger die Freigabeanfrage nach Ablauf des Ablaufdatums nicht mehr annehmen.

Eine Freigabeanfrage widerrufen

1. Wählen Sie im Navigationsbereich Freigabeanfragen aus.
2. Wählen Sie die Registerkarte Gesendete Anfragen.
3. Wählen Sie das Framework aus, das Sie widerrufen möchten, und wählen Sie Anfrage widerrufen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster zur Bestätigung die Option Widerrufen.

> **Note**
>
> Sie können den Zugriff nur für Freigabeanfragen widerrufen, die den Status Aktiv oder Läuft ab haben. Nachdem ein Empfänger eine Freigabeanfrage akzeptiert hat, können Sie ihm den Zugriff auf dieses benutzerdefinierte Framework nicht mehr entziehen. Dies liegt daran, dass eine Kopie des benutzerdefinierten Frameworks jetzt in der Framework-Bibliothek des Empfängers vorhanden ist.
> Bei der gemeinsamen Nutzung von AWS-Regionen Frameworks kann es bis zu 10 Minuten dauern, bis Aktionen zur Freigabe von Anfragen bearbeitet sind. Nach dem Widerruf einer regionsübergreifenden Freigabeanfrage empfehlen wir Ihnen, später zu prüfen, ob die Freigabeanfrage erfolgreich widerrufen wurde.

Nächste Schritte

Eine Freigabeanfrage für ein aktualisiertes Framework erneut senden

Sie können eine Freigabeanforderung für ein benutzerdefiniertes Framework senden und dann dasselbe Framework aktualisieren. In diesem Fall wird die Freigabeanfrage nicht automatisch aktualisiert, sodass sie die neueste Version des Frameworks wiedergibt. Wenn ihr Status jedoch aktiv, freigegeben oder läuft ab zeigt, können Sie eine bestehende Freigabeanfrage aktualisieren. Dazu senden Sie erneut eine Freigabeanfrage mit den gleichen Angaben wie die bestehende Anfrage. Geben Sie in der neuen Freigabeanfrage dieselbe benutzerdefinierte Framework-ID, Empfängerkonto-ID und die dieselbe AWS-Region des Empfänger an. Sie können der neuen Freigabeanfrage auch einen neuen Kommentar beifügen.

Beachten Sie Folgendes, wenn Sie eine Freigabeanforderung erneut senden:

- Damit die Änderung erfolgreich ist, muss sich die neue Anfrage auf dieselbe benutzerdefinierte Framework-ID beziehen. Außerdem müssen dieselbe Empfängerkonto-ID und Region wie in der vorhandenen Anfrage angegeben werden.
- Wenn sich der Name des benutzerdefinierten Frameworks geändert hat, wird in der aktualisierten Freigabeanforderung der neueste Name angezeigt.
- Nach der Eingabe eines neuen Kommentars wird dieser in der aktualisierten Freigabeanforderung angezeigt.
- Wenn Sie eine Freigabeanfrage erneut senden, verlängert sich das Ablaufdatum um sechs Monate.

Eine Freigabeanfrage für ein aktualisiertes Framework erneut senden

1. Wählen Sie in Framework-Bibliothek die Registerkarte Benutzerdefinierte Frameworks den Namen eines Frameworks aus, um die Details zu öffnen. Dadurch wird die Ansicht „Framework-Details“ geöffnet.
2. Wählen Sie Aktionen und anschließend Benutzerdefiniertes Framework teilen aus.
3. Prüfen Sie den im Dialogfeld angezeigten Hinweis, geben Sie **`agree`** ein und wählen Sie Zustimmen, um fortzufahren.
4. Befolgen Sie in der nächsten Ansicht diese Schritte:
   - Geben Sie unter AWS-Konto dieselbe Konto-ID ein, die Sie in der vorhandenen Freigabeanfrage angegeben haben.
   - Wählen Sie unter AWS-Region dieselbe Region aus, die Sie in der bestehenden Freigabeanfrage angegeben haben.
   - (Optional) geben Sie unter Nachricht an den Empfänger einen Kommentar zum benutzerdefinierten Framework ein, das Sie freigeben.
   - Überprüfen Sie unter Details zum benutzerdefinierten Framework die Details, um zu bestätigen, dass Sie die Freigabeanfrage erneut senden möchten.
5. Wählen Sie Freigeben aus, um die Freigabeanfrage erneut zu senden und zu aktualisieren.

Weitere Ressourcen

Lösungen für Probleme, die beim Teilen eines benutzerdefinierten Frameworks auftreten können, finden Sie unterBehebung von Framework-Problemen.

Antworten auf Anfragen zum Teilen in AWS Audit Manager

In diesem Tutorial werden die auszuführenden Aktionen beschrieben, wenn Sie eine Freigabeanforderung für ein benutzerdefiniertes Framework erhalten. Audit Manager benachrichtigt bei Erhalt einer Freigabeanfrage. Sie erhalten außerdem eine Erinnerung, wenn eine Freigabeanfrage in den nächsten 30 Tagen abläuft.

Voraussetzungen

Machen Sie sich zunächst in Audit Manager mit Framework-Konzepte und -Terminologie freigeben vertraut.

Verfahren

Aufgaben

- Schritt 1: Überprüfen Sie Ihre erhaltenen Benachrichtigungen über Anfragen
- Schritt 2: Ergreifen Sie Maßnahmen in Bezug auf die Anfrage
- Schritt 3: Sehen Sie sich den Verlauf Ihrer eingegangenen Anfragen an

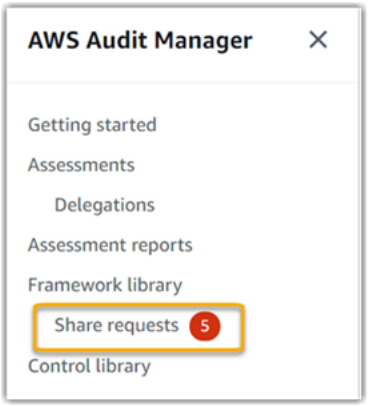
Schritt 1: Überprüfen Sie Ihre erhaltenen Benachrichtigungen über Anfragen

Überprüfen Sie zunächst Ihre Benachrichtigungen zu Freigabeanfragen. Auf der Registerkarte Empfangene Anfragen wird eine Liste der Teilungsanfragen angezeigt, die Sie von anderen erhalten haben AWS-Konten. Offene Anfragen werden mit einem blauen Punkt markiert. Sie können diese Ansicht auch so filtern, dass nur Anfragen angezeigt werden, die innerhalb der nächsten 30 Tage ablaufen.

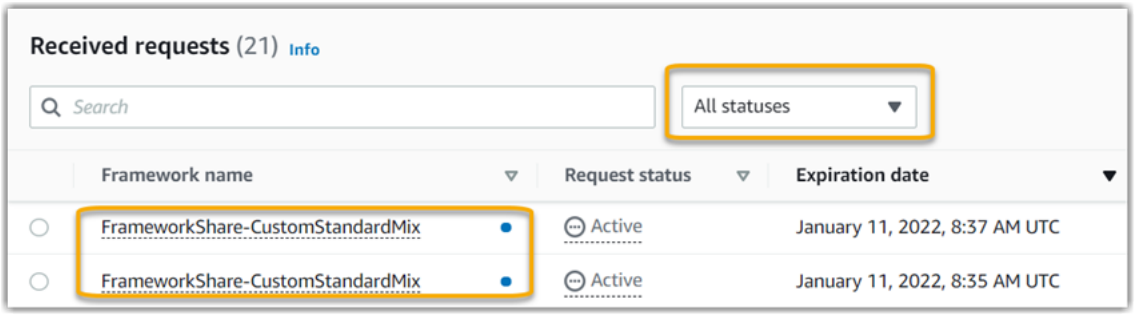
Eingegangene Anfragen anzeigen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wenn Sie eine Benachrichtigung über eine Freigabeanfrage haben, sehen Sie in Audit Manager einen roten Punkt neben dem Navigationssymbol.

3. Erweitern Sie den Navigationsbereich und suchen Sie nach Freigabeanfragen. Ein Benachrichtigungssymbol gibt die Anzahl der Freigabeanfragen an, die Ihre Aufmerksamkeit erfordern.



4. Wählen Sie Freigabeanfragen aus. Standardmäßig wird diese Seite auf der Registerkarte Empfangene Anfragen geöffnet.
5. Identifizieren Sie die Freigabeanfrage, die Sie bearbeiten müssen, indem Sie nach Elementen mit einem blauen Punkt suchen.



6. Um (optional) nur Anfragen anzuzeigen, die in den nächsten 30 Tagen ablaufen, suchen Sie in der Dropdownliste Alle Status nach und wählen Sie Läuft ab.

Schritt 2: Ergreifen Sie Maßnahmen in Bezug auf die Anfrage

Um den blauen Statuspunkt zu entfernen, müssen Sie Maßnahmen ergreifen, indem Sie die Freigabeanfrage entweder annehmen oder ablehnen.

Akzeptieren eines geteilten Frameworks

Wenn Sie eine Freigabeanfrage annehmen, repliziert Audit Manager einen Snapshot des ursprünglichen Frameworks in die Registerkarte „Benutzerdefinierte Frameworks“ Ihrer Framework-Bibliothek. Audit Manager repliziert und verschlüsselt das neue benutzerdefinierte Framework mithilfe des KMS-Schlüssels, den Sie in Ihren Audit Manager-Einstellungen angegeben haben.

Akzeptieren einer Freigabeanfrage

1. Öffnen Sie die Seite Anfragen freigeben und vergewissern Sie sich, dass die Registerkarte Empfangene Anfragen angezeigt wird.
2. (Optional) wählen Sie in der Filter-Dropdownliste die Option Aktiv oder Läuft ab aus.
3. (Optional) wählen Sie einen Framework-Namen aus, um die Details der Freigabeanforderung anzuzeigen. Dazu gehören Informationen, wie die Framework-Beschreibung, die Anzahl der Kontrollen, die sich im Framework befinden, und die Nachricht des Absenders.
4. Wählen Sie die Freigabeanfrage aus, die Sie annehmen möchten, klicken Sie auf Aktionen und dann auf Annehmen.

Nachdem Sie eine Freigabeanfrage akzeptiert haben, ändert sich der Status auf Replizieren, während das freigegebene benutzerdefinierte Framework zu Ihrer Framework-Bibliothek hinzugefügt wird. Wenn das Framework benutzerdefinierte Kontrollen enthält, werden diese zu diesem Zeitpunkt zu Ihrer Kontrollbibliothek hinzugefügt.

Wenn die Framework-Replikation abgeschlossen ist, ändert sich der Status in Freigegeben. Eine Bestätigung informiert Sie darüber, dass das benutzerdefinierte Framework einsatzbereit ist.

> **Tip**
>
> Wenn Sie ein benutzerdefiniertes Framework akzeptieren, wird es nur in Ihre aktuelle AWS-Region repliziert. Möglicherweise möchten Sie, dass das neue gemeinsame Framework in allen Regionen Ihres AWS-Konto verfügbar ist. Falls ja, können Sie nach der Akzeptanz der Freigabeanfrage das Framework freigeben, je nach Bedarf unter Ihrem Konto für andere Regionen.

Ein freigegebenes Framework ablehnen

Wenn Sie eine Freigabeanfrage ablehnen, fügt Audit Manager dieses benutzerdefinierte Framework nicht zu Ihrer Framework-Bibliothek hinzu. Eine Aufzeichnung der abgelehnten Freigabeanfrage verbleibt jedoch auf der Registerkarte Empfangene Anfragen mit dem Status Inaktiv.

Eine Freigabeanfrage ablehnen

1. Öffnen Sie die Seite Anfragen freigeben und vergewissern Sie sich, dass die Registerkarte Empfangene Anfragen angezeigt wird.
2. (Optional) wählen Sie in der Filter-Dropdownliste die Option Aktiv oder Läuft ab aus.
3. (Optional) wählen Sie einen Framework-Namen aus, um die Details der Freigabeanforderung anzuzeigen. Dazu gehören Informationen, wie die Framework-Beschreibung, die Anzahl der Kontrollen, die sich im Framework befinden, und die Nachricht des Absenders.
4. Wählen Sie die Freigabeanfrage aus, die Sie ablehnen möchten, wählen Sie Aktionen und dann Ablehnen aus.
5. Wählen Sie im jetzt angezeigten Dialogfeld Löschen aus, um Ihre Wahl zu bestätigen.

> **Tip**
>
> Wenn Sie später doch Zugriff auf ein freigegebenes Framework möchten, nachdem Sie es abgelehnt haben, bitten Sie den Absender, eine neue Freigabeanfrage zu senden.

> **Note**
>
> Wenn Frameworks über AWS-Regionen freigegeben werden, kann es bis zu 10 Minuten dauern, bis die Freigabeanforderung bearbeitet wird. Nach den Maßnahmen zu einer regionsübergreifenden Freigabeanfrage empfehlen wir Ihnen, später zu prüfen, ob die Freigabeanfrage erfolgreich angenommen oder abgelehnt wurde.

Schritt 3: Sehen Sie sich den Verlauf Ihrer eingegangenen Anfragen an

Nachdem Sie ein geteiltes Framework akzeptiert oder abgelehnt haben, können Sie zur Seite Anfragen freigeben zurückkehren, um den Verlauf Ihrer Freigabeanfragen einzusehen. Sie können diese Liste nach Bedarf filtern. Sie können beispielsweise Filter anwenden, um nur Anfragen anzuzeigen, die Sie akzeptiert haben.

Einen Verlauf Ihrer Freigabeanfrage einsehen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Freigabeanfragen aus.
3. Wählen Sie die Registerkarte Empfangene Anfragen.
4. Suchen Sie die Dropdownliste Alle Status und wählen Sie einen der folgenden Filter aus:

Name	Beschreibung
Aktiv	Dieser Filter zeigt Anfragen zum Teilen an, die Sie noch nicht akzeptiert oder abgelehnt haben.
Läuft ab	Dieser Filter zeigt Share-Anfragen an, die in den nächsten 30 Tagen ablaufen.

Name	Beschreibung
Geteilt	Dieser Filter zeigt Anfragen zum Teilen an, die Sie akzeptiert haben. Das freigegebene Framework ist jetzt in Ihrer Framework -Bibliothek verfügbar.
Inaktiv	Dieser Filter zeigt Freigabeanfragen an, die abgelehnt wurden oder abgelaufen sind.
Fehlgeschlagen	Dieser Filter zeigt die Teilungsanfragen an, die nicht erfolgreich gesendet wurden. Wählen Sie die Option Fehlgeschlagen, um weitere Details anzuzeigen.

Nächste Schritte

Nachdem Sie ein freigegebenes benutzerdefiniertes Framework akzeptiert haben, finden Sie es hinter der Registerkarte „Benutzerdefinierte Frameworks“ der Framework-Bibliothek. Sie können dieses Framework jetzt verwenden, um eine Bewertung zu erstellen. Weitere Informationen hierzu finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Anweisungen zur Bearbeitung Ihres neuen benutzerdefinierten Frameworks finden Sie unterBearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager.

Weitere Ressourcen

Lösungen für Probleme, auf die Sie möglicherweise stoßen, finden Sie unterBehebung von Framework-Problemen.

Löschen von Anfragen zum Teilen in AWS Audit Manager

Wenn Sie eine Freigabeanfrage nicht mehr benötigen, können Sie sie aus Ihrer Audit Manager Manager-Umgebung löschen. Auf diese Weise können Sie Ihren Arbeitsbereich aufräumen und sich auf die Anfragen konzentrieren, die für Ihre aktuellen Aufgaben und Prioritäten relevant sind.

Wenn Sie eine Freigabeanfrage löschen, wird nur die Anfrage selbst gelöscht. Das freigegebene Framework selbst verbleibt in Ihrer Framework-Bibliothek.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass du zuvor eine Anfrage zum Teilen gesendet oder empfangen hast. Sie können keine Freigabeanfragen löschen, die den Status Aktiv oder Replizieren haben.

Stellen Sie sicher, dass Ihre IAM-Identität über die erforderlichen Berechtigungen zum Löschen einer Freigabeanfrage in AWS Audit Manager verfügt. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Eine Freigabeanfrage löschen

1. Wählen Sie im Navigationsbereich Freigabeanfragen aus.
2. Wählen Sie entweder die Registerkarte Gesendete Anfragen oder Empfangene Anfragen.
3. Wählen Sie das Framework aus, das Sie nicht mehr benötigen, und wählen Sie Löschen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option Löschen.

Weitere Ressourcen

Lösungen für Probleme, auf die Sie möglicherweise stoßen, finden Sie unterBehebung von Framework-Problemen.

Löschen eines benutzerdefinierten Frameworks in AWS Audit Manager

Wenn Sie ein benutzerdefiniertes Framework nicht mehr benötigen, können Sie es aus Ihrer Audit Manager Manager-Umgebung löschen. Auf diese Weise können Sie Ihren Arbeitsbereich aufräumen und sich auf die benutzerdefinierten Frameworks konzentrieren, die für Ihre aktuellen Aufgaben und Prioritäten relevant sind.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor ein benutzerdefiniertes Framework erstellt haben.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Löschen eines benutzerdefinierten Frameworks verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können benutzerdefinierte Frameworks mithilfe der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) löschen.

> **Note**
>
> Das Löschen eines benutzerdefinierten Frameworks hat keine Auswirkungen auf bestehende Bewertungen, die vor dem Löschen aus dem Framework erstellt wurden.

Audit Manager console

Um ein benutzerdefiniertes Framework in der Audit Manager Manager-Konsole zu löschen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek und dann Benutzerdefiniertes Framework aus.
3. Wählen Sie das zu löschende Framework aus, klicken Sie auf Aktionen und dann auf Löschen.
   - Alternativ können Sie ein benutzerdefiniertes Framework öffnen und oben rechts auf der Zusammenfassung des Frameworks Aktionen, Löschen auswählen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster Löschen, um den Löschvorgang zu bestätigen.

AWS CLI

Um ein benutzerdefiniertes Framework in der AWS CLI

1. Identifizieren des benutzerdefinierten Frameworks, das Sie löschen möchten. Führen Sie dazu den list-assessment-frameworksBefehl aus und geben Sie `--framework-type` as an`Custom`.

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Als Antwort wird eine Liste von benutzerdefinierten Frameworks zurückgegeben. Suchen Sie das benutzerdefinierte Framework, das Sie löschen möchten, und notieren Sie sich die Framework-ID.

2. Führen Sie als Nächstes den delete-assessment-frameworkBefehl aus und geben Sie das Framework an, das Sie löschen möchten. `--framework-id`

   Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Um ein benutzerdefiniertes Framework mithilfe der API zu löschen

1. Verwenden Sie den ListAssessmentFrameworksVorgang und geben Sie den FrameworkType als an. `Custom` Suchen Sie aus den Rückmeldungen das benutzerdefinierte Framework, das Sie löschen möchten, und notieren Sie sich die Framework-ID.
2. Verwenden Sie den DeleteAssessmentFrameworkVorgang, um das Framework zu löschen. Verwenden Sie in der Anforderung den FrameworkID-Parameter, um das Framework anzugeben, das Sie löschen möchten.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, indem Sie auf einen der Links im vorherigen Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Weitere Ressourcen

Informationen zur Datenspeicherung in Audit Manager finden Sie unterLöschung von Audit Manager-Daten.

Verwenden der Steuerbibliothek zur Verwaltung von Steuerelementen in AWS Audit Manager

Sie können in der Kontrollbibliothek unter auf Kontrollen zugreifen und diese verwalten AWS Audit Manager.

Wichtige Punkte

In der Steuerbibliothek sind die Steuerelemente in die folgenden Kategorien unterteilt.

- Bei Common Controls werden Nachweise gesammelt, die mehrere sich überschneidende Compliance-Standards belegen. Automatisierte gemeinsame Kontrollen enthalten eine oder mehrere verwandte Kernkontrollen, bei denen jeweils unterstützende Nachweise aus einer vordefinierten Gruppe von Datenquellen gesammelt werden. Auf diese Weise können Sie auf effiziente Weise die AWS Datenquellen identifizieren, die Ihrem Portfolio an Compliance-Anforderungen entsprechen. Die zugrunde liegenden Datenquellen für jede automatisierte gemeinsame Kontrolle werden von branchenweit zertifizierten Prüfern der AWS Security Assurance Services validiert und verwaltet.
- Bei Standardkontrollen werden Nachweise zur Unterstützung eines bestimmten Compliance-Standards gesammelt. Sie können die Details der Standardkontrollen anzeigen, sie jedoch nicht bearbeiten oder löschen. Sie können jedoch von jedem Standardsteuerelement eine bearbeitbare Kopie erstellen, um ein neues Steuerelement zu erstellen, das Ihren spezifischen Anforderungen entspricht.
- Benutzerdefinierte Steuerelemente sind Steuerelemente, die Ihnen gehören und die Sie selbst definieren. Wenn Sie ein benutzerdefiniertes Steuerelement erstellen, empfehlen wir Ihnen, die allgemeinen Steuerelemente auszuwählen, die Ihren Zielen entsprechen, und sie als Beweisquelle zu verwenden. Somit kann Ihr benutzerdefiniertes Steuerelement alle Beweise sammeln, die für diese allgemeinen Kontrollen relevant sind. Sie können auch zentrale Kontrollen als Beweisquelle verwenden oder andere Quellen verwenden, die Sie selbst definieren. Wenn Sie fertig sind, fügen Sie Ihre benutzerdefinierten Kontrollen zu einem benutzerdefinierten Framework hinzu und erstellen Sie dann eine Bewertung, um mit der Erfassung von Nachweisen zu beginnen.

Weitere Ressourcen

Folgen Sie den hier beschriebenen Verfahren, um Kontrollen in Audit Manager zu erstellen und zu verwalten.

- Finden Sie die verfügbaren Steuerelemente in AWS Audit Manager
- Überprüfung einer Kontrolle in AWS Audit Manager
  - Überprüfung einer gemeinsamen Kontrolle
  - Überprüfung einer zentralen Kontrolle
  - Überprüfung einer Standardkontrolle
  - Überprüfung eines benutzerdefinierten Steuerelements
- Erstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager
  - Ein benutzerdefiniertes Steuerelement von Grund auf neu erstellen in AWS Audit Manager
  - Eine bearbeitbare Kopie einer Kontrolle erstellen in AWS Audit Manager
- Bearbeiten eines benutzerdefinierten Steuerelements in AWS Audit Manager
- Ändern der Häufigkeit, mit der eine Kontrolle Beweise sammelt
- Löschen eines benutzerdefinierten Steuerelements in AWS Audit Manager
- Unterstützte Datenquellentypen für automatisierte Beweise
  - AWS-Config-Regeln unterstützt von AWS Audit Manager
  - AWS Security Hub CSPM Steuerelemente, die unterstützt werden von AWS Audit Manager
  - AWS API-Aufrufe werden unterstützt von AWS Audit Manager
  - AWS CloudTrail Eventnamen werden unterstützt von AWS Audit Manager

Finden Sie die verfügbaren Steuerelemente in AWS Audit Manager

Sie finden alle verfügbaren Steuerelemente auf der Seite „Kontrollbibliothek“ in der Audit Manager Manager-Konsole.

Sie können alle verfügbaren Kontrollen auch mithilfe der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) anzeigen.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen von Kontrollen verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Audit Manager console

So zeigen Sie die verfügbaren Steuerelemente in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie eine Registerkarte, um die verfügbaren Steuerelemente zu durchsuchen.
   - Wählen Sie Allgemein, um die allgemeinen Steuerelemente anzuzeigen, die von bereitgestellt werden AWS.
   - Wählen Sie Standard, um die Standardsteuerungen zu sehen, die von bereitgestellt werden AWS.
   - Wählen Sie Benutzerdefiniert, um die von Ihnen erstellten benutzerdefinierten Steuerelemente anzuzeigen.

AWS CLI

Um häufig verwendete Steuerelemente in der Datei (AWS CLI

Führen Sie den list-common-controlsBefehl aus, um eine Liste gängiger Steuerelemente anzuzeigen.

```
aws controlcatalog list-common-controls
```

Sie können das optionale `common-control-filter` Attribut auch verwenden, um eine Liste gängiger Steuerelemente zurückzugeben, die ein bestimmtes Ziel verfolgen.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

Weitere Arten von Steuerelementen finden Sie in AWS CLI

Führen Sie den Befehl list-controls aus und geben Sie den Wert `--control-type` als `CustomStandard`, oder an. `Core`

Ersetzen Sie im folgenden Beispiel die *placeholder text* durch Ihre eigenen Informationen.

```
aws auditmanager list-controls --control-type Type
```

Audit Manager API

Um allgemeine Steuerelemente mithilfe der API zu finden

Verwenden Sie den ListCommonControlsVorgang, um eine Liste der verfügbaren allgemeinen Steuerelemente anzuzeigen. Sie können das optionale `commonControlFilter` Attribut auch verwenden, um eine Liste von Kontrollen zurückzugeben, die ein bestimmtes Ziel verfolgen.

Um andere Arten von Kontrollen mithilfe der API zu finden

Verwenden Sie die ListControlsOperation und geben Sie den ControlType als `CustomStandard`, oder `Core` an.

Weitere Informationen erhalten Sie, indem Sie einen der Links aus dem vorherigen Verfahren auswählen, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Wenn Sie bereit sind, sich mit den Details eines Steuerelements vertraut zu machen, folgen Sie den Schritten unter. Überprüfung einer Kontrolle in AWS Audit Manager Diese Seite führt Sie durch die Kontrolldetails und erklärt die dort angezeigten Informationen.

Auf der Seite mit der Steuerelementbibliothek können Sie auch ein benutzerdefiniertes Steuerelement erstellen, ein benutzerdefiniertes Steuerelement bearbeiten oder ein benutzerdefiniertes Steuerelement löschen.

Weitere Ressourcen

Lösungen zur Kontrolle von Problemen in Audit Manager finden Sie unterBehebung von Problemen mit Kontrollen und Kontrollsätzen.

Überprüfung einer Kontrolle in AWS Audit Manager

Sie können die Details einer Kontrolle überprüfen, indem Sie die Audit Manager Manager-Konsole, die Audit Manager Manager-API oder die AWS Command Line Interface (AWS CLI) verwenden.

Um mit der Überprüfung einer Kontrolle in Audit Manager zu beginnen, folgen Sie den hier beschriebenen Verfahren.

- Überprüfung einer gemeinsamen Kontrolle
- Überprüfung einer zentralen Kontrolle
- Überprüfung einer Standardkontrolle
- Überprüfung eines benutzerdefinierten Steuerelements

Überprüfung einer gemeinsamen Kontrolle

Wenn Sie die Details einer Kontrolle überprüfen möchten, finden Sie die Informationen auf der Seite mit den Kontrolldetails in mehreren Abschnitten. Diese Abschnitte helfen Ihnen, auf einfache Weise auf die relevanten Informationen für dieses Steuerelement zuzugreifen und diese zu verstehen.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen verfügt, um allgemeine Kontrollen in Audit Manager anzuzeigen. Insbesondere benötigen Sie die folgenden Berechtigungen, um die allgemeinen Kontrollen, Kontrollziele und Kontrolldomänen anzuzeigen, die von AWS Control Catalog bereitgestellt werden:

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

Eine vorgeschlagene Richtlinie, die diese Berechtigungen gewährt, ist AWSAuditManagerAdministratorAccess.

Verfahren

Sie können ein allgemeines Steuerelement mithilfe der Audit Manager Manager-Konsole, der AWS Control Catalog API oder der AWS Command Line Interface (AWS CLI) überprüfen.

Audit Manager console

So zeigen Sie allgemeine Kontrolldetails in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie Allgemein, um die allgemeinen Kontrollen zu sehen, die von bereitgestellt werden AWS.
4. Wählen Sie einen beliebigen allgemeinen Steuerelementnamen, um die Details für dieses Steuerelement anzuzeigen.
5. Überprüfen Sie die allgemeinen Kontrolldetails anhand der folgenden Informationen als Referenz.

Abschnitt „Überblick“

In diesem Abschnitt wird die allgemeine Steuerung beschrieben.

Registerkarte „Beweisquellen“

Diese Registerkarte enthält die folgenden Informationen:

Name	Description
Wichtigste Steuerelemente	Dies sind die Kernkontrollen, mit denen Beweise gesammelt werden, um die gemeinsame Kontrolle zu stützen. • Wenn Sie Beweise für diese gemeinsame Kontrolle sammeln, sammeln Sie automatisch Beweise für alle hier aufgeführten Kernkontrollen. Wenn jede dieser zentralen Kontrollen erfolgreich implementiert wurde, können Sie

Name	Description
	damit nachweisen, dass Sie die Anforderungen der gemeinsamen Kontrolle erfüllen. • Jedes zentrale Steuerelement verwendet eine vordefinierte Gruppierung von Datenquellen, um Beweise für eine AWS-Service zu sammeln. AWS verwaltet diese Datenquellen für Sie. Das bedeutet, dass sie automatisch aktualisiert werden, wenn sich Vorschriften und Standards ändern und neue Datenquellen identifiziert werden. Wählen Sie ein beliebige s zentrales Steuerelement aus, um die zugrunde liegenden Datenquellen zu sehen.

Registerkarte „Verwandte Anforderungen“

Wenn Sie Nachweise für diese allgemeine Kontrolle sammeln, können Sie anhand derselben Nachweise die Einhaltung der Anforderungen der entsprechenden Standardkontrollen nachweisen, die auf dieser Registerkarte aufgeführt sind. Wählen Sie ein beliebiges Standardsteuerelement aus, um weitere Informationen zu erhalten.

> **Note**
>
> - Bei der gemeinsamen Kontrolle kann der Nachweis erbracht werden, dass eine Standardkontrolle nur teilweise eingehalten wird. Es ist möglich, dass Sie zusätzliche Nachweise benötigen, um die vollständige Einhaltung einer Standardkontrolle nachzuweisen.
> - Derzeit werden auf der Registerkarte „Verwandte Anforderungen“ nur entsprechende Standardkontrollen angezeigt. Obwohl ein allgemeines Steuerelement mit einem oder mehreren benutzerdefinierten Steuerelementen verknüpft werden kann, werden diese Beziehungen auf dieser Registerkarte nicht angezeigt.

AWS CLI

Um allgemeine Steuerelementdetails anzuzeigen, finden Sie im AWS CLI

1. Führen Sie den list-common-controlsBefehl aus, um eine Liste der verfügbaren allgemeinen Steuerelemente anzuzeigen. Wenn Sie diesen Vorgang verwenden, können Sie eine optionale Option verwenden, `common-control-filter` um allgemeine Steuerelemente anzuzeigen, die einem bestimmten Zweck dienen.

   ```
   aws controlcatalog list-common-controls
   ```

2. Identifizieren Sie in der Antwort die allgemeine Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Einzelheiten.

AWS Control Catalog API

Um allgemeine Kontrolldetails mithilfe der API anzuzeigen

1. Verwenden Sie den ListCommonControlsVorgang, um eine Liste der verfügbaren allgemeinen Steuerelemente anzuzeigen. Wenn Sie diese Operation verwenden, können Sie eine optionale Option anwenden, `commonControlFilter` um eine Liste von Steuerelementen anzuzeigen, die einem bestimmten Zweck dienen.
2. Identifizieren Sie in der Antwort das Steuerelement, das Sie überprüfen möchten, und notieren Sie sich die Einzelheiten.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, wenn Sie auf den Link in diesem Verfahren klicken, um weitere Informationen in der API-Referenz zum AWS Kontrollkatalog zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Sie können die allgemeinen Steuerelemente auswählen, die Ihre Ziele repräsentieren, und sie als Bausteine verwenden, um ein benutzerdefiniertes Steuerelement zu erstellen. Jedes automatisierte gemeinsame Steuerelement ist einer vordefinierten Gruppierung von AWS Datenquellen zugeordnet, die Audit Manager für Sie verwaltet. Das bedeutet, dass Sie kein AWS Experte sein müssen, um zu

wissen, welche Datenquellen die relevanten Beweise für Ihre Ziele sammeln. Darüber hinaus müssen Sie diese Datenquellenzuordnungen nicht selbst verwalten.

Anweisungen zum Erstellen eines benutzerdefinierten Steuerelements, das allgemeine Steuerelemente als Beweisquelle verwendet, finden Sie unter. Erstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager

Weitere Ressourcen

- Überprüfung eines zentralen Steuerelements
- Überprüfung einer Standardkontrolle
- Überprüfung eines benutzerdefinierten Steuerelements

Überprüfung einer Kernkontrolle

Sie können die Details einer zentralen Steuerung mithilfe der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) überprüfen.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen von Kontrollen verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Audit Manager console

So zeigen Sie die wichtigsten Kontrolldetails in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie Allgemein, um die allgemeinen Kontrollen zu sehen, die von bereitgestellt werden AWS.
4. Suchen Sie nach dem allgemeinen Steuerelement, das Ihrem Anwendungsfall entspricht.

5. Wählen Sie das Symbol für die Strukturansicht neben dem Namen des allgemeinen Steuerelements aus. Dadurch werden die wichtigsten Steuerelemente angezeigt, die das gemeinsame Steuerelement unterstützen.
6. Wählen Sie den Namen des zentralen Steuerelements, das Sie überprüfen möchten.
7. Überprüfen Sie die Details der Kernkontrolle anhand der folgenden Informationen als Referenz.

Abschnitt „Überblick“

In diesem Abschnitt wird das zentrale Steuerelement beschrieben und die Datenquellentypen aufgeführt, aus denen Beweise gesammelt werden.

Registerkarte „Quellen der Beweise“

Diese Registerkarte enthält die folgenden Informationen:

Name	Description

Datenquellen	Dies sind die AWS verwalteten Datenquellen, aus denen die zentrale Steuerung Beweise sammelt. Diese Datenquellen werden automatisch aktualisiert, wenn sich Vorschriften und Standards ändern und neue Datenquellen identifiziert werden.
	• Kartierung — Das spezifische Schlüsselwort, das zum Sammeln von Beweisen verwendet wird.
	  • Wenn der Typ ist AWS Config, handelt es sich bei der Zuordnung um eine AWS Config Regel (z. B. `SNS_ENCRYPTED_KMS`).
	  • Wenn der Typ ist AWS Security Hub CSPM, handelt es sich bei der Zuordnung um ein Security Hub CSPM-Steuerelement (z. B. `EC2.1`).
	  • Handelt es sich bei dem Typ um AWS API-Aufrufe, handelt es sich bei der Zuordnung um einen API-Aufruf (z. B. `kms_ListKeys`).
	  • Wenn es sich um einen Typ handelt AWS CloudTrail, handelt es sich bei der Zuordnung um ein CloudTrail Ereignis (z. B. `CreateAccessKey`).

Name	Description

	• Typ — Der Typ der Datenquelle, aus der die Beweise stammen.
	  • Wenn Audit Manager die Beweise sammelt, kann es sich bei dem Typ um AWS Security Hub CSPMAWS Config, AWS CloudTrail, oder AWS API-Aufrufe handeln.
	  • Wenn Sie Ihre eigenen Nachweise hochladen, ist der Typ Manuell. Eine Beschreibung gibt an, ob es sich bei den erforderlichen manuellen Beweisen um einen Datei-Upl oad oder eine Textantwort handelt.
	• Häufigkeit — Wie oft Audit Manager Beweise für eine AWS API-Aufruf-Datenquelle sammelt.

Registerkarte Details

Diese Registerkarte enthält die folgenden Informationen:

Name	Description
Anweisungen	Die Anweisungen, die beschreiben, wie die Steuerung getestet und behoben werden kann.
Informationen zum Testen	Die empfohlenen Testverfahren.
Aktionsplan	Die empfohlenen Maßnahmen, die Sie ergreifen sollten, wenn Sie die Kontrolle korrigieren müssen.

AWS CLI

Um Details zu den wichtigsten Steuerelementen einzusehen, finden Sie AWS CLI

1. Folgen Sie den Schritten, um ein Steuerelement zu finden. Stellen Sie sicher, dass Sie das `--control-type` als festlegen`Core`, und wenden Sie bei Bedarf alle optionalen Filter an.

```
aws auditmanager list-controls --control-type Core
```

2. Identifizieren Sie in der Antwort die Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den Amazon-Ressourcennamen (ARN).
3. Führen Sie den Befehl get-control aus und geben Sie den `--control-id` an. Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Die Kontrolldetails werden im JSON-Format zurückgegeben. Informationen zum besseren Verständnis dieser Daten finden Sie in der AWS CLI Befehlsreferenz unter get-control Output.

4. Um die Tag-Details zu sehen, führen Sie den list-tags-for-resourceBefehl aus und geben Sie den `--resource-arn` an. Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Um die wichtigsten Kontrolldetails mithilfe der API anzuzeigen

1. Folgen Sie den Schritten, um ein Steuerelement zu finden. Stellen Sie sicher, dass der ControlType auf eingestellt ist`Core`, und wenden Sie bei Bedarf alle optionalen Filter an.
2. Identifizieren Sie in der Antwort die Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den Amazon-Ressourcennamen (ARN).
3. Verwenden Sie den GetControlVorgang und geben Sie die Kontroll-ID an, die Sie sich in Schritt 2 notiert haben.

> **Tip**
>
> Die Kontrolldetails werden im JSON-Format zurückgegeben. Informationen zum besseren Verständnis dieser Daten finden Sie unter GetControl Antwortelemente in der AWS Audit Manager API-Referenz.

4. Um Tag-Details anzuzeigen, verwenden Sie den ListTagsForResourceVorgang und geben Sie den resourceArn, den Sie in Schritt 2 notiert haben.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, indem Sie auf einen der Links in diesem Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Sie können die wichtigsten Steuerelemente auswählen, die Ihre Ziele repräsentieren, und sie als Bausteine verwenden, um ein benutzerdefiniertes Steuerelement zu erstellen. Jede automatisierte Kernsteuerung ist einer vordefinierten Gruppierung von AWS Datenquellen zugeordnet, die Audit Manager für Sie verwaltet. Das bedeutet, dass Sie kein AWS Experte sein müssen, um zu wissen, welche Datenquellen die relevanten Beweise für Ihre Ziele sammeln. Darüber hinaus müssen Sie diese Datenquellenzuordnungen nicht selbst verwalten.

Anweisungen zum Erstellen eines benutzerdefinierten Steuerelements, das zentrale Steuerelemente als Beweisquelle verwendet, finden Sie unter. Erstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager

Weitere Ressourcen

- Ein allgemeines Steuerelement überprüfen
- Überprüfung einer Standardkontrolle
- Überprüfung eines benutzerdefinierten Steuerelements

Überprüfung einer Standardkontrolle

Sie können die Details einer Standardkontrolle überprüfen, indem Sie die Audit Manager Manager-Konsole, die Audit Manager Manager-API oder die AWS Command Line Interface (AWS CLI) verwenden.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen von Kontrollen verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können die Details einer Standardkontrolle überprüfen, indem Sie die Audit Manager Manager-Konsole, die Audit Manager Manager-API oder die AWS Command Line Interface (AWS CLI) verwenden.

Audit Manager console

So zeigen Sie Standardkontrolldetails in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie Standard, um die Standardkontrollen zu sehen, die von bereitgestellt werden AWS.
4. Wählen Sie einen beliebigen Namen für das Standardsteuerelement, um die Details für dieses Steuerelement anzuzeigen.
5. Überprüfen Sie die Standardkontrolldetails anhand der folgenden Informationen als Referenz.

Abschnitt „Überblick“

In diesem Abschnitt wird das Standardsteuerelement beschrieben und die Datenquellentypen aufgeführt, die zum Sammeln von Nachweisen verwendet werden.

Registerkarte „Quellen für Nachweise“

Diese Registerkarte enthält die folgenden Informationen:

Name	Description
Wichtigste Steuerelemente	Dies sind die Kernkontrollen, mit denen Beweise zur Unterstützung der Standardkontrolle gesammelt werden. Jede Kernkontrolle verwendet eine vordefinierte Gruppierung von Datenquellen, um Beweise für eine AWS-Service zu sammeln. Diese Datenquellen werden für Sie von verwaltet und automatisch aktualisiert AWS, wenn sich Vorschriften und Standards ändern und neue Datenquellen identifiziert werden. Wählen Sie ein beliebiges zentrales Steuerelement aus, um die zugrunde liegenden Datenquellen zu sehen.

Datenquellen	Dies sind die anderen AWS verwalteten Datenquellen, die Beweise zur Unterstützung der Standardkontrolle sammeln.
	• Zuordnung — Das spezifische Schlüsselwort, das zum Sammeln von Beweisen verwendet wird.
	  • Wenn der Typ ist AWS Config, handelt es sich bei der Zuordnung um eine AWS Config Regel (z. B.`SNS_ENCRYPTED_KMS`).
	  • Wenn der Typ ist AWS Security Hub CSPM, handelt es sich bei der Zuordnung um ein Security Hub CSPM-Steuerelement (z. B.`EC2.1`).
	  • Handelt es sich bei dem Typ um AWS API-Aufrufe, handelt es sich bei der Zuordnung um einen API-Aufruf (z. B.`kms_ListKeys`).
	  • Wenn es sich um einen Typ handelt AWS CloudTrail, handelt es sich bei der Zuordnung um ein CloudTrail Ereignis (z. B.`CreateAccessKey`).
	• Typ — Der Typ der Datenquelle, aus der die Beweise stammen.
	  • Wenn Audit Manager die Beweise sammelt, kann es sich bei dem Typ um AWS Security Hub CSPMAWS Config, AWS CloudTrail, oder AWS API-Aufrufe handeln.

Name	Description
	• Wenn Sie Ihre eigenen Nachweise hochladen, ist der Typ Manuell. Eine Beschreibung gibt an, ob es sich bei den erforderlichen manuellen Beweisen um einen Datei-Upl oad oder eine Textantwort handelt. • Häufigkeit — Wie oft Audit Manager Beweise für eine AWS API-Aufruf-Datenquelle sammelt.

Registerkarte Details

Diese Registerkarte enthält die folgenden Informationen:

Name	Description
Anweisungen	Die Anweisungen, die beschreiben, wie die Steuerung getestet und behoben werden kann.
Informationen zum Testen	Die empfohlenen Testverfahren.
Aktionsplan	Die empfohlenen Maßnahmen, die Sie ergreifen sollten, wenn Sie die Kontrolle korrigieren müssen.
Tags	Die Tags, die dem Steuerelement zugeordnet sind.
Key (Schlüssel)	Der Tag-Schlüssel (z. B. ein Konformitätsstandard, eine Vorschrift oder eine Kategorie).
Wert	Der Tag-Wert.

AWS CLI

Um Standardkontrolldetails anzuzeigen, finden Sie im AWS CLI

1. Folgen Sie den Schritten, um ein Steuerelement zu finden. Stellen Sie sicher, dass Sie das `--control-type` als festlegen`Standard`, und wenden Sie bei Bedarf alle optionalen Filter an.

```
aws auditmanager list-controls --control-type Standard
```

2. Identifizieren Sie in der Antwort die Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den Amazon-Ressourcennamen (ARN).
3. Führen Sie den Befehl get-control aus und geben Sie den `--control-id` an. Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Die Kontrolldetails werden im JSON-Format zurückgegeben. Zum besseren Verständnis dieser Daten finden Sie in der AWS CLI Befehlsreferenz unter get-control Output

4. Um die Tag-Details zu sehen, führen Sie den list-tags-for-resourceBefehl aus und geben Sie den `--resource-arn` an. Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Um Standardkontrolldetails mithilfe der API anzuzeigen

1. Folgen Sie den Schritten, um ein Steuerelement zu finden. Stellen Sie sicher, dass der ControlType auf eingestellt ist`Standard`, und wenden Sie bei Bedarf alle optionalen Filter an.
2. Identifizieren Sie in der Antwort die Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den Amazon-Ressourcennamen (ARN).
3. Verwenden Sie den GetControlVorgang und geben Sie die Kontroll-ID an, die Sie sich in Schritt 2 notiert haben.

> **Tip**
>
> Die Kontrolldetails werden im JSON-Format zurückgegeben. Informationen zum besseren Verständnis dieser Daten finden Sie unter GetControl Antwortelemente in der AWS Audit Manager API-Referenz.

4. Um Tag-Details anzuzeigen, verwenden Sie den ListTagsForResourceVorgang und geben Sie den resourceArn, den Sie in Schritt 2 notiert haben.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, indem Sie auf einen der Links in diesem Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Sie können jedem Ihrer benutzerdefinierten Frameworks ein Standardsteuerelement hinzufügen. Detaillierte Anweisungen finden Sie unter Erstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager.

Sie können auch jedes Standardsteuerelement so anpassen, dass es Ihren Anforderungen entspricht. Detaillierte Anweisungen finden Sie unter Eine bearbeitbare Kopie einer Kontrolle erstellen in AWS Audit Manager.

Weitere Ressourcen

- Überprüfung eines gemeinsamen Steuerelements
- Überprüfung einer zentralen Kontrolle
- Überprüfung eines benutzerdefinierten Steuerelements

Überprüfung eines benutzerdefinierten Steuerelements

Sie können die Details eines benutzerdefinierten Steuerelements mithilfe der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) überprüfen.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Anzeigen von Steuerelementen verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können die Details eines benutzerdefinierten Steuerelements mithilfe der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) überprüfen.

Audit Manager console

So zeigen Sie benutzerdefinierte Kontrolldetails in der Audit Manager Manager-Konsole an

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie Benutzerdefiniert, um die von Ihnen erstellten benutzerdefinierten Steuerelemente anzuzeigen.
4. Wählen Sie einen beliebigen Namen für ein benutzerdefiniertes Steuerelement, um die Details für dieses Steuerelement anzuzeigen.
5. Überprüfen Sie die Details des benutzerdefinierten Steuerelements anhand der folgenden Informationen als Referenz.

Abschnitt „Überblick“

In diesem Abschnitt wird das benutzerdefinierte Steuerelement beschrieben und die Datenquellentypen aufgeführt, die es zum Sammeln von Nachweisen verwendet. Er enthält auch Informationen darüber, wann das Steuerelement erstellt und zuletzt aktualisiert wurde.

Registerkarte „Beweisquellen“

Auf dieser Registerkarte wird angezeigt, woher das benutzerdefinierte Steuerelement Beweise sammelt. Dazu gehören folgende Informationen:

Name	Description
Allgemeine Steuerelemente	Dies sind die üblichen Kontrollen, mit denen Beweise gesammelt werden, um die benutzerdefinierte Kontrolle zu unterstützen. Mithilfe von Common Controls werden Beweise mithilfe von zugrunde liegenden Datenquellen gesammelt, die für Sie AWS verwaltet werden. Für jede aufgelistete gemeinsame Kontrolle sammelt Audit Manager die relevanten Nachweise für alle unterstützenden Kernkontrollen. Wählen Sie eine gemeinsame Kontrolle aus, um die zugehörigen Kernkontrollen zu sehen.
Zentrale Steuerelemente	Dies sind die wichtigsten Kontrollen, mit denen Beweise gesammelt werden, um die benutzerdefinierte Kontrolle zu unterstützen. Core Controls sammelt Beweise mithilfe einer vordefinierten Gruppe von Datenquellen, die für Sie AWS verwaltet werden. Wählen Sie ein zentrales Steuerelement aus, um die zugrunde liegenden Datenquellen zu sehen.
Datenquellen	Dies sind die Datenquellen, die Beweise zur Unterstützung des benutzerdefinierten Steuerelements sammeln. **Note** Diese Datenquellen werden nicht für Sie verwaltet von AWS. Sie sind für deren Pflege verantwortlich. • Name — Der Name der Datenquelle. • Typ — Der Typ der Datenquelle, aus der die Beweise stammen. • Wenn Audit Manager die Beweise sammelt, kann es sich bei dem Typ um AWS Security Hub CSPMAWS Config, AWS CloudTrail, oder AWS API-Aufrufe handeln.

Name	Description

	• Wenn Sie Ihre eigenen Nachweise hochladen, ist der Typ Manuell. Eine Beschreibung gibt an, ob es sich bei den erforderlichen manuellen Beweisen um einen Datei-Upl oad oder eine Textantwort handelt.
	• Zuordnung — Das spezifische Schlüsselwort, das zum Sammeln von Beweisen verwendet wird.
	  • Wenn der Typ ist AWS Config, handelt es sich bei der Zuordnung um eine AWS Config Regel (z. B.`SNS_ENCRY PTED_KMS`).
	  • Wenn der Typ ist AWS Security Hub CSPM, handelt es sich bei der Zuordnung um ein Security Hub CSPM-Steu erelement (z. B.`EC2.1`).
	  • Handelt es sich bei dem Typ um AWS API-Aufrufe, handelt es sich bei der Zuordnung um einen API-Aufruf (z. B.`kms_ListKeys`).
	  • Wenn es sich um einen Typ handelt AWS CloudTrail, handelt es sich bei der Zuordnung um ein CloudTrail Ereignis (z. B.`CreateAccessKey`).
	• Häufigkeit — Wie oft Audit Manager Beweise für eine AWS API-Aufruf-Datenquelle sammelt.

Registerkarte Details

Diese Registerkarte enthält die folgenden Informationen:

Name	Description
Anweisungen	Die Anweisungen, die beschreiben, wie die Steuerung getestet und behoben werden kann.
Informationen zum Testen	Die empfohlenen Testverfahren.

Name	Description
Aktionsplan	Die empfohlenen Maßnahmen, die Sie ergreifen sollten, wenn Sie die Kontrolle korrigieren müssen.
Tags	Die Tags, die dem Steuerelement zugeordnet sind.
Key (Schlüssel)	Der Tag-Schlüssel (z. B. ein Konformitätsstandard, eine Vorschrift oder eine Kategorie).
Wert	Der Tag-Wert.

AWS CLI

Um die Details der benutzerdefinierten Steuerung anzuzeigen, finden Sie im AWS CLI

1. Folgen Sie den Schritten, um ein Steuerelement zu finden. Stellen Sie sicher, dass Sie das `--control-type` als festlegen`Custom`, und wenden Sie bei Bedarf alle optionalen Filter an.

```
aws auditmanager list-controls --control-type Custom
```

2. Identifizieren Sie in der Antwort die Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den Amazon-Ressourcennamen (ARN).
3. Führen Sie den Befehl get-control aus und geben Sie den `--control-id` an. Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Die Kontrolldetails werden im JSON-Format zurückgegeben. Informationen zum besseren Verständnis dieser Daten finden Sie in der AWS CLI Befehlsreferenz unter get-control Output.

4. Um die Tags für ein Steuerelement anzuzeigen, verwenden Sie den list-tags-for-resourceBefehl und geben Sie den `--resource-arn` an. Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

So zeigen Sie Details zu benutzerdefinierten Steuerelementen mithilfe der API an

1. Folgen Sie den Schritten, um ein Steuerelement zu finden. Stellen Sie sicher, dass der ControlType auf eingestellt ist`Custom`, und wenden Sie bei Bedarf alle optionalen Filter an.
2. Identifizieren Sie in der Antwort das Steuerelement, das Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den zugehörigen Amazon-Ressourcennamen (ARN).
3. Verwenden Sie den GetControlVorgang und geben Sie die Kontroll-ID an, die Sie sich in Schritt 2 notiert haben.

   > **Tip**
   >
   > Die Kontrolldetails werden im JSON-Format zurückgegeben. Informationen zum besseren Verständnis dieser Daten finden Sie unter GetControl Antwortelemente in der AWS Audit Manager API-Referenz.

4. Um Tags für das Steuerelement anzuzeigen, verwenden Sie den ListTagsForResourceVorgang und geben Sie das Steuerelement resourceArn an, das Sie in Schritt 2 notiert haben.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, indem Sie auf einen der Links in diesem Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Sie können jedem Ihrer benutzerdefinierten Frameworks ein benutzerdefiniertes Steuerelement hinzufügen. Detaillierte Anweisungen finden Sie unter Erstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager.

Sie können auch ein benutzerdefiniertes Steuerelement bearbeiten, eine bearbeitbare Kopie eines benutzerdefinierten Steuerelements erstellen oder ein benutzerdefiniertes Steuerelement löschen, das Sie nicht mehr benötigen.

Weitere Ressourcen

- Ein allgemeines Steuerelement überprüfen
- Überprüfung einer zentralen Kontrolle
- Überprüfung einer Standardkontrolle

Erstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager

Sie können benutzerdefinierte Kontrollen verwenden, um Nachweise für Ihre spezifischen Compliance-Anforderungen zu sammeln.

Genau wie Standardkontrollen erfassen benutzerdefinierte Kontrollen kontinuierlich Beweise, wenn sie in Ihren Bewertungen aktiv sind. Sie können jeder benutzerdefinierten Kontrolle, die Sie erstellen, auch manuelle Beweise hinzufügen. Jeder Beweis wird zu einem Datensatz, anhand dessen Sie die Einhaltung der Anforderungen Ihrer benutzerdefinierten Kontrolle nachweisen können.

Hier sehen Sie einige Beispiele für die Verwendung von benutzerdefinierten Kontrollen:

Ordnen Sie Ihre Unternehmenskontrollen vordefinierten Gruppierungen von AWS Datenquellen zu

> Sie können Ihre Unternehmenskontrollen in Audit Manager integrieren, indem Sie allgemeine Kontrollen als Beweisquelle verwenden. Wählen Sie die allgemeinen Kontrollen aus, die Ihren Zielen entsprechen, und verwenden Sie sie als Bausteine, um ein Kontrollsystem zu erstellen, das Belege für Ihr gesamtes Portfolio an Compliance-Anforderungen sammelt. Jedes automatisierte gemeinsame Steuerelement ist einer vordefinierten Gruppierung von Datenquellen zugeordnet. Das bedeutet, dass Sie kein AWS Experte sein müssen, um zu wissen, welche Datenquellen die relevanten Beweise für Ihre Ziele sammeln. Und wenn Sie Common Controls als Beweisquelle verwenden, müssen Sie keine Datenquellenzuordnungen mehr verwalten, da Audit Manager das für Sie erledigt.

Erstellen Sie eine Frage zur Risikobewertung eines Anbieters

Sie können benutzerdefinierte Kontrollen verwenden, um Sie bei der Verwaltung von Lieferantenrisikobewertungen zu unterstützen. Jede Kontrolle, die Sie erstellen, kann eine individuelle Frage zur Risikobewertung darstellen. Der Name des Steuerelements kann beispielsweise eine Frage sein, und Sie können eine Antwort geben, indem Sie eine Datei hochladen oder eine Textantwort als manuellen Nachweis eingeben.

Wichtige Punkte

Wenn es darum geht, benutzerdefinierte Steuerelemente in Audit Manager zu erstellen, stehen Ihnen zwei Methoden zur Auswahl:

1. Ein Steuerelement von Grund auf neu erstellen — Diese Methode bietet maximale Flexibilität und ermöglicht es Ihnen, das Steuerelement genau auf Ihre Bedürfnisse zuzuschneiden. Dies ist eine gute Option, wenn Sie eine bestimmte Konformitätsanforderung haben, die durch eine bestehende Kontrolle nicht ausreichend abgedeckt wird. Diese Methode ist besonders nützlich, wenn Sie die Unternehmenskontrollen Ihres Unternehmens vordefinierten Gruppierungen von AWS Datenquellen zuordnen müssen oder wenn Sie Fragen zur Lieferantenrisikobewertung als individuelle Kontrollen erstellen möchten.
2. Eine bearbeitbare Kopie eines vorhandenen Steuerelements erstellen — Wenn ein vorhandenes Standardsteuerelement oder ein benutzerdefiniertes Steuerelement Ihren Anforderungen teilweise entspricht, können Sie eine bearbeitbare Kopie dieses Steuerelements erstellen. Dieser Ansatz ist effizienter, wenn Sie nur geringfügige Änderungen an einem vorhandenen Steuerelement vornehmen müssen. Dies ist eine gute Option, wenn Sie einige Attribute anpassen möchten, um das Steuerelement besser an Ihre spezifischen Anforderungen anzupassen. Sie können beispielsweise ändern, wie oft ein Steuerelement einen API-Aufruf zum Sammeln von Beweisen verwendet, und dann den Namen des Steuerelements ändern, um dies widerzuspiegeln.

Weitere Ressourcen

Anweisungen zum Erstellen eines benutzerdefinierten Steuerelements finden Sie in den folgenden Ressourcen.

- Ein benutzerdefiniertes Steuerelement von Grund auf neu erstellen in AWS Audit Manager
- Eine bearbeitbare Kopie einer Kontrolle erstellen in AWS Audit Manager

Ein benutzerdefiniertes Steuerelement von Grund auf neu erstellen in AWS Audit Manager

Wenn die Compliance-Anforderungen Ihres Unternehmens nicht mit den vordefinierten Standardkontrollen übereinstimmen, die in verfügbar sind AWS Audit Manager, können Sie Ihre eigene benutzerdefinierte Steuerung von Grund auf neu erstellen.

Auf dieser Seite werden die Schritte zum Erstellen eines benutzerdefinierten Steuerelements beschrieben, das auf Ihre spezifischen Bedürfnisse zugeschnitten ist.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen verfügt, um ein benutzerdefiniertes Steuerelement in AWS Audit Manager zu erstellen. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Gehen Sie wie folgt vor, um erfolgreich Beweise von AWS Config und Security Hub CSPM zu sammeln:

- Aktivieren AWS Config und dann die erforderlichen Einstellungen für die Verwendung AWS Config mit Audit Manager anwenden
- Aktivieren Sie Security Hub CSPM und wenden Sie dann die erforderlichen Einstellungen für die Verwendung von Security Hub CSPM mit Audit Manager an

Audit Manager kann dann jedes Mal, wenn eine Bewertung für eine bestimmte AWS Config Regel oder Security Hub CSPM-Kontrolle stattfindet, Beweise sammeln.

Verfahren

Aufgaben

- Schritt 1: Geben Sie die Kontrolldetails an
- Schritt 2: Geben Sie die Quellen der Beweise an
- Schritt 3 (optional): Definieren Sie einen Aktionsplan
- Schritt 4: Überprüfen und Erstellen der Kontrolle

Schritt 1: Geben Sie die Kontrolldetails an

Geben Sie zunächst die Details Ihrer benutzerdefinierten Kontrolle an.

> **Important**
>
> Wir empfehlen dringend, vertrauliche Daten niemals in frei formatierte Felder wie Kontrolldetails oder Testinformationen einzugeben. Wenn Sie benutzerdefinierte Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

Um Kontrolldetails anzugeben

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich Kontrollbibliothek und anschließend Benutzerdefinierte Kontrolle erstellen aus.
3. Geben Sie unter Kontrolldetails die folgenden Informationen über die Kontrolle ein.
   - Kontrolle – Geben Sie einen benutzerfreundlichen Namen, einen Titel oder eine Frage zur Risikobewertung ein. Dieser Wert hilft Ihnen dabei, Ihre Kontrolle in der Kontrollbibliothek zu identifizieren.
   - Beschreibung (optional) – Geben Sie Details ein, damit andere das Ziel der Kontrolle besser verstehen. Diese Beschreibung wird auf der Seite mit den Kontrolldetails angezeigt.
4. Geben Sie unter Testinformationen die empfohlenen Schritte zum Testen der Kontrolle ein.
5. Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um der Kontrolle ein Tag zuzuordnen. Sie können für jedes Tag einen Schlüssel angeben, der das von dieser Kontrolle unterstützte Compliance-Framework am besten beschreibt. Der Tagschlüssel ist obligatorisch und kann als Suchkriterium verwendet werden, wenn Sie in der Kontrollbibliothek nach dieser Kontrolle suchen.
6. Wählen Sie Weiter aus.

Schritt 2: Geben Sie die Quellen der Beweise an

Geben Sie als Nächstes einige Beweisquellen an. Eine Beweisquelle bestimmt, woher Ihr benutzerdefiniertes Steuerelement Beweise sammelt. Sie können AWS verwaltete Quellen, vom Kunden verwaltete Quellen oder beides verwenden.

> **Tip**
>
> Wir empfehlen, AWS verwaltete Quellen zu verwenden. Immer wenn eine AWS verwaltete Quelle aktualisiert wird, werden dieselben Updates automatisch auf alle benutzerdefinierten Steuerelemente angewendet, die diese Quellen verwenden. Das bedeutet, dass Ihre benutzerdefinierten Kontrollen Beweise anhand der neuesten Definitionen dieser Beweisquelle sammeln.

Wenn Sie sich nicht sicher sind, welche Optionen Sie wählen sollen, sehen Sie sich die folgenden Beispiele und unsere Empfehlungen an.

Ihre Rolle	Ihr Ziel	Empfohlene Beweisquelle
GRC-Profi	Ich möchte Beweise für einen bestimmten Bereich oder ein bestimmtes Ziel sammeln	AWS verwaltet (common control) Verwenden Sie eine vordefinierte Gruppierung von Datenquellen, die einem bestimmten gemeinsamen Steuerelement zugeordnet sind.
Technischer Experte	Ich möchte Beweise über die AWS Ressourcen sammeln, für die ich verantwortlich bin	AWS verwaltet (core control) Verwenden Sie eine vordefinierte Gruppierung von Datenquellen, die einer AWS Anforderung zugeordnet sind.
Technischer Experte	Ich möchte eine benutzerdefinierte AWS Config Regel	Vom Kunden verwaltet (automatisiertdata source)

Ihre Rolle	Ihr Ziel	Empfohlene Beweisquelle
	verwenden, um Beweise zu sammeln	Verwenden Sie eine benutzerdefinierte Datenquelle, um bestimmte automatisierte Beweise zu sammeln.
GRC-Profi	Ich möchte Beweise wie Dokumente und Textantworten sammeln	Vom Kunden verwaltet (manuelldata source) Verwenden Sie eine benutzerdefinierte Datenquelle, um Ihre eigenen manuellen Nachweise hochzuladen.

Um eine AWS verwaltete Quelle anzugeben (empfohlen)

Wir empfehlen, dass Sie zunächst eine oder mehrere gängige Steuerelemente auswählen. Wenn Sie sich für die gemeinsame Kontrolle entscheiden, die Ihrem Ziel entspricht, sammelt Audit Manager die relevanten Nachweise für alle unterstützenden Kernkontrollen. Sie können auch einzelne Kernkontrollen auswählen, wenn Sie gezielte Nachweise über Ihre AWS Umgebung sammeln möchten.

Um eine AWS verwaltete Quelle anzugeben

1. Gehen Sie zum Abschnitt „AWS Verwaltete Quellen“ der Seite.
2. Gehen Sie wie folgt vor, um ein gemeinsames Steuerelement hinzuzufügen:
    a. Wählen Sie Verwenden Sie eine gemeinsame Kontrolle, die Ihrem Compliance-Ziel entspricht.
    b. Wählen Sie ein allgemeines Steuerelement aus der Dropdownliste aus.
    c. (Optional) Wiederholen Sie Schritt 2 nach Bedarf. Sie können bis zu fünf allgemeine Steuerelemente hinzufügen.
3. Um ein gemeinsames Steuerelement zu entfernen, wählen Sie das X neben dem Namen des Steuerelements aus.
4. Gehen Sie wie folgt vor, um ein zentrales Steuerelement hinzuzufügen:

a. Wählen Sie „Eine zentrale Kontrolle verwenden, die einer vorgeschriebenen Richtlinie entspricht“ AWS aus.

b. Wählen Sie ein allgemeines Steuerelement aus der Dropdownliste aus.

c. (Optional) Wiederholen Sie Schritt 4 nach Bedarf. Sie können bis zu 50 Kernsteuerungen hinzufügen.

5. Um ein zentrales Steuerelement zu entfernen, wählen Sie das X neben dem Namen des Steuerelements aus.
6. Gehen Sie wie folgt vor, um vom Kunden verwaltete Datenquellen hinzuzufügen. Klicken Sie andernfalls auf Next (Weiter).

Um eine vom Kunden verwaltete Quelle anzugeben

Um automatisierte Beweise aus einer Datenquelle zu sammeln, müssen Sie einen Datenquellentyp und eine Datenquellenzuordnung auswählen. Diese Angaben entsprechen Ihrer AWS Nutzung und teilen Audit Manager mit, wo die Beweise gesammelt werden sollen. Wenn Sie Ihre eigenen Nachweise vorlegen möchten, wählen Sie stattdessen eine manuelle Datenquelle.

> **Note**
>
> Sie sind dafür verantwortlich, die Datenquellenzuordnungen zu verwalten, die Sie in diesem Schritt erstellen.

Um eine vom Kunden verwaltete Quelle anzugeben

1. Gehen Sie auf der Seite zum Abschnitt Kundenverwaltete Quellen.
2. Wählen Sie Eine Datenquelle verwenden, um manuelle oder automatisierte Beweise zu sammeln aus.
3. Wählen Sie Hinzufügen aus.
4. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie AWS API-Aufrufe und anschließend einen API-Aufruf und die Häufigkeit der Beweiserhebung aus.
   - Wählen Sie „AWS CloudTrail Ereignis“ und anschließend einen Namen für das Ereignis.
   - Wählen Sie „AWS Config Verwaltete Regel“ und anschließend eine Regel-ID aus.

- Wählen Sie eine AWS Config benutzerdefinierte Regel und anschließend eine Regel-ID aus.
- Wählen Sie AWS Security Hub CSPM Steuerung und anschließend ein Security Hub CSPM-Steuerelement aus.
- Wählen Sie Manuelle Datenquelle und anschließend eine Option aus:
  - Datei-Upload — Verwenden Sie diese Option, wenn für die Kontrolle Unterlagen als Nachweis erforderlich sind.
  - Textantwort — Verwenden Sie diese Option, wenn die Kontrolle eine Antwort auf eine Frage zur Risikobewertung benötigt.

> **Tip**
>
> Informationen zu automatisierten Datenquellentypen und Tipps zur Problembehandlung finden Sie unterUnterstützte Datenquellentypen für automatisierte Beweise.
> Wenn Sie Ihre Datenquelleneinrichtung mit einem Experten überprüfen müssen, wählen Sie vorerst Manuelle Datenquelle. Auf diese Weise können Sie die Kontrolle jetzt erstellen und zu einem Framework hinzufügen und die Kontrolle dann später nach Bedarf bearbeiten.

5. Geben Sie unter Datenquellenname einen beschreibenden Namen ein.
6. (Optional) Geben Sie unter Zusätzliche Details eine Beschreibung der Datenquelle und eine Beschreibung der Fehlerbehebung ein.
7. Wählen Sie Datenquelle hinzufügen aus.
8. (Optional) Um eine weitere Datenquelle hinzuzufügen, wählen Sie Hinzufügen aus und wiederholen Sie die Schritte 1—7. Sie können bis zu 100 Datenquellen hinzufügen.
9. Um eine Datenquelle zu entfernen, wählen Sie die Datenquelle aus der Tabelle aus und klicken Sie dann auf Entfernen.
10. Wählen Sie Weiter aus, sobald Sie fertig sind.

Schritt 3 (optional): Definieren Sie einen Aktionsplan

Geben Sie als Nächstes die Maßnahmen an, die ergriffen werden sollen, wenn diese Kontrolle behoben werden muss.

> **Important**
>
> Wir empfehlen dringend, niemals vertrauliche Informationen zur Identifizierung in Freiformfelder wie den Aktionsplan einzugeben. Wenn Sie benutzerdefinierte Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

Um einen Aktionsplan zu definieren

1. Geben Sie unter Titel einen aussagekräftigen Titel für den Aktionsplan ein.
2. Geben Sie unter Anweisungen detaillierte Anweisungen für den Aktionsplan ein.
3. Wählen Sie Weiter aus.

Schritt 4: Überprüfen und Erstellen der Kontrolle

Überprüfen Sie die Informationen für die Kontrolle. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten.

Wenn Sie fertig sind, wählen Sie Erstellen aus.

Nächste Schritte

Nachdem Sie eine neue benutzerdefinierte Kontrolle erstellt haben, können Sie es einem benutzerdefinierten Framework hinzufügen. Weitere Informationen hierzu finden Sie unter Erstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager oder Bearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager.

Nachdem Sie das benutzerdefinierte Steuerelement zu einem benutzerdefinierten Framework hinzugefügt haben, können Sie eine Bewertung erstellen und mit der Erfassung von Nachweisen beginnen. Weitere Informationen hierzu finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Informationen dazu, wie Sie Ihr benutzerdefiniertes Steuerelement zu einem späteren Zeitpunkt erneut aufrufen können, finden Sie unterFinden Sie die verfügbaren Steuerelemente in AWS Audit Manager. Gehen Sie wie folgt vor, um Ihr benutzerdefiniertes Steuerelement zu finden, sodass Sie es anzeigen, bearbeiten oder löschen können.

Weitere Ressourcen

Lösungen zur Kontrolle von Problemen in Audit Manager finden Sie unterBehebung von Problemen mit Kontrollen und Kontrollsätzen.

Eine bearbeitbare Kopie einer Kontrolle erstellen in AWS Audit Manager

Anstatt ein benutzerdefiniertes Steuerelement von Grund auf neu zu erstellen, können Sie ein vorhandenes Standardsteuerelement oder ein benutzerdefiniertes Steuerelement als Ausgangspunkt verwenden und eine bearbeitbare Kopie erstellen, die Ihren Anforderungen entspricht. Wenn Sie dies tun, verbleibt das vorhandene Standardsteuerelement in der Steuerelementbibliothek, und es wird ein neues Steuerelement mit Ihren benutzerdefinierten Einstellungen erstellt.

Voraussetzungen

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Erstellen eines benutzerdefinierten Frameworks verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Gehen Sie wie folgt vor, um erfolgreich Beweise von AWS Config und Security Hub CSPM zu sammeln:

- Aktivieren Sie AWS Config und wenden Sie dann die erforderlichen Einstellungen für die Verwendung AWS Config mit Audit Manager an.
- Aktivieren Sie Security Hub CSPM und wenden Sie dann die erforderlichen Einstellungen für die Verwendung von Security Hub CSPM mit Audit Manager an.

Audit Manager kann dann jedes Mal, wenn eine Bewertung für eine bestimmte AWS Config Regel oder Security Hub CSPM-Kontrolle stattfindet, Beweise sammeln.

Verfahren

Aufgaben

- Schritt 1: Geben Sie die Kontrolldetails an
- Schritt 2: Geben Sie die Quellen der Beweise an
- Schritt 3 (optional): Definieren Sie einen Aktionsplan

- Schritt 4: Überprüfen und Erstellen der Kontrolle

Schritt 1: Geben Sie die Kontrolldetails an

Die Kontrolldetails werden von der ursprünglichen Kontrolle übernommen. Überprüfen und ändern dieser Details nach Bedarf.

> **Important**
>
> Wir empfehlen dringend, vertrauliche Daten niemals in frei formatierte Felder wie Kontrolldetails oder Testinformationen einzugeben. Wenn Sie benutzerdefinierte Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

Um Kontrolldetails anzugeben

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie das Standardsteuerelement oder das benutzerdefinierte Steuerelement aus, an dem Sie Änderungen vornehmen möchten, und wählen Sie dann Kopie erstellen aus.
4. Geben Sie den neuen Namen des Steuerelements an und wählen Sie Weiter.
5. Passen Sie unter Kontrolldetails die Kontrolldetails nach Bedarf an.
6. Nehmen Sie unter Testinformationen nach Bedarf Änderungen an den Anweisungen vor.
7. Passen Sie unter Tags die Tags nach Bedarf an.
8. Wählen Sie Weiter aus.

Schritt 2: Geben Sie die Quellen der Beweise an

Beweisquellen werden von der ursprünglichen Kontrolle übernommen. Sie können Beweisquellen nach Bedarf ändern, hinzufügen oder entfernen.

Um eine AWS verwaltete Quelle anzugeben (empfohlen)

> **Tip**
>
> Wir empfehlen, dass Sie zunächst eine oder mehrere gängige Steuerelemente auswählen. Wenn Sie detailliertere Compliance-Anforderungen haben, können Sie auch eine oder mehrere spezifische Kernkontrollen auswählen.

Um eine verwaltete Quelle AWS anzugeben

1. Überprüfen Sie unter AWS Verwaltete Quellen die aktuelle Auswahl und nehmen Sie bei Bedarf Änderungen vor.
2. Gehen Sie wie folgt vor, um ein gemeinsames Steuerelement hinzuzufügen:
   a. Wählen Sie Verwenden Sie eine gemeinsame Kontrolle, die Ihrem Compliance-Ziel entspricht.
   b. Wählen Sie ein allgemeines Steuerelement aus der Dropdownliste aus.
   c. (Optional) Wiederholen Sie Schritt 2 nach Bedarf. Sie können bis zu fünf allgemeine Steuerelemente hinzufügen.
3. Um ein gemeinsames Steuerelement zu entfernen, wählen Sie das X neben dem Namen des Steuerelements aus.
4. Gehen Sie wie folgt vor, um ein zentrales Steuerelement hinzuzufügen:
   a. Wählen Sie „Eine zentrale Kontrolle verwenden, die einer vorgeschriebenen Richtlinie entspricht“ AWS aus.
   b. Wählen Sie ein allgemeines Steuerelement aus der Dropdownliste aus.
   c. (Optional) Wiederholen Sie Schritt 4 nach Bedarf. Sie können bis zu 50 Kernsteuerungen hinzufügen.
5. Um ein zentrales Steuerelement zu entfernen, wählen Sie das X neben dem Namen des Steuerelements aus.
6. Gehen Sie wie folgt vor, um vom Kunden verwaltete Datenquellen zu bearbeiten. Klicken Sie andernfalls auf Next (Weiter).

Um eine vom Kunden verwaltete Quelle anzugeben

Um automatisierte Beweise aus einer Datenquelle zu sammeln, müssen Sie einen Datenquellentyp und eine Datenquellenzuordnung auswählen. Diese Angaben entsprechen Ihrer AWS Nutzung und teilen Audit Manager mit, wo die Beweise gesammelt werden sollen. Wenn Sie Ihre eigenen Nachweise vorlegen möchten, wählen Sie stattdessen eine manuelle Datenquelle.

> **Note**
>
> Sie sind dafür verantwortlich, die Datenquellenzuordnungen zu verwalten, die Sie in diesem Schritt erstellen.

Um eine vom Kunden verwaltete Quelle anzugeben

1. Überprüfen Sie unter Vom Kunden verwaltete Quellen die aktuellen Datenquellen und nehmen Sie bei Bedarf Änderungen vor.
2. Um eine Datenquelle zu entfernen, wählen Sie eine Datenquelle aus der Tabelle aus und klicken Sie auf Entfernen.
3. Gehen Sie folgendermaßen vor, um eine neue Datenquelle hinzuzufügen:

    a. Wählen Sie Eine Datenquelle verwenden, um manuelle oder automatisierte Beweise zu sammeln aus.
    b. Wählen Sie Hinzufügen aus.
    c. Wählen Sie eine der folgenden Optionen:

        - Wählen Sie AWS API-Aufrufe und anschließend einen API-Aufruf und die Häufigkeit der Beweiserhebung aus.
        - Wählen Sie „AWS CloudTrail Ereignis“ und anschließend einen Namen für das Ereignis.
        - Wählen Sie „AWS Config Verwaltete Regel“ und anschließend eine Regel-ID aus.
        - Wählen Sie eine AWS Config benutzerdefinierte Regel und anschließend eine Regel-ID aus.
        - Wählen Sie AWS Security Hub CSPM Steuerung und anschließend ein Security Hub CSPM-Steuerelement aus.
        - Wählen Sie Manuelle Datenquelle und anschließend eine Option aus:
            - Datei-Upload — Verwenden Sie diese Option, wenn für die Kontrolle Unterlagen als Nachweis erforderlich sind.

- Textantwort — Verwenden Sie diese Option, wenn die Kontrolle eine Antwort auf eine Frage zur Risikobewertung benötigt.

> **Tip**
>
> Informationen zu automatisierten Datenquellentypen und Tipps zur Problembehandlung finden Sie unterUnterstützte Datenquellentypen für automatisierte Beweise.
> Wenn Sie Ihre Datenquelleneinrichtung mit einem Experten überprüfen müssen, wählen Sie vorerst Manuelle Datenquelle. Auf diese Weise können Sie die Kontrolle jetzt erstellen und zu einem Framework hinzufügen und die Kontrolle dann später nach Bedarf bearbeiten.

d. Geben Sie unter Datenquellenname einen beschreibenden Namen ein.

e. (Optional) Geben Sie unter Zusätzliche Details eine Beschreibung der Datenquelle und eine Beschreibung der Fehlerbehebung ein.

f. Wählen Sie Datenquelle hinzufügen aus.

g. (Optional) Um eine weitere Datenquelle hinzuzufügen, wählen Sie Hinzufügen aus und wiederholen Sie Schritt 3. Sie können bis zu 100 Datenquellen hinzufügen.

4. Wählen Sie Weiter aus, sobald Sie fertig sind.

Schritt 3 (optional): Definieren Sie einen Aktionsplan

Der Aktionsplan wird von der ursprünglichen Kontrolle übernommen. Sie können diesen Aktionsplan nach Bedarf bearbeiten.

> **Important**
>
> Wir empfehlen dringend, niemals vertrauliche Informationen zur Identifizierung in Freiformfelder wie den Aktionsplan einzugeben. Wenn Sie benutzerdefinierte Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

Um Anweisungen zu spezifizieren

1. Überprüfen Sie unter Titel den Titel und nehmen Sie bei Bedarf Änderungen vor.
2. Lesen Sie die Anweisungen unter Anweisungen und nehmen Sie bei Bedarf Änderungen vor.
3. Wählen Sie Weiter aus.

Schritt 4: Überprüfen und Erstellen der Kontrolle

Überprüfen Sie die Informationen für die Kontrolle. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten. Wenn Sie fertig sind, wählen Sie Erstellen aus.

Nächste Schritte

Nachdem Sie eine neue benutzerdefinierte Kontrolle erstellt haben, können Sie es einem benutzerdefinierten Framework hinzufügen. Weitere Informationen hierzu finden Sie unter Erstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager oder Bearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager.

Nachdem Sie einem benutzerdefinierten Framework ein benutzerdefiniertes Steuerelement hinzugefügt haben, können Sie eine Bewertung erstellen und mit der Erfassung von Nachweisen beginnen. Weitere Informationen hierzu finden Sie unter Erstellen Sie eine Bewertung in AWS Audit Manager.

Informationen dazu, wie Sie Ihr benutzerdefiniertes Steuerelement zu einem späteren Zeitpunkt erneut aufrufen können, finden Sie unterFinden Sie die verfügbaren Steuerelemente in AWS Audit Manager. Gehen Sie wie folgt vor, um Ihr benutzerdefiniertes Steuerelement zu finden, sodass Sie es anzeigen, bearbeiten oder löschen können.

Weitere Ressourcen

Lösungen zur Kontrolle von Problemen in Audit Manager finden Sie unterBehebung von Problemen mit Kontrollen und Kontrollsätzen.

Bearbeiten eines benutzerdefinierten Steuerelements in AWS Audit Manager

Möglicherweise müssen Sie Ihre benutzerdefinierten Steuerelemente ändern, wenn AWS Audit Manager sich Ihre Compliance-Anforderungen ändern.

Auf dieser Seite werden die Schritte zum Bearbeiten der Details, Nachweisquellen und Anweisungen zum Aktionsplan einer benutzerdefinierten Kontrolle beschrieben.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor ein benutzerdefiniertes Steuerelement erstellt haben.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen verfügt, um ein benutzerdefiniertes Steuerelement in AWS Audit Manager zu bearbeiten. Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Gehen Sie wie folgt vor, um ein benutzerdefiniertes Steuerelement zu bearbeiten.

> **Note**
>
> Wenn Sie ein Steuerelement bearbeiten, werden Ihre Änderungen auf alle Tests angewendet, bei denen das Steuerelement aktiv ist. Bei all diesen Bewertungen beginnt der Audit Manager automatisch mit der Erfassung von Nachweisen gemäß der neuesten Kontrolldefinition.

Aufgaben

- Schritt 1: Bearbeiten der Kontrolldetails
- Schritt 2: Bearbeiten Sie die Beweisquellen
- Schritt 3: Bearbeiten eines Aktionsplans

Schritt 1: Bearbeiten der Kontrolldetails

Überprüfen und bearbeiten Sie die Kontrolldetails nach Bedarf.

> **Important**
>
> Wir empfehlen dringend, niemals vertrauliche Identifikationsinformationen in Freiformfelder wie Kontrolldetails oder Testinformationen einzugeben. Wenn Sie benutzerdefinierte

Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

So bearbeiten Sie Kontrolldetails

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Control Library und dann die Registerkarte Benutzerdefiniert aus.
3. Wählen Sie die Kontrolle aus, die Sie bearbeiten möchten, und wählen Sie dann Bearbeiten.
4. Bearbeiten Sie unter Kontrolldetails die Kontrolldetails nach Bedarf.
5. Bearbeiten Sie unter Testinformationen die Beschreibung nach Bedarf.
6. Wählen Sie Weiter aus.

Schritt 2: Bearbeiten Sie die Beweisquellen

Als Nächstes können Sie Beweisquellen für die Kontrolle bearbeiten, entfernen oder hinzufügen.

Note

Wenn Sie eine Kontrolle bearbeiten, um mehr oder weniger Evidenzquellen einzubeziehen, kann sich dies darauf auswirken, wie viele Beweise Ihre Kontrolle in den Bewertungen sammelt, bei denen sie aktiv ist. Wenn Sie beispielsweise Beweisquellen hinzufügen, stellen Sie möglicherweise fest, dass Audit Manager mehr Ressourcenbewertungen durchführt und mehr Beweise sammelt als zuvor. Wenn Sie Beweisquellen entfernen, ist es wahrscheinlich, dass Ihre Kontrollgruppe in Zukunft weniger Beweise sammelt.
Weitere Informationen zu Ressourcenbewertungen und Preisen finden Sie unter AWS Audit Manager Preise.

Um eine AWS verwaltete Quelle zu bearbeiten

Um eine AWS verwaltete Quelle zu bearbeiten

1. Überprüfen Sie unter AWS Verwaltete Quellen die aktuelle Auswahl und nehmen Sie bei Bedarf Änderungen vor.

2. Gehen Sie wie folgt vor, um ein gemeinsames Steuerelement hinzuzufügen:

   a. Wählen Sie Verwenden Sie eine gemeinsame Kontrolle, die Ihrem Compliance-Ziel entspricht.
   b. Wählen Sie ein allgemeines Steuerelement aus der Dropdownliste aus.
   c. (Optional) Wiederholen Sie Schritt 2 nach Bedarf. Sie können bis zu fünf allgemeine Steuerelemente hinzufügen.
3. Um ein gemeinsames Steuerelement zu entfernen, wählen Sie das X neben dem Namen des Steuerelements aus.
4. Gehen Sie wie folgt vor, um ein zentrales Steuerelement hinzuzufügen:

   a. Wählen Sie „Eine zentrale Kontrolle verwenden, die einer vorgeschriebenen Richtlinie entspricht“ AWS aus.
   b. Wählen Sie ein allgemeines Steuerelement aus der Dropdownliste aus.
   c. (Optional) Wiederholen Sie Schritt 4 nach Bedarf. Sie können bis zu 50 Kernsteuerungen hinzufügen.
5. Um ein zentrales Steuerelement zu entfernen, wählen Sie das X neben dem Namen des Steuerelements aus.
6. Gehen Sie wie folgt vor, um vom Kunden verwaltete Datenquellen hinzuzufügen. Klicken Sie andernfalls auf Next (Weiter).

Um eine vom Kunden verwaltete Quelle zu bearbeiten

> **Note**
>
> Sie sind dafür verantwortlich, die Datenquellenzuordnungen zu verwalten, die Sie in diesem Schritt bearbeiten.

Um eine vom Kunden verwaltete Quelle zu bearbeiten

1. Überprüfen Sie unter Vom Kunden verwaltete Quellen die aktuellen Datenquellen und nehmen Sie bei Bedarf Änderungen vor.
2. Um eine Datenquelle zu entfernen, wählen Sie eine Datenquelle aus der Tabelle aus und klicken Sie dann auf Entfernen.
3. Gehen Sie folgendermaßen vor, um eine neue Datenquelle hinzuzufügen:

a. Wählen Sie Eine Datenquelle verwenden, um manuelle oder automatisierte Beweise zu sammeln aus.

b. Wählen Sie Hinzufügen aus.

c. Wählen Sie eine der folgenden Optionen:

- Wählen Sie AWS API-Aufrufe und anschließend einen API-Aufruf und die Häufigkeit der Beweiserhebung aus.
- Wählen Sie „AWS CloudTrail Ereignis“ und anschließend einen Namen für das Ereignis.
- Wählen Sie „AWS Config Verwaltete Regel“ und anschließend eine Regel-ID aus.
- Wählen Sie eine AWS Config benutzerdefinierte Regel und anschließend eine Regel-ID aus.
- Wählen Sie AWS Security Hub CSPM Steuerung und anschließend ein Security Hub CSPM-Steuerelement aus.
- Wählen Sie Manuelle Datenquelle und anschließend eine Option aus:
  - Datei-Upload — Verwenden Sie diese Option, wenn für die Kontrolle Unterlagen als Nachweis erforderlich sind.
  - Textantwort — Verwenden Sie diese Option, wenn die Kontrolle eine Antwort auf eine Frage zur Risikobewertung benötigt.

> **Tip**
>
> Informationen zu automatisierten Datenquellentypen und Tipps zur Problembehandlung finden Sie unterUnterstützte Datenquellentypen für automatisierte Beweise.
> Wenn Sie Ihre Datenquelleneinrichtung mit einem Experten überprüfen müssen, wählen Sie vorerst Manuelle Datenquelle. Auf diese Weise können Sie die Kontrolle jetzt erstellen und zu einem Framework hinzufügen und die Kontrolle dann später nach Bedarf bearbeiten.

d. Geben Sie unter Datenquellenname einen beschreibenden Namen ein.

e. (Optional) Geben Sie unter Zusätzliche Details eine Beschreibung der Datenquelle und eine Beschreibung der Fehlerbehebung ein.

f. Wählen Sie Datenquelle hinzufügen aus.

g. (Optional) Um eine weitere Datenquelle hinzuzufügen, wählen Sie Hinzufügen aus und wiederholen Sie Schritt 3. Sie können bis zu 100 Datenquellen hinzufügen.

4. Wählen Sie Weiter aus, sobald Sie fertig sind.

Schritt 3: Bearbeiten eines Aktionsplans

Überprüfen und bearbeiten Sie als nächstes den optionalen Aktionsplan.

> **Important**
>
> Wir empfehlen dringend, vertrauliche Daten niemals in frei formatierte Felder wie den Aktionsplan einzugeben. Wenn Sie benutzerdefinierte Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

Um einen Aktionsplan zu bearbeiten

1. Bearbeiten Sie den Titel unter Titel nach Bedarf.
2. Bearbeiten Sie die Anweisungen unter Anweisungen nach Bedarf.
3. Wählen Sie Weiter aus.

Schritt 4: Überprüfen und speichern

Überprüfen Sie die Informationen für die Kontrolle. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten.

Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.

> **Note**
>
> Nachdem Sie eine Kontrolle bearbeitet haben, werden die Änderungen in allen aktiven Bewertungen, die die Kontrolle enthalten, wie folgt wirksam:
>
> - Bei Kontrollen mit AWS API-Aufrufen als Datenquellentyp werden die Änderungen am darauffolgenden Tag um 00:00 Uhr UTC wirksam.
> - Bei allen anderen Kontrollen werden die Änderungen sofort wirksam.

Nächste Schritte

Wenn Sie sicher sind, dass Sie ein benutzerdefiniertes Steuerelement nicht mehr benötigen, können Sie Ihre Audit Manager Manager-Umgebung bereinigen, indem Sie das Steuerelement löschen. Detaillierte Anweisungen finden Sie unter Löschen eines benutzerdefinierten Steuerelements in AWS Audit Manager.

Weitere Ressourcen

Lösungen zur Kontrolle von Problemen in Audit Manager finden Sie unterBehebung von Problemen mit Kontrollen und Kontrollsätzen.

Ändern der Häufigkeit, mit der eine Kontrolle Beweise sammelt

AWS Audit Manager kann Beweise aus verschiedenen Datenquellen sammeln. Die Häufigkeit der Beweiserhebung hängt von der Art der Datenquelle ab, die die Kontrolle verwendet.

In den folgenden Abschnitten finden Sie weitere Informationen zur Häufigkeit der Erfassung von Beweisen für jeden Kontrolldatenquellentyp und dazu, wie Sie diese ändern können (falls zutreffend).

Themen

Wichtige Punkte

- Bei AWS API-Aufrufen sammelt Audit Manager Beweise mithilfe eines API-Beschreibungsaufrufs an einen anderen AWS-Service. Sie können die Häufigkeit der Beweissuche direkt in Audit Manager angeben (nur für benutzerdefinierte Kontrollen).
- Denn AWS ConfigAudit Manager meldet das Ergebnis einer Konformitätsprüfung direkt von AWS Config. Die Häufigkeit richtet sich nach den Triggern, die in der AWS Config Regel definiert sind.
- Denn AWS Security Hub CSPMAudit Manager meldet das Ergebnis einer Konformitätsprüfung direkt vom Security Hub CSPM. Die Frequenz folgt dem Zeitplan der Security Hub CSPM-Prüfung.

- Denn AWS CloudTrailAudit Manager sammelt kontinuierlich Beweise von CloudTrail. Sie können die Häufigkeit für diese Beweisart nicht ändern.

Schnappschüsse der Konfiguration von AWS API-Aufrufen

> **Note**
>
> Das Folgende gilt nur für benutzerdefinierte Kontrollen. Sie können die Häufigkeit der Beweiserhebung für eine Standardkontrolle nicht ändern.

Wenn ein benutzerdefiniertes Steuerelement AWS API-Aufrufe als Datenquellentyp verwendet, können Sie die Häufigkeit der Beweiserhebung in Audit Manager ändern, indem Sie die folgenden Schritte ausführen.

Um die Häufigkeit der Erfassung von Beweisen für eine benutzerdefinierte Kontrolle mit einer API-Aufruf-Datenquelle zu ändern

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Control Library und dann die Registerkarte Benutzerdefiniert aus.
3. Wählen Sie die benutzerdefinierte Kontrolle aus, die Sie bearbeiten möchten, und wählen Sie dann Bearbeiten.
4. Klicken Sie auf der Seite Kontrolldetails bearbeiten auf Weiter.
5. Suchen Sie unter Vom Kunden verwaltete Quellen nach der API-Aufruf-Datenquelle, die Sie aktualisieren möchten.
6. Wählen Sie die Datenquelle aus der Tabelle aus und klicken Sie dann auf Entfernen.
7. Wählen Sie Hinzufügen aus.
8. Wählen Sie AWS API-Aufrufe aus.
9. Wählen Sie denselben API-Aufruf aus, den Sie in Schritt 5 entfernt haben, und wählen Sie dann Ihre bevorzugte Häufigkeit für die Erfassung von Nachweisen aus.
10. Geben Sie unter Datenquellenname einen aussagekräftigen Namen ein.
11. (Optional) Geben Sie unter Zusätzliche Details eine Beschreibung der Datenquelle und eine Beschreibung der Fehlerbehebung ein.

12. Wählen Sie Weiter aus.
13. Wählen Sie auf der Seite Einen Aktion bearbeiten Weiter aus.
14. Überprüfen Sie auf der Seite Überprüfen und aktualisieren die Informationen für das benutzerdefinierte Steuerelement. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten.
15. Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.

Nachdem Sie ein Steuerelement bearbeitet haben, werden die Änderungen am Folgetag um 00:00 Uhr UTC in allen aktiven Bewertungen wirksam, die das Steuerelement beinhalten.

Konformitätsprüfungen von AWS Config

> **Note**
>
> Das Folgende gilt sowohl für Standard-Kontrollen als auch für benutzerdefinierte Kontrollen, die AWS-Config-Regeln als Datenquelle verwenden.

Wenn ein Steuerelement AWS Config als Datenquellentyp verwendet wird, können Sie die Häufigkeit der Beweiserhebung nicht direkt in Audit Manager ändern. Das liegt daran, dass die Frequenz den Triggern folgt, die in der AWS Config Regel definiert sind.

Es gibt zwei Arten von Triggern für AWS-Config-Regeln:

1. Konfigurationsänderungen — AWS Config führt Evaluierungen für die Regel durch, wenn bestimmte Ressourcentypen erstellt, geändert oder gelöscht werden.
2. Periodisch — AWS Config Führt Evaluierungen für die Regel mit einer von Ihnen gewählten Häufigkeit aus (z. B. alle 24 Stunden).

Weitere Informationen zu den Triggern für AWS-Config-Regeln finden Sie unter Triggertypen im AWS Config Entwicklerhandbuch.

Anweisungen zur Verwaltung finden Sie AWS-Config-Regeln unter AWS Config Regeln verwalten.

Konformitätsprüfungen von Security Hub CSPM

> **Note**
>
> Das Folgende gilt sowohl für Standardsteuerungen als auch für benutzerdefinierte Steuerelemente, die Security Hub CSPM-Prüfungen als Datenquelle verwenden.

Wenn ein Steuerelement Security Hub CSPM als Datenquellentyp verwendet, können Sie die Häufigkeit der Beweiserhebung nicht direkt in Audit Manager ändern. Dies liegt daran, dass die Frequenz dem Zeitplan der Security Hub CSPM-Prüfungen folgt.

- Regelmäßige Prüfungen werden automatisch innerhalb von 12 Stunden nach der letzten Ausführung ausgeführt. Sie können die Periodizität nicht ändern.
- Durch Änderungen ausgelöste Prüfungen werden ausgeführt, wenn sich der Status der zugeordneten Ressource ändert. Auch wenn die Ressource den Status nicht ändert, wird die aktualisierte Aktualisierung für Änderungen ausgelöste Prüfungen alle 18 Stunden aktualisiert. Dies zeigt an, dass das Kontrollelement noch aktiviert ist. Im Allgemeinen verwendet Security Hub CSPM wann immer möglich durch Änderungen ausgelöste Regeln.

Weitere Informationen finden Sie im AWS Security Hub CSPM -Benutzerhandbuch unter Zeitplan für die Durchführung von Sicherheitsprüfungen.

Benutzeraktivitätsprotokolle von AWS CloudTrail

> **Note**
>
> Das Folgende gilt sowohl für Standard-Kontrollen als auch für benutzerdefinierte Kontrollen, die AWS CloudTrail Benutzeraktivitätsprotokolle als Datenquelle verwenden.

Sie können die Häufigkeit der Beweiserhebung für Kontrollen, die Aktivitätsprotokolle CloudTrail als Datenquellentyp verwenden, nicht ändern. Audit Manager sammelt diese Art von CloudTrail Nachweisen kontinuierlich. Die Häufigkeit ist kontinuierlich, da Benutzeraktivitäten zu jeder Tageszeit auftreten können.

Löschen eines benutzerdefinierten Steuerelements in AWS Audit Manager

Wenn Sie ein benutzerdefiniertes Steuerelement erstellt haben und es nicht mehr benötigen, können Sie es aus Ihrer Audit Manager Manager-Umgebung löschen. Auf diese Weise können Sie Ihren Arbeitsbereich aufräumen und sich auf die benutzerdefinierten Steuerelemente konzentrieren, die für Ihre aktuellen Aufgaben und Prioritäten relevant sind.

Voraussetzungen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie zuvor ein benutzerdefiniertes Steuerelement erstellt haben.

Stellen Sie sicher, dass Ihre IAM-Identität über die entsprechenden Berechtigungen zum Löschen eines benutzerdefinierten Steuerelements verfügt. AWS Audit Manager Zwei vorgeschlagene Richtlinien, die diese Berechtigungen gewähren, sind AWSAuditManagerAdministratorAccessundErlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager.

Verfahren

Sie können benutzerdefinierte Steuerelemente mithilfe der Audit Manager Manager-Konsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) löschen.

> **Important**
>
> Wenn Sie eine benutzerdefinierte Kontrolle löschen, wird die Kontrolle durch diese Aktion aus allen benutzerdefinierten Frameworks oder Bewertungen entfernt, mit denen sie derzeit verknüpft ist. Infolgedessen wird Audit Manager in all Ihren Bewertungen keine Beweise für diese benutzerdefinierte Kontrolle mehr sammeln. Dazu gehören auch Bewertungen, die Sie zuvor erstellt haben, bevor Sie die benutzerdefinierte Kontrolle gelöscht haben.

Audit Manager console

Um ein benutzerdefiniertes Steuerelement in der Audit Manager Manager-Konsole zu löschen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek und dann die Registerkarte Benutzerdefinierte Kontrollen aus.
3. Wählen Sie die zu löschende Kontrolle aus und klicken Sie auf Löschen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster Löschen, um den Löschvorgang zu bestätigen.

AWS CLI

Um ein benutzerdefiniertes Steuerelement in der AWS CLI

1. Identifizieren Sie zunächst die benutzerdefinierte Kontrolle, die Sie löschen möchten. Führen Sie dazu den Befehl Kontrollen auflisten aus und geben Sie den `--control-type` als `Custom` an.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   Die Antwort gibt eine Liste von benutzerdefinierten Kontrollen zurück. Suchen Sie die Kontrolle, die Sie löschen möchten, und notieren Sie sich die Kontroll-ID.
2. Führen Sie als Nächstes den Befehl Kontrolle löschen aus und geben Sie mit dem `--control-id`-Parameter die Kontrolle an, die Sie löschen möchten.

   Ersetzen Sie im folgenden Beispiel das *`placeholder text`* durch Ihre eigenen Informationen.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Um ein benutzerdefiniertes Steuerelement mithilfe der API zu löschen

1. Verwenden Sie den ListControlsVorgang und geben Sie den ControlType als `Custom` an. Suchen Sie in der Antwort die Kontrolle, die Sie löschen möchten, und notieren Sie sich die Kontrollelement-ID.
2. Verwenden Sie den DeleteControlVorgang, um das benutzerdefinierte Steuerelement zu löschen. Verwenden Sie in der Anforderung den Parameter controlId, um die Kontrolle anzugeben, die Sie löschen möchten.

Weitere Informationen zu diesen API-Vorgängen erhalten Sie, indem Sie auf einen der Links im vorherigen Verfahren klicken, um weitere Informationen in der AWS Audit Manager API-Referenz zu erhalten. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Weitere Ressourcen

Informationen zur Datenspeicherung in Audit Manager finden Sie unterLöschung von Audit Manager-Daten.

Überprüfung und Konfiguration Ihrer AWS Audit Manager Einstellungen

Sie können Ihre AWS Audit Manager Einstellungen jederzeit überprüfen und konfigurieren, um sicherzustellen, dass sie Ihren spezifischen Anforderungen entsprechen.

In diesem Kapitel erfahren Sie, wie Sie auf Ihre Audit Manager Manager-Einstellungen zugreifen, diese überprüfen und anpassen step-by-step. Im Folgenden erfahren Sie, wie Sie Ihre allgemeinen Einstellungen, Bewertungseinstellungen und Einstellungen für die Beweissuche ändern können, um sie an Ihre sich ändernden Compliance-Ziele und Geschäftsanforderungen anzupassen.

Verfahren

Gehen Sie zunächst wie folgt vor, um Ihre Audit Manager-Einstellungen einzusehen. Sie können Ihre Audit Manager Manager-Einstellungen über die Audit Manager Manager-Konsole, die AWS Command Line Interface (AWS CLI) oder die Audit Manager Manager-API anzeigen.

Um Ihre Einstellungen einzusehen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie den Tab, der Ihrem Ziel entspricht.

   - Allgemeine Einstellungen — Wählen Sie diese Registerkarte, um Ihre allgemeinen Audit Manager Manager-Einstellungen zu überprüfen und zu aktualisieren.
   - Bewertungseinstellungen — Wählen Sie diese Registerkarte, um die Standardeinstellungen für Ihre Bewertungen zu überprüfen und zu aktualisieren.
   - Einstellungen für die Evidenzsuche — Wählen Sie diese Registerkarte, um Ihre Einstellungen für die Evidenzsuche zu überprüfen und zu aktualisieren.

Nächste Schritte

Um Ihre Audit Manager Manager-Einstellungen an Ihren Anwendungsfall anzupassen, folgen Sie den hier beschriebenen Verfahren.

- Allgemeine Einstellungen
  - Konfiguration Ihrer Datenverschlüsselungseinstellungen
  - Hinzufügen eines delegierten Administrators
  - Einen delegierten Administrator ändern
  - Einen delegierten Administrator entfernen
  - Deaktivierung AWS Audit Manager
- Einstellungen für die Bewertung
  - Konfiguration Ihrer standardmäßigen Prüfinhaber
  - Konfiguration Ihres Standardziels für Bewertungsberichte
  - Konfiguration Ihrer Audit Manager Manager-Benachrichtigungen
- Einstellungen für die Beweissuche
  - Beweissuche aktivieren
  - Bestätigung des Status von Evidence Finder
  - Konfiguration Ihres Standardexportziels für Evidence Finder
  - Beweissuche deaktivieren

Konfiguration Ihrer Datenverschlüsselungseinstellungen

Sie können wählen, wie Sie Ihre Daten verschlüsseln möchten. AWS Audit Manager Audit Manager erstellt automatisch ein Unikat Von AWS verwalteter Schlüssel für die sichere Speicherung Ihrer Daten. Standardmäßig werden Ihre Audit Manager-Daten mit diesem KMS-Schlüssel verschlüsselt. Wenn Sie jedoch Ihre Datenverschlüsselungseinstellungen anpassen möchten, können Sie Ihren eigenen, vom Kunden verwalteten symmetrischen Verschlüsselungsschlüssel angeben. Die Verwendung eines eigenen Verschlüsselung gibt Ihnen mehr Flexibilität, einschließlich der Fähigkeit, Schlüssel zu erstellen, zu rotieren und zu deaktivieren.

Voraussetzungen

Wenn Sie einen vom Kunden verwalteten Schlüssel angeben, muss dieser in Ihrer Bewertung enthalten AWS-Region sein, damit Bewertungsberichte erstellt und die Suchergebnisse von Evidence Finder erfolgreich exportiert werden können.

Verfahren

Sie können Ihre Verschlüsselungseinstellungen aktualisieren, indem Sie die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI), oder die Audit Manager-API nutzen.

> **Note**
>
> Wenn Sie Ihre Audit Manager-Datenverschlüsselungseinstellungen ändern, gelten diese Änderungen für die neuen Bewertungen, die Sie erstellen. Dies schließt alle Bewertungsberichte und Beweissuche-Berichte mit ein, die Sie anhand Ihrer neuen Bewertungen erstellen.
> Die Änderungen gelten nicht für bestehende Bewertungen, die Sie erstellt haben, bevor Sie Ihre Verschlüsselungseinstellungen geändert haben. Dazu gehören neben bestehenden Bewertungsberichten und CSV-Berichten auch neue Bewertungsberichte und CSV-Berichte, die Sie anhand vorhandener Bewertungen erstellen. Bestehende Bewertungen – und all ihre Bewertungsberichte und CSV-Berichte – verwenden weiterhin den alten KMS-Schlüssel. Wenn die IAM-Identität, die den Bewertungsbericht generiert, den alten KMS-Schlüssel nicht verwenden kann, können Sie Berechtigungen auf der Ebene der Schlüsselrichtlinie gewähren.

Audit Manager console

So aktualisieren Sie Ihre Datenverschlüsselungseinstellungen in der Audit Manager Manager-Konsole

1. Gehen Sie auf der Registerkarte Allgemeine Einstellungen zum Abschnitt Datenverschlüsselung.
2. Um den von Audit Manager bereitgestellten Standard-KMS-Schlüssel zu verwenden, deaktivieren Sie das Kontrollkästchen Verschlüsselungseinstellungen anpassen (erweitert).
3. Um einen kundenverwalteten Schlüssel zu verwenden, aktivieren Sie das Kontrollkästchen Verschlüsselungseinstellungen anpassen (erweitert). Sie können dann ein vorhandenes Schlüsselpaar wählen oder ein neues erstellen.

AWS CLI

So aktualisieren Sie Ihre Datenverschlüsselungseinstellungen im AWS CLI

Führen Sie den Befehl Einstellungen aktualisieren aus und verwenden Sie den `--kms-key`-Parameter, um Ihren eigenen vom Kunden verwalteten Schlüssel anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Um Ihre Datenverschlüsselungseinstellungen mithilfe der API zu aktualisieren

Rufen Sie den UpdateSettingsVorgang auf und verwenden Sie den Parameter KMSKey, um Ihren eigenen vom Kunden verwalteten Schlüssel anzugeben.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operation und dieses Parameters in einer der sprachspezifischen Sprachen. AWS SDKs

Weitere Ressourcen

- Anweisungen zum Erstellen von Schlüsseln finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Benutzerhandbuch.
- Anweisungen zum Erteilen von Berechtigungen auf der Ebene der wichtigsten Richtlinien finden Sie unter Erlauben der Verwendung eines KMS-Schlüssels für Benutzer mit anderen Konten im AWS Key Management Service Entwicklerhandbuch.

Hinzufügen eines delegierten Administrators

Wenn Sie die Unterstützung mehrerer Konten für verwenden AWS Organizations und aktivieren möchten AWS Audit Manager, können Sie ein Mitgliedskonto in Ihrer Organisation als delegierten Administrator für Audit Manager festlegen.

Wenn Sie Audit Manager in mehr als einer Region verwenden möchten AWS-Region, müssen Sie in jeder Region separat ein delegiertes Administratorkonto einrichten. Sie sollten in Ihren Audit Manager-Einstellungen für alle Regionen dasselbe delegierte Administratorkonto angeben.

Voraussetzungen

Beachten Sie die folgenden Faktoren, die die Arbeitsweise des delegierten Administrators in Audit Manager definieren:

- Ihre Konten müssen Teil einer Organisation sein.
- Bevor Sie einen delegierten Administrator benennen, müssen Sie alle Funktionen in Ihrer Organisation aktivieren. Sie müssen auch die Security Hub CSPM-Einstellungen Ihres Unternehmens konfigurieren. Auf diese Weise kann Audit Manager Security Hub CSPM-Beweise von Ihren Mitgliedskonten sammeln.
- Das Konto des delegierten Administrators muss Zugriff auf den KMS-Schlüssel haben, den Sie bei der Einrichtung von Audit Manager angegeben haben.
- Sie können Ihr AWS Organizations Verwaltungskonto nicht als delegierter Administrator in Audit Manager verwenden.

Verfahren

Sie können einen delegierten Administrator mithilfe der Audit Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager-API hinzufügen.

> **Note**
>
> Nachdem Sie in Ihren Audit Manager-Einstellungen einen delegierten Administrator hinzugefügt haben, kann Ihr Verwaltungskonto keine zusätzlichen Bewertungen mehr in Audit Manager erstellen. Darüber hinaus wird die Erfassung von Nachweisen für alle vorhandenen Bewertungen, die vom Verwaltungskonto erstellt wurden, beendet. Audit Manager sammelt Nachweise und fügt sie dem delegierten Administratorkonto hinzu. Dabei handelt es sich um das Hauptkonto für die Verwaltung der Bewertungen Ihrer Organisation.

Audit Manager console

So fügen Sie einen delegierten Administrator zur Audit Manager Manager-Konsole hinzu

1. Gehen Sie auf der Registerkarte Allgemeine Einstellungen zum Bereich Delegierter Administrator.

2. Geben Sie unter Delegierter Administratorkonto-ID die Konto-ID des delegierten Administrators ein.
3. Wählen Sie Delegieren.

AWS CLI

Um einen delegierten Administrator hinzuzufügen AWS CLI

Führen Sie den register-organization-admin-accountBefehl aus und verwenden Sie den `--admin-account-id` Parameter, um die Konto-ID des delegierten Administrators anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Um einen delegierten Administrator mithilfe der API hinzuzufügen

Rufen Sie den RegisterOrganizationAdminAccountVorgang auf und verwenden Sie den adminAccountIdParameter, um die Konto-ID des delegierten Administrators anzugeben.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operation und dieses Parameters in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Informationen zum Ändern Ihres delegierten Administratorkontos finden Sie unter. Einen delegierten Administrator ändern

Informationen zum Entfernen Ihres delegierten Administratorkontos finden Sie unter. Einen delegierten Administrator entfernen

Weitere Ressourcen

- Eine Organisation erstellen und verwalten
- Behebung von Problemen mit delegierten AWS Organizations -Administratoren

Einen delegierten Administrator ändern

Das Ändern Ihres delegierten Administrators AWS Audit Manager erfolgt in zwei Schritten. Zunächst müssen Sie das aktuelle delegierte Administratorkonto entfernen. Anschließend können Sie ein neues Konto als delegierter Administrator hinzufügen.

Folgen Sie den Schritten auf dieser Seite, um Ihren delegierten Administrator zu ändern.

Inhalt

Voraussetzungen

Bevor Sie das aktuelle Konto entfernen

Bevor Sie das aktuelle delegierte Administratorkonto entfernen, sollten Sie die folgenden Überlegungen berücksichtigen:

- Aufgabe zur Bereinigung von Nachweisen — Wenn der aktuelle delegierte Administrator (Konto A) die Beweissuche aktiviert hat, müssen Sie eine Säuberungsaufgabe ausführen, bevor Sie Konto B dem neuen delegierten Administrator zuweisen.

  Bevor Sie Ihr Verwaltungskonto verwenden, um Konto A zu entfernen, stellen Sie sicher, dass Konto A sich bei Audit Manager anmeldet und die Beweissuche deaktiviert. Durch die Deaktivierung der Beweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Beweissuche aktiviert wurde.

  Wenn diese Aufgabe nicht abgeschlossen ist, verbleibt der Ereignisdatenspeicher in Konto A. In diesem Fall empfehlen wir, dass der ursprüngliche delegierte Administrator CloudTrail Lake verwendet, um den Ereignisdatenspeicher manuell zu löschen.

Diese Bereinigungsaufgabe ist erforderlich, um sicherzustellen, dass Sie am Ende nicht mehrere Ereignisdatenspeicher haben. Audit Manager ignoriert einen ungenutzten Ereignisdatenspeicher, nachdem Sie ein delegiertes Administratorkonto entfernt oder geändert haben. Wenn Sie den ungenutzten Ereignisdatenspeicher jedoch nicht löschen, fallen für den Ereignisdatenspeicher weiterhin Speicherkosten von CloudTrail Lake an.

- Datenlöschung — Wenn Sie ein delegiertes Administratorkonto für Audit Manager entfernen, werden die Daten für dieses Konto nicht gelöscht. Wenn Sie Ressourcendaten für ein delegiertes Administratorkonto löschen möchten, müssen Sie diese Aufgabe separat ausführen, bevor Sie das Konto entfernen. Sie können dies von der Audit Manager-Konsole aus erledigen. Sie können aber auch einen der API-Löschvorgänge verwenden, die von Audit Manager bereitgestellt werden. Eine Liste der verfügbaren Löschvorgänge finden Sie unter Löschen von Audit Manager-Daten.

  Derzeit bietet Audit Manager keine Option zum Löschen von Nachweisen für einen bestimmten delegierten Administrator. Wenn Ihr Verwaltungskonto Audit Manager abmeldet, führen wir stattdessen eine Bereinigung für das aktuelle delegierte Administratorkonto zum Zeitpunkt der Abmeldung durch.

Bevor Sie das neue Konto hinzufügen

Bevor Sie das neue delegierte Administratorkonto hinzufügen, sollten Sie die folgenden Überlegungen berücksichtigen:

- Das neue Konto muss Teil einer Organisation sein.
- Bevor Sie einen neuen delegierten Administrator benennen, müssen Sie alle Funktionen in Ihrer Organisation aktivieren. Sie müssen auch die Security Hub CSPM-Einstellungen Ihres Unternehmens konfigurieren. Auf diese Weise kann Audit Manager Security Hub CSPM-Beweise von Ihren Mitgliedskonten sammeln.
- Das Konto des delegierten Administrators muss Zugriff auf den KMS-Schlüssel haben, den Sie bei der Einrichtung von Audit Manager angegeben haben.
- Sie können Ihr AWS Organizations Verwaltungskonto nicht als delegierter Administrator in Audit Manager verwenden.

Verfahren

Sie können einen delegierten Administrator mithilfe der Audit-Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager-API ändern.

> **Warning**
>
> Wenn Sie einen delegierten Administrator ändern, haben Sie weiterhin Zugriff auf die Nachweise, die Sie zuvor unter dem alten delegierten Administratorkonto gesammelt haben. Audit Manager sammelt jedoch keine Nachweise mehr und fügt dem alten delegierten Administratorkonto keine Nachweise mehr hinzu.

Audit Manager console

So ändern Sie den aktuellen delegierten Administrator in der Audit Manager Manager-Konsole

1. (Optional) Wenn der aktuelle delegierte Administrator (Konto A) die Beweissuche aktiviert hat, führen Sie die folgende Bereinigungsaufgabe aus:

   - Bevor Sie Konto B als neuen delegierten Administrator zuweisen, stellen Sie sicher, dass Konto A sich bei Audit Manager anmeldet und die Beweissuche deaktiviert.

     Durch die Deaktivierung der Beweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als Konto A die Beweissuche aktiviert hat. Wenn Sie diesen Schritt nicht abschließen, muss Konto A zu CloudTrail Lake wechseln und den Ereignisdatenspeicher manuell löschen. Andernfalls verbleibt der Ereignisdatenspeicher in Konto A und es fallen weiterhin CloudTrail Lake-Speichergebühren an.
2. Gehen Sie auf der Registerkarte Allgemeine Einstellungen zum Bereich Delegierter Administrator und wählen Sie Entfernen.
3. Wählen Sie im daraufhin angezeigten Popup-Fenster zur Bestätigung die Option Entfernen.
4. Geben Sie unter Delegierter Administratorkonto-ID die Konto-ID des neuen delegierten Administrators ein.
5. Wählen Sie Delegieren.

AWS CLI

Um den aktuellen delegierten Administrator in der AWS CLI

Führen Sie zunächst den deregister-organization-admin-accountBefehl aus, indem Sie den `--admin-account-id` Parameter verwenden, um die Konto-ID des aktuellen delegierten Administrators anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Führen Sie dann den register-organization-admin-accountBefehl mit dem `--admin-account-id` Parameter aus, um die Konto-ID des neuen delegierten Administrators anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Um den aktuellen delegierten Administrator mithilfe der API zu ändern

Rufen Sie zunächst den DeregisterOrganizationAdminAccountVorgang auf und verwenden Sie den adminAccountIdParameter, um die Konto-ID des aktuellen delegierten Administrators anzugeben.

Rufen Sie dann den RegisterOrganizationAdminAccountVorgang auf und verwenden Sie den adminAccountIdParameter, um die Konto-ID des neuen delegierten Administrators anzugeben.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operation und dieses Parameters in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Informationen zum Entfernen Ihres delegierten Administratorkontos finden Sie unter. Einen delegierten Administrator entfernen

Weitere Ressourcen

- Eine Organisation erstellen und verwalten
- Behebung von Problemen mit delegierten AWS Organizations -Administratoren

Einen delegierten Administrator entfernen

Durch das Entfernen des delegierten Administratorkontos wird die weitere Erfassung von Nachweisen für dieses Konto gestoppt, Sie haben jedoch weiterhin Zugriff auf die zuvor gesammelten Nachweise.

Wenn Sie Ihr delegiertes Administratorkonto für Audit Manager entfernen müssen, können Sie die erforderlichen Schritte auf dieser Seite ausführen. Halten Sie sich sorgfältig an die Voraussetzungen und Verfahren, da dabei Ressourcen bereinigt werden müssen, um unnötige Speicherkosten zu vermeiden.

Voraussetzungen

Bevor Sie das delegierte Administratorkonto aus Audit Manager entfernen, sollten Sie die folgenden Überlegungen berücksichtigen:

Bereinigungsaufgabe der Beweissuche

Wenn der aktuelle delegierte Administrator die Evidence Finder aktiviert hat, müssen Sie eine Säuberungsaufgabe durchführen.

Bevor Sie Ihr Verwaltungskonto verwenden, um den aktuellen delegierten Administrator zu entfernen, stellen Sie sicher, dass sich das aktuelle delegierte Administratorkonto bei Audit Manager anmeldet und die Evidence Finder deaktiviert. Durch die Deaktivierung der Beweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Beweissuche aktiviert wurde.

Wenn diese Aufgabe nicht abgeschlossen ist, verbleibt der Ereignisdatenspeicher in deren Konto. In diesem Fall empfehlen wir, dass der ursprüngliche delegierte Administrator CloudTrail Lake verwendet, um den Ereignisdatenspeicher manuell zu löschen.

Diese Bereinigungsaufgabe ist erforderlich, um sicherzustellen, dass Sie am Ende nicht mehrere Ereignisdatenspeicher haben. Audit Manager ignoriert einen ungenutzten Ereignisdatenspeicher, nachdem Sie ein delegiertes Administratorkonto entfernt oder geändert haben. Wenn Sie den

ungenutzten Ereignisdatenspeicher jedoch nicht löschen, fallen für den Ereignisdatenspeicher weiterhin Speicherkosten von CloudTrail Lake an.

Löschen von Daten

Wenn Sie ein delegiertes Administratorkonto für Audit Manager entfernen, werden die Daten für dieses Konto nicht gelöscht. Wenn Sie Ressourcendaten für ein delegiertes Administratorkonto löschen möchten, müssen Sie diese Aufgabe separat ausführen, bevor Sie das Konto entfernen. Sie können dies von der Audit Manager-Konsole aus erledigen. Sie können aber auch einen der API-Löschvorgänge verwenden, die von Audit Manager bereitgestellt werden. Eine Liste der verfügbaren Löschvorgänge finden Sie unter Löschen von Audit Manager-Daten.

Derzeit bietet Audit Manager keine Option zum Löschen von Nachweisen für einen bestimmten delegierten Administrator. Wenn Ihr Verwaltungskonto Audit Manager abmeldet, führen wir stattdessen eine Bereinigung für das aktuelle delegierte Administratorkonto zum Zeitpunkt der Abmeldung durch.

Verfahren

Sie können einen delegierten Administrator mithilfe der Audit Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager-API entfernen.

> **Warning**
>
> Wenn Sie einen delegierten Administrator entfernen, haben Sie weiterhin Zugriff auf die Nachweise, die Sie zuvor unter diesem delegierten Administratorkonto gesammelt haben. Audit Manager sammelt jedoch keine Nachweise mehr und fügt dem alten delegierten Administratorkonto keine Nachweise mehr hinzu.

Audit Manager console

Um den aktuellen delegierten Administrator von der Audit Manager Manager-Konsole zu entfernen

1. (Optional) Wenn der aktuelle delegierte Administrator die Beweissuche aktiviert hat, führen Sie die folgende Bereinigungsaufgabe aus:

   - Stellen Sie sicher, dass sich das aktuelle Konto des delegierten Administrators bei Audit Manager anmeldet und die Beweissuche deaktiviert.

Durch die Deaktivierung der Beweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Beweissuche aktiviert wurde. Wenn dieser Schritt nicht abgeschlossen ist, muss das delegierte Administratorkonto CloudTrail Lake verwenden, um den Ereignisdatenspeicher manuell zu löschen. Andernfalls verbleibt der Ereignisdatenspeicher in ihrem Konto und es fallen weiterhin CloudTrail Lake-Speichergebühren an.

2. Gehen Sie auf der Registerkarte Allgemeine Einstellungen zum Bereich Delegierter Administrator und wählen Sie Entfernen.
3. Wählen Sie im daraufhin angezeigten Popup-Fenster zur Bestätigung die Option Entfernen.

AWS CLI

Durch die Deaktivierung der Beweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Beweissuche aktiviert wurde. Wenn dieser Schritt nicht abgeschlossen ist, muss das delegierte Administratorkonto CloudTrail Lake verwenden, um den Ereignisdatenspeicher manuell zu löschen. Andernfalls verbleibt der Ereignisdatenspeicher in ihrem Konto und es fallen weiterhin CloudTrail Lake-Speichergebühren an.

Um den aktuellen delegierten Administrator zu entfernen AWS CLI

Führen Sie den deregister-organization-admin-accountBefehl aus und verwenden Sie den `--admin-account-id` Parameter, um die Konto-ID des delegierten Administrators anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Um den aktuellen delegierten Administrator mithilfe der API zu entfernen

Rufen Sie den DeregisterOrganizationAdminAccountVorgang auf und verwenden Sie den adminAccountIdParameter, um die Konto-ID des delegierten Administrators anzugeben.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operation und dieses Parameters in einer der sprachspezifischen Sprachen AWS SDKs.

Weitere Ressourcen

- Behebung von Problemen mit delegierten AWS Organizations -Administratoren

Konfiguration Ihrer standardmäßigen Prüfinhaber

Sie können diese Einstellung verwenden, um die Standardbenutzer audit owner anzugeben, die primären Zugriff auf Ihre Bewertungen in Audit Manager haben.

Verfahren

Sie können diese Einstellung mit der Audit Manager Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager Manager-API aktualisieren.

Audit Manager console

Sie können aus den in der Tabelle AWS-Konten aufgelisteten Optionen wählen oder die Suchleiste verwenden, um nach anderen zu suchen AWS-Konten.

So aktualisieren Sie Ihre standardmäßigen Auditbesitzer in der Audit Manager Manager-Konsole

1. Gehen Sie auf der Registerkarte Bewertungseinstellungen zum Abschnitt Standard-Audit-Verantwortliche und wählen Sie Bearbeiten aus.
2. Um einen standardmäßigen Audit-Verantwortlichen hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dem Kontonamen unter Audit-Verantwortlicher.
3. Um einen standardmäßigen Audit-Verantwortlichen zu entfernen, deaktivieren Sie das Kontrollkästchen neben dem Kontonamen unter Audit-Verantwortlicher.
4. Klicken Sie abschließend auf Speichern.

AWS CLI

So aktualisieren Sie Ihren standardmäßigen Prüfinhaber in der AWS CLI

Führen Sie den Befehl update-settings aus und verwenden Sie den `--default-process-owners` Parameter, um einen Audit-Verantwortlichen anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen. Beachten Sie, dass `roleType` nur `PROCESS_OWNER` sein kann.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Um Ihren Standard-Audit-Besitzer mithilfe der API zu aktualisieren

Rufen Sie den UpdateSettingsVorgang auf und verwenden Sie den defaultProcessOwnersParameter, um die Standard-Audit-Besitzer anzugeben. Beachten Sie, dass `roleType` nur `PROCESS_OWNER` sein kann.

Weitere Ressourcen

- Weitere Informationen zu Audit-Verantwortlichen finden Sie im Abschnitt Konzepte und Terminologie dieses Handbuchs unter Audit-Verantwortliche.

Konfiguration Ihres Standardziels für Bewertungsberichte

Wenn Sie einen Bewertungsbericht generieren, veröffentlicht Audit Manager den Bericht im S3-Bucket Ihrer Wahl. Dieser S3-Bucket wird als bezeichnetassessment report destination. Sie können den S3-Bucket auswählen, in dem Audit Manager Ihre Bewertungsberichte speichert.

Voraussetzungen

Konfigurationstipps für das Ziel Ihres Bewertungsberichts

Um die erfolgreiche Erstellung Ihres Bewertungsberichts sicherzustellen, empfehlen wir Ihnen, die folgenden Konfigurationen für Ihr Bewertungsberichtziel zu verwenden.

Buckets derselben Region

Wir empfehlen, einen S3-Bucket zu verwenden, der sich im selben AWS-Region wie Ihre Bewertung befindet. Wenn Sie einen Bucket und eine Bewertung in derselben Region verwenden, kann Ihr Bewertungsbericht bis zu 22.000 Nachweiselemente enthalten. Umgekehrt können bei Verwendung eines regionsübergreifenden Buckets und einer regionsübergreifenden Bewertung nur 3.500 Nachweiselemente berücksichtigt werden.

AWS-Region

Der AWS-Region von Ihrem Kunden verwaltete Schlüssel (falls Sie einen angegeben haben) muss mit der Region Ihrer Bewertung und dem Ziel-S3-Bucket Ihres Bewertungsberichts übereinstimmen. Anweisungen zum Ändern des KMS-Schlüssels finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen. Eine Liste der unterstützen Regionen für Audit Manager finden Sie unter AWS Audit Manager Endpunkte und Kontingente in Allgemeine Amazon Web Services-Referenz.

S3-Bucket-Verschlüsselung

Wenn Ihr Bewertungsberichtsziel über eine Bucket-Richtlinie verfügt, die serverseitige Verschlüsselung (SSE) mit SSE-KMS erfordert, muss der in dieser Bucket-Richtlinie verwendete KMS-Schlüssel mit dem KMS-Schlüssel übereinstimmen, den Sie in Ihren Audit Manager-Datenverschlüsselungseinstellungen konfiguriert haben. Wenn Sie in Ihren Audit Manager-Einstellungen keinen KMS-Schlüssel konfiguriert haben und die Bucket-Richtlinie Ihrer Zieleinstellungen für den Bewertungsbericht SSE erfordert, stellen Sie sicher, dass die Bucket-Richtlinie SSE-S3 zulässt. Anweisungen zur Konfiguration des KMS-Schlüssels, der für die Datenverschlüsselung verwendet wird, finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen.

Kontoübergreifende S3-Buckets

Die Verwendung eines kontoübergreifenden S3-Buckets als Ziel für Ihren Bewertungsbericht wird in der Audit Manager-Konsole nicht unterstützt. Sie können einen kontoübergreifenden Bucket als Ziel für Ihren Bewertungsbericht angeben, indem Sie den AWS CLI oder einen der beiden verwenden. Der Einfachheit halber empfehlen wir jedoch AWS SDKs, dies nicht zu tun.

> **Tip**
>
> Für optimale Sicherheit und Leistung empfehlen wir, einen S3-Bucket in demselben AWS Konto und derselben Region wie Ihre Bewertung zu verwenden.

Wenn Sie sich dafür entscheiden, einen kontoübergreifenden S3-Bucket als Ziel für Ihren Bewertungsbericht zu verwenden, sollten Sie die folgenden Punkte berücksichtigen.

- Standardmäßig gehören S3-Objekte — wie z. B. Bewertungsberichte — demjenigen, der das Objekt hochlädt. AWS-Konto Sie können die Einstellung S3 Object Ownership verwenden, um dieses Standardverhalten so zu ändern, dass alle neuen Objekte, die von Konten mit der

`bucket-owner-full-control` vordefinierten Zugriffssteuerungsliste (Access Control List, ACL) geschrieben werden, automatisch in den Besitz des Bucket-Eigentümers übergehen.

Dies ist zwar keine Voraussetzung, wir empfehlen Ihnen jedoch, die folgenden Änderungen an Ihren kontoübergreifenden Bucket-Einstellungen vorzunehmen. Durch diese Änderungen wird sichergestellt, dass der Bucket-Besitzer die volle Kontrolle über die Bewertungsberichte hat, die Sie in seinem Bucket veröffentlichen.

- Setzen Sie den Objekteigentum des S3-Buckets auf Bucket Owner Preferred und nicht auf den standardmäßigen Objektschreiber
- Fügen Sie eine Bucket-Richtlinie hinzu, um sicherzustellen, dass Objekte, die in diesen Bucket hochgeladen werden, den `bucket-owner-full-control` ACL haben

- Damit Audit Manager Berichte in einem kontoübergreifenden S3-Bucket veröffentlichen kann, müssen Sie Ihrem Bewertungsberichtziel die folgende S3-Bucket-Richtlinie hinzufügen. Ersetzen Sie *`placeholder text`* durch Ihre Informationen. Das `Principal` Element in dieser Richtlinie ist der Benutzer oder die Rolle, die für die Bewertung verantwortlich ist und die den Bewertungsbericht erstellt. Der `Resource` gibt den kontoübergreifenden S3-Bucket an, in dem der Bericht veröffentlicht wird.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow cross account assessment report publishing",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
```

```
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Verfahren

Sie können diese Einstellung mit der Audit Manager Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager Manager-API aktualisieren.

Audit Manager console

So aktualisieren Sie Ihr Standardziel für Bewertungsberichte in der Audit Manager Manager-Konsole

1. Gehen Sie auf der Registerkarte Bewertungseinstellungen zum Abschnitt Ziel des Bewertungsberichts.
2. Um einen vorhandenen S3-Bucket zu verwenden, wählen Sie einen Bucket-Namen aus dem Drop-down-Menü aus.
3. Um einen neuen S3-Bucket zu erstellen, wählen Sie Neuen Bucket erstellen.
4. Klicken Sie abschließend auf Speichern.

AWS CLI

Um Ihr standardmäßiges Ziel für Bewertungsberichte zu aktualisieren, finden Sie im AWS CLI

Führen Sie den Befehl update-settings aus und verwenden Sie den `--default-assessment-reports-destination`-Parameter, um einen S3-Bucket anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen:

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://amzn-s3-demo-destination-bucket
```

Audit Manager API

Um Ihr standardmäßiges Ziel für Bewertungsberichte mithilfe der API zu aktualisieren

Rufen Sie den UpdateSettingsVorgang auf und verwenden Sie den defaultAssessmentReportsDestination-Parameter, um einen S3-Bucket anzugeben.

Weitere Ressourcen

- Erstellen eines Buckets
- Bewertungsberichte

Konfiguration Ihrer Audit Manager Manager-Benachrichtigungen

Sie können Audit Manager so konfigurieren, dass Benachrichtigungen an das Amazon SNS SNS-Thema Ihrer Wahl gesendet werden. Wenn Sie dieses SNS-Thema abonniert haben, erhalten Sie bei jeder Anmeldung bei Audit Manager direkt Benachrichtigungen.

Folgen Sie den Schritten auf dieser Seite, um zu erfahren, wie Sie Ihre Benachrichtigungseinstellungen nach Ihren Wünschen anzeigen und aktualisieren können. Sie können entweder ein Standard-SNS-Thema oder ein FIFO (first-in-first-out) -SNS-Thema verwenden. Obwohl Audit Manager das Senden von Benachrichtigungen zu FIFO-Themen unterstützt, kann die Reihenfolge, in der Nachrichten gesendet werden, nicht garantiert werden.

Voraussetzungen

Wenn Sie ein Amazon SNS SNS-Thema verwenden möchten, das Sie nicht besitzen, müssen Sie Ihre AWS Identity and Access Management (IAM-) Richtlinie dafür konfigurieren. Insbesondere müssen Sie sie so konfigurieren, dass das Veröffentlichen über den Amazon-Ressourcennamen (ARN) des Themas ermöglicht wird. Eine Beispielrichtlinie, die Sie verwenden können, finden Sie unter. Beispiel 1 (Berechtigungen für das SNS-Thema)

Verfahren

Sie können diese Einstellung mit der Audit Manager Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager Manager-API aktualisieren.

Audit Manager console

So aktualisieren Sie Ihre Benachrichtigungseinstellungen in der Audit Manager Manager-Konsole

1. Gehen Sie auf der Registerkarte Bewertungseinstellungen zum Abschnitt Benachrichtigungen.
2. Um ein vorhandenes SNS-Thema zu verwenden, wählen Sie den Namen des Themas im Dropdown-Menü aus.
3. Um ein neues SNS-Thema zu erstellen, wählen Sie Create new topic aus.
4. Klicken Sie abschließend auf Speichern.

AWS CLI

So aktualisieren Sie Ihre Benachrichtigungseinstellungen im AWS CLI

Führen Sie den Befehl update-settings aus und verwenden Sie den `--sns-topic`-Parameter, um ein SNS-Thema anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Um Ihre Benachrichtigungseinstellungen mithilfe der API zu aktualisieren

Rufen Sie den UpdateSettingsVorgang auf und geben Sie mit dem Parameter snsTopic ein SNS-Thema an.

Weitere Ressourcen

- Anweisungen zum Erstellen eines Amazon-SNS-Themas finden Sie unter Erstellen eines Amazon SNS-Themas im Amazon SNS-Benutzerhandbuch.
- Eine Beispielrichtlinie, mit der Sie Audit Manager das Senden von Benachrichtigungen an Amazon SNS SNS-Themen ermöglichen können, finden Sie unter Beispiel 1 (Berechtigungen für das SNS-Thema)

- Weitere Informationen zur Liste der Handlungen, die Benachrichtigungen in Audit Manager auslösen, finden Sie unter Benachrichtigungen in AWS Audit Manager.
- Lösungen für Benachrichtigungsprobleme in Audit Manager finden Sie unterFehlerbehebung bei Benachrichtigungsproblemen.

Beweissuche aktivieren

Sie können die Funktion zur Beweissuche in Audit Manager aktivieren, um in Ihrem nach Beweisen zu suchen AWS-Konto. Wenn Sie ein delegierter Administrator für Audit Manager sind, können Sie nach Nachweisen für alle Mitgliedskonten in Ihrer Organisation suchen.

Folgen Sie diesen Schritten, um zu erfahren, wie Sie den Evidence Finder aktivieren. Achten Sie genau auf die Voraussetzungen, da Sie für diese Funktion spezielle Berechtigungen benötigen, um einen Ereignisdatenspeicher in CloudTrail Lake zu erstellen und zu verwalten.

Voraussetzungen

Erforderliche Berechtigungen zur Aktivierung der Beweissuche

Um Evidence Finder zu aktivieren, benötigen Sie Berechtigungen zum Erstellen und Verwalten eines Ereignisdatenspeichers in CloudTrail Lake. Um die Funktion nutzen zu können, benötigen Sie Berechtigungen zur Durchführung von CloudTrail Lake-Abfragen. Ein Beispiel für eine Berechtigungsrichtlinie, die Sie verwenden können, finden Sie unterBeispiel 3 (Berechtigungen zur Aktivierung von Evidence Finder).

Wenn Sie Hilfe zu Berechtigungen benötigen, wenden Sie sich an Ihren AWS Administrator. Wenn Sie ein AWS Administrator sind, können Sie die erforderliche Berechtigungserklärung kopieren und an eine IAM-Richtlinie anhängen.

Verfahren

Anforderung der Aktivierung der Beweissuche

Sie können diese Aufgabe mit der Audit Manager Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager Manager-API ausführen.

> **Note**
>
> Sie müssen den Evidence Finder in allen Bereichen aktivieren, in AWS-Region denen Sie nach Beweisen suchen möchten.

Audit Manager console

Um die Aktivierung der Evidence Finder auf der Audit Manager Manager-Konsole anzufordern

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Gehen Sie auf der Registerkarte Einstellungen für die Beweissuche zum Abschnitt Beweissuche.
3. Wählen Sie Erforderliche Berechtigungsrichtlinie und dann View CloudTrail Lake-Berechtigungen aus, um die erforderlichen Evidence Finder-Berechtigungen einzusehen. Wenn Sie diese Berechtigungen noch nicht haben, können Sie diese Richtlinienerklärung kopieren und an eine IAM-Richtlinie anhängen.
4. Wählen Sie Enable (Aktivieren) aus.
5. Wählen Sie im Popup-Fenster die Option Aktivierungsanfragen aus.

AWS CLI

Um die Aktivierung der Evidence Finder im zu beantragen AWS CLI

Führen Sie den Befehl update-settings mit dem `--evidence-finder-enabled`-Parameter aus.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Um die Aktivierung der Evidence Finder mithilfe der API zu beantragen

Rufen Sie die UpdateSettingsOperation auf und verwenden Sie den evidenceFinderEnabledParameter.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operation und dieses Parameters in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Nachdem Sie die Aktivierung von Evidence Finder angefordert haben, können Sie den Status Ihrer Anfrage überprüfen. Detaillierte Anweisungen finden Sie unter Bestätigung des Status von Evidence Finder .

Weitere Ressourcen

- Beweissuche
- Behebung von Problemen mit der Beweiserhebung

Bestätigung des Status von Evidence Finder

Nachdem Sie Ihre Anfrage zur Aktivierung von Evidence Finder eingereicht haben, dauert es bis zu 10 Minuten, bis die Funktion aktiviert und ein Ereignisdatenspeicher erstellt ist. Sobald der Ereignisdatenspeicher erstellt ist, werden ab sofort alle neuen Nachweise in den Ereignisdatenspeicher aufgenommen.

Wenn die Evidenzsuche aktiviert und der Ereignisdatenspeicher erstellt wurde, füllen wir den neu erstellten Ereignisdatenspeicher mit Ihren bisherigen Nachweisen aus bis zu zwei Jahren auf. Dieser Vorgang erfolgt automatisch und dauert bis zu sieben Tage.

Folgen Sie den Schritten auf dieser Seite, um den Status Ihrer Anfrage zur Aktivierung von Evidence Finder zu überprüfen und zu verstehen.

Voraussetzungen

Vergewissern Sie sich, dass Sie die Schritte zur Aktivierung von Evidence Finder befolgt haben. Detaillierte Anweisungen finden Sie unter Beweissuche aktivieren.

Verfahren

Sie können den aktuellen Status der Beweissuche mithilfe der Audit Manager-Konsole, der AWS CLI, oder der Audit Manager-API überprüfen.

Audit Manager console

Um den aktuellen Status von Evidence Finder auf der Audit Manager Manager-Konsole zu sehen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Überprüfen Sie unter Beweissuche aktivieren – optional den aktuellen Status.

   Jeder Status ist wie folgt definiert:

Status	Description
Der Evidence Finder ist nicht aktiviert	Sie haben die Beweissuche noch nicht erfolgreich aktiviert.
Sie haben beantragt , Evidence Finder zu aktivieren	Ihre Anfrage steht noch aus, bis der Ereignisdatenspeicher erstellt wird.
Der Evidence Finder ist aktiviert	Der Ereignisdatenspeicher wurde erstellt. Sie können jetzt die Beweissuche verwenden. Je nachdem, wie viele Nachweise Sie haben, dauert es bis zu sieben Tage, bis der neue Ereignisdatenspeicher mit Ihren früheren Nachweisdaten aufgefüllt ist. Ein blaues Informati onspanel zeigt an, dass die Datenauffüllung im Gange ist. In der Zwischenzeit können Sie gerne mit der Suche nach Nachweisen beginnen. Beachten Sie jedoch, dass nicht alle Daten verfügbar sind, bis die Auffüllung abgeschlossen ist.
Sie haben beantragt, den Evidence Finder zu deaktivieren	Ihre Anfrage steht noch aus, bis der Ereignisdatenspeicher gelöscht wird.
Der Evidence Finder wurde deaktiviert	Die Beweissuche wurde dauerhaft deaktiviert und der Ereignisdatenspeicher wurde gelöscht.

AWS CLI

Um den aktuellen Status der Evidence Finder zu sehen, finden Sie im AWS CLI

Führen Sie den Befehl get-settings mit dem `--attribute` Parameter auf `EVIDENCE_FINDER_ENABLEMENT` aus.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Dieses Verfahren gibt die folgenden Informationen zurück:

enablementStatus

Dieses Attribut zeigt den aktuellen Status der Beweissuche an.

- `ENABLE_IN_PROGRESS` - Sie haben die Aktivierung der Beweissuche angefordert. Ein Ereignisdatenspeicher wird derzeit erstellt, um Abfragen zur Nachweismittelsuche zu unterstützen.
- `ENABLED` - Der Ereignisdatenspeicher wurde erstellt und die Beweissuche ist aktiviert. Wir empfehlen, sieben Tage zu warten, bis der Ereignisdatenspeicher mit Ihren früheren Nachweisdaten aufgefüllt ist. In der Zwischenzeit können Sie die Beweissuche verwenden, aber nicht alle Daten sind verfügbar, bis die Datenspeicherung abgeschlossen ist.
- `DISABLE_IN_PROGRESS` - Sie haben die Deaktivierung der Beweissuche beantragt, Ihre Anfrage steht allerdings noch aus, bis der Ereignisdatenspeicher gelöscht ist.
- `DISABLED` - Sie haben die Beweissuche dauerhaft deaktiviert und der Ereignisdatenspeicher wird gelöscht. Nach diesem Zeitpunkt können Sie die Beweissuche nicht mehr reaktivieren.

backfillStatus

Dieses Attribut zeigt den aktuellen Status der Auffüllung der Nachweisdaten an.

- `NOT_STARTED` - Die Auffüllung hat noch nicht begonnen.
- `IN_PROGRESS` - Die Auffüllung ist im Gange. Dieser Vorgang dauert je nach Menge der Nachweisdaten bis zu sieben Tage.
- `COMPLETED` - Die Auffüllung ist abgeschlossen. All Ihre früheren Nachweise sind jetzt abfragbar.

Audit Manager API

Um den aktuellen Status der Evidence Finder mithilfe der API zu sehen

Rufen Sie die GetSettingsOperation auf, wobei der `attribute` Parameter auf gesetzt ist`EVIDENCE_FINDER_ENABLEMENT`. Dieses Verfahren gibt die folgenden Informationen zurück:

enablementStatus

Dieses Attribut zeigt den aktuellen Status der Beweissuche an.

- `ENABLE_IN_PROGRESS` - Sie haben die Aktivierung der Beweissuche angefordert. Ein Ereignisdatenspeicher wird derzeit erstellt, um Abfragen zur Nachweismittelsuche zu unterstützen.
- `ENABLED` - Der Ereignisdatenspeicher wurde erstellt und die Beweissuche ist aktiviert. Wir empfehlen, sieben Tage zu warten, bis der Ereignisdatenspeicher mit Ihren früheren Nachweisdaten aufgefüllt ist. In der Zwischenzeit können Sie die Beweissuche verwenden, aber nicht alle Daten sind verfügbar, bis die Datenspeicherung abgeschlossen ist.
- `DISABLE_IN_PROGRESS` - Sie haben die Deaktivierung der Beweissuche beantragt, Ihre Anfrage steht allerdings noch aus, bis der Ereignisdatenspeicher gelöscht wird.
- `DISABLED` - Sie haben die Beweissuche dauerhaft deaktiviert und der Ereignisdatenspeicher wird gelöscht. Nach diesem Zeitpunkt können Sie die Beweissuche nicht mehr reaktivieren.

backfillStatus

Dieses Attribut zeigt den aktuellen Status der Auffüllung der Nachweisdaten an.

- `NOT_STARTED` bedeutet, dass die Auffüllung noch nicht begonnen hat.
- `IN_PROGRESS` bedeutet, dass die Auffüllung im Gange ist. Dieser Vorgang dauert je nach Menge der Nachweisdaten bis zu sieben Tage.
- `COMPLETED` bedeutet, dass die Auffüllung abgeschlossen ist. All Ihre früheren Nachweise sind jetzt abfragbar.

Weitere Informationen finden Sie evidenceFinderEnablementin der Audit Manager API-Referenz.

Nächste Schritte

Nachdem der Evidence Finder erfolgreich aktiviert wurde, können Sie mit der Nutzung der Funktion beginnen. Wir empfehlen, sieben Tage zu warten, bis der Ereignisdatenspeicher mit Ihren früheren Nachweisdaten aufgefüllt ist. In der Zwischenzeit können Sie Evidence Finder verwenden, aber möglicherweise sind nicht alle Daten verfügbar, bis der Backfill abgeschlossen ist.

Informationen zu den ersten Schritten mit Evidence Finder finden Sie unterIm Evidence Finder nach Beweisen suchen.

Weitere Ressourcen

- Behebung von Problemen mit der Beweiserhebung

Beweissuche deaktivieren

Wenn Sie den Evidence Finder nicht mehr verwenden möchten, können Sie die Funktion jederzeit deaktivieren.

Folgen Sie diesen Schritten, um zu erfahren, wie Sie die Beweissuche deaktivieren können. Achten Sie genau auf die Voraussetzungen, da Sie spezielle Berechtigungen benötigen, um den Ereignisdatenspeicher in CloudTrail Lake zu löschen, der bei der Aktivierung von Evidence Finder erstellt wurde.

Voraussetzungen

Erforderliche Berechtigungen zur Deaktivierung der Beweissuche

Um Evidence Finder zu deaktivieren, benötigen Sie Berechtigungen zum Löschen eines Ereignisdatenspeichers in CloudTrail Lake. Eine Beispielrichtlinie, die Sie verwenden können, finden Sie unter Berechtigungen zur Deaktivierung der Beweissuche.

Wenn Sie Hilfe mit Berechtigungen benötigen, wenden Sie sich an Ihren AWS Administrator. Wenn Sie ein AWS Administrator sind, können Sie die erforderliche Berechtigungserklärung an eine IAM-Richtlinie anhängen.

Verfahren

Sie können diese Aufgabe mit der Audit Manager Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager Manager-API ausführen.

> **Warning**
>
> Durch das Deaktivieren der Evidence Finder wird der von Audit Manager erstellte CloudTrail Lake-Ereignisdatenspeicher gelöscht. Daher können Sie das Feature nicht erneut aktivieren. Um die Beweissuche nach der Deaktivierung erneut verwenden zu können, müssen Sie AWS Audit Manager deaktivieren und den Service anschließend vollständig wieder aktivieren.

Audit Manager console

So deaktivieren Sie den Evidence Finder auf der Audit Manager Manager-Konsole

1. Wählen Sie auf der Seite mit den Einstellungen von Audit Manager im Bereich Beweissuche die Option Deaktivieren aus.
2. Geben Sie in dem angezeigten Popup-Fenster **`Yes`** ein, um Ihre Entscheidung zu bestätigen.
3. Wählen Sie Anfrage zur Deaktivierung aus.

AWS CLI

Um den Evidence Finder im zu deaktivieren AWS CLI

Führen Sie den Befehl update-settings mit dem `--no-evidence-finder-enabled`-Parameter aus.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Um den Evidence Finder mithilfe der API zu deaktivieren

Rufen Sie die UpdateSettingsOperation auf und verwenden Sie den evidenceFinderEnabledParameter.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operation und dieses Parameters in einer der sprachspezifischen Sprachen AWS SDKs.

Weitere Ressourcen

- Behebung von Problemen mit der Beweiserhebung

Konfiguration Ihres Standardexportziels für Evidence Finder

Wenn Sie Abfragen im Evidence Finder ausführen, können Sie Ihre Suchergebnisse in eine Datei mit kommagetrennten Werten (CSV) exportieren. Verwenden Sie diese Einstellung, um den Standard-S3-Bucket auszuwählen, in dem Audit Manager Ihre exportierten Dateien speichert.

Voraussetzungen

Ihr S3-Bucket muss über die erforderlichen Berechtigungsrichtlinien verfügen, CloudTrail damit die Exportdateien in ihn geschrieben werden können. Genauer gesagt muss die Bucket-Richtlinie eine `s3:PutObject` Aktion und den Bucket-ARN enthalten und CloudTrail als Dienstprinzipal auflisten.

- Ein Beispiel für eine Berechtigungsrichtlinie, die Sie verwenden können, finden Sie unterBeispiele für ressourcenbasierte Richtlinien AWS Audit Manager.
- Anweisungen zum Anhängen dieser Richtlinie an Ihren S3-Bucket finden Sie unter Hinzufügen einer Bucket-Richtlinie mithilfe der Amazon S3 S3-Konsole.
- Weitere Tipps finden Sie auf dieser Seite unter Konfigurationstipps für Ihr Exportziel.

Konfigurationstipps für Ihr Exportziel

Um einen erfolgreichen Dateiexport zu gewährleisten, empfehlen wir Ihnen, die folgenden Konfigurationen für Ihr Exportziel zu überprüfen.

AWS-Region

Der AWS-Region Ihres vom Kunden verwalteten Schlüssels (falls Sie einen angegeben haben) muss der Region entsprechen, in der Sie Ihre Bewertung vorgenommen haben. Anweisungen zum Ändern Ihres KMS-Schlüssels finden Sie unter Datenverschlüsselungseinstellungen für Audit Manager.

Kontoübergreifende S3-Buckets

Die Verwendung eines kontoübergreifenden S3-Buckets als Exportziel wird in der Audit Manager-Konsole nicht unterstützt. Es ist möglich, einen kontenübergreifenden Bucket mit dem AWS CLI oder einem der beiden anzugeben AWS SDKs, aber der Einfachheit halber empfehlen wir, dies nicht zu tun. Wenn Sie sich dafür entscheiden, einen kontoübergreifenden S3-Bucket als Exportziel zu verwenden, sollten Sie die folgenden Punkte berücksichtigen.

- Standardmäßig gehören S3-Objekte — wie CSV-Exporte — demjenigen, der das Objekt hochlädt. AWS-Konto Sie können die Einstellung S3 Object Ownership verwenden, um dieses Standardverhalten so zu ändern, dass alle neuen Objekte, die von Konten mit der `bucket-owner-full-control` vordefinierten Zugriffssteuerungsliste (Access Control List, ACL) geschrieben werden, automatisch in den Besitz des Bucket-Eigentümers übergehen.

  Dies ist zwar keine Voraussetzung, wir empfehlen Ihnen jedoch, die folgenden Änderungen an Ihren kontoübergreifenden Bucket-Einstellungen vorzunehmen. Durch diese Änderungen wird sichergestellt, dass der Bucket-Besitzer die volle Kontrolle über die exportierten Dateien hat, die Sie in seinem Bucket veröffentlichen.

  - Setzen Sie den Objekteigentum des S3-Buckets auf Bucket Owner Preferred und nicht auf den standardmäßigen Objektschreiber
  - Fügen Sie eine Bucket-Richtlinie hinzu, um sicherzustellen, dass Objekte, die in diesen Bucket hochgeladen werden, den `bucket-owner-full-control` ACL haben
- Damit Audit Manager Dateien in einen kontoübergreifenden S3-Bucket exportieren kann, müssen Sie Ihrem Exportzielbucket die folgende S3-Bucket-Richtlinie hinzufügen. Ersetzen Sie *`placeholder text`* durch Ihre Informationen. Das `Principal`-Element in dieser Richtlinie ist der Benutzer oder die Rolle, die für die Bewertung verantwortlich ist und die die Bewertung innehat und exportiert. Der `Resource` gibt den kontoübergreifenden S3-Bucket an, in den die Datei exportiert wird.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Allow cross account file exports",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
```

```
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Verfahren

Sie können diese Einstellung mit der Audit Manager Manager-Konsole, der AWS Command Line Interface (AWS CLI) oder der Audit Manager Manager-API aktualisieren.

Audit Manager console

So aktualisieren Sie Ihre Exportzieleinstellungen in der Audit Manager Manager-Konsole

1. Gehen Sie auf der Registerkarte Einstellungen für die Beweissuche zum Abschnitt Exportziel.
2. Wählen Sie eine der folgenden Optionen:
   - Wenn Sie den aktuellen S3-Bucket entfernen möchten, wählen Sie Entfernen, um Ihre Einstellungen zu löschen.
   - Wenn Sie zum ersten Mal einen Standard-S3-Bucket speichern möchten, fahren Sie mit Schritt 3 fort.
3. Geben Sie den S3-Bucket an, in dem Sie Ihre exportierten Dateien speichern möchten.
   - Wählen Sie S3 durchsuchen, um aus einer Liste Ihrer Buckets auszuwählen.
   - Alternativ können Sie den Bucket-URI in diesem Format eingeben: **`s3://bucketname/prefix`**

> **Tip**
>
> Um Ihren Ziel-Bucket zu organisieren, können Sie einen optionalen Ordner für Ihre CSV-Exporte erstellen. Hängen Sie dazu einen Schrägstrich (**/**) und ein Präfix an den Wert im Feld Ressourcen-URI an (z. B. **/evidenceFinderCSVExports**). Audit Manager fügt dann dieses Präfix hinzu, wenn es die CSV-Datei zum Bucket hinzufügt, und Amazon S3 generiert den durch das Präfix angegebenen Pfad. Weitere Informationen zu Präfixen in Amazon S3 finden Sie unter Organisieren von Objekten in der Amazon S3-Konsole im Amazon Simple Storage Service-Benutzerhandbuch.

4. Klicken Sie abschließend auf Speichern.

Weitere Anleitungen zum Erstellen eines S3-Buckets finden Sie unter Erstellen eines Buckets im Benutzerhandbuch für Amazon S3.

AWS CLI

So aktualisieren Sie Ihre Exportzieleinstellungen in der AWS CLI

Führen Sie den Befehl update-settings aus und verwenden Sie den `--default-export-destination`-Parameter, um einen S3-Bucket anzugeben.

Ersetzen Sie im folgenden Beispiel die *`placeholder text`* durch Ihre eigenen Informationen:

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=amzn-s3-demo-destination-bucket
```

Anweisungen zum Erstellen eines S3-Buckets finden Sie unter create-bucket in der AWS CLI Befehlsreferenz.

Audit Manager API

Um Ihre Exportzieleinstellungen mithilfe der API zu aktualisieren

Rufen Sie den UpdateSettingsVorgang auf und verwenden Sie den defaultExportDestinationParameter, um einen S3-Bucket anzugeben.

Anweisungen zum Erstellen eines S3-Buckets finden Sie CreateBucketin der Amazon S3 S3-API-Referenz.

Benachrichtigungen in AWS Audit Manager

AWS Audit Manager kann Sie über Amazon Simple Notification Service (Amazon SNS) über Benutzeraktionen informieren.

Audit Manager sendet Benachrichtigungen, wenn eine der folgenden Situationen eintritt:

- Ein Audit-Verantwortlicher delegiert einen Kontrollsatz zur Überprüfung
- Ein Delegierter reicht einen überprüften Kontrollsatz an den Audit-Verantwortlichen zurück.
- Ein Audit-Verantwortlicher schließt die Prüfung eines Kontrollsatzes ab.

Weitere Ressourcen

- Informationen zur Konfiguration Ihrer Benachrichtigungen in Audit Manager finden Sie unterKonfiguration Ihrer Audit Manager Manager-Benachrichtigungen.
- Antworten auf häufig gestellte Fragen und Probleme finden Sie Fehlerbehebung bei Benachrichtigungsproblemen im Abschnitt zur Fehlerbehebung in diesem Handbuch.

Behebung häufig auftretender Probleme in AWS Audit Manager

Während der Nutzung AWS Audit Manager können Sie auf bestimmte Probleme oder Herausforderungen stoßen, die behoben werden müssen. Ganz gleich, ob Sie Probleme bei der Einrichtung von Bewertungen, der Erfassung von Nachweisen oder einem anderen Aspekt des Services haben, in diesem Leitfaden zur Fehlerbehebung finden Sie unsere Empfehlungen, mit denen Sie häufig auftretende Probleme schnell und effizient lösen können.

Wir empfehlen Ihnen, die folgende Themenliste zu lesen, das am besten zu Ihrem Szenario passt, und die bereitgestellten Anleitungen zu befolgen, um wieder auf den richtigen Weg zu kommen. Wenn Sie die angegebenen Schritte zur Fehlerbehebung befolgen, können Sie das Problem wahrscheinlich selbstständig lösen und weiterhin alle Funktionen von Audit Manager nutzen. Wenn Ihr spezielles Problem hier jedoch nicht behandelt wird oder Sie es nicht lösen können, nachdem Sie die empfohlenen Schritte befolgt haben, empfehlen wir Ihnen, sich an uns zu wenden, um weitere SupportUnterstützung zu erhalten.

Themen

Fehlersuche bei der Bewertung und Beweiserhebung

Mithilfe der Informationen auf dieser Seite können Sie häufig auftretende Probleme mit der Bewertung und Beweiserhebung in Audit Manager lösen.

Probleme bei der Beweiserhebung

Probleme mit der Bewertung

Ich habe eine Bewertung erstellt, sehe aber noch keine Beweise

Wenn Sie keine Beweise sehen können, haben Sie wahrscheinlich entweder nicht mindestens 24 Stunden gewartet, nachdem Sie die Bewertung erstellt haben, oder es liegt ein Konfigurationsfehler vor.

Wir empfehlen Folgendes:

1. Vergewissern Sie sich, dass seit der Erstellung der Bewertung 24 Stunden vergangen sind. Automatisierte Beweise werden erst 24 Stunden nach Erstellung der Bewertung verfügbar.
2. Stellen Sie sicher, dass Sie Audit Manager in der gleichen AWS-Region AWS-Service Weise verwenden, für die Sie Beweise erwarten.
3. Wenn Sie erwarten, dass von AWS Config und Beweise für Konformitätsprüfungen angezeigt werden AWS Security Hub CSPM, stellen Sie sicher, dass sowohl auf der AWS Config Security Hub CSPM-Konsole als auch auf der Security Hub CSPM-Konsole Ergebnisse für diese Prüfungen angezeigt werden. Die AWS Config CSPM-Ergebnisse von Security Hub sollten in derselben Form angezeigt werden AWS-Region , in der Sie Audit Manager verwenden.

Wenn Sie immer noch keine Beweise in Ihrer Bewertung sehen können und dies nicht auf eines dieser Probleme zurückzuführen ist, überprüfen Sie die anderen möglichen Ursachen, die auf dieser Seite beschrieben werden.

Meine Bewertung bezieht sich nicht auf die Erfassung von Nachweisen zur Konformitätsprüfung von AWS Security Hub CSPM

Wenn Sie für eine AWS Security Hub CSPM Kontrolle keine Nachweise zur Konformitätsprüfung finden, kann dies an einem der folgenden Probleme liegen.

Fehlende Konfiguration in AWS Security Hub CSPM

Dieses Problem kann auftreten, wenn Sie bei der Aktivierung von AWS Security Hub CSPM einige Konfigurationsschritte übersprungen haben.

Um dieses Problem zu beheben, stellen Sie sicher, dass Sie Security Hub CSPM mit den erforderlichen Einstellungen für Audit Manager aktiviert haben. Detaillierte Anweisungen finden Sie unter Aktivieren und einrichten AWS Security Hub CSPM.

Der Name eines Security Hub-CSPM-Steuerelements wurde falsch in Ihrem **`ControlMappingSource`**

Wenn Sie die Audit Manager Manager-API verwenden, um ein benutzerdefiniertes Steuerelement zu erstellen, können Sie ein Security Hub CSPM-Steuerelement als Datenquellenzuordnung für die Beweiserhebung angeben. Dazu geben Sie eine Kontroll-ID als `keywordValue` ein.

Wenn Sie keine Nachweise zur Konformitätsprüfung für ein Security Hub CSPM-Steuerelement sehen, kann es sein, dass das in Ihrem falsch eingegeben `keywordValue` wurde. `ControlMappingSource` Bei der Angabe der `keywordValue` ist die Groß- und Kleinschreibung zu beachten. Wenn Sie sie falsch eingeben, erkennt Audit Manager diese Regel möglicherweise nicht. Deshalb ist es möglich, dass Sie nicht wie erwartet Beweise zur Konformitätsprüfung für diese Kontrolle sammeln.

Um dieses Problem zu beheben, aktualisieren Sie die benutzerdefinierte Kontrolle und überarbeiten Sie das `keywordValue`. Das korrekte Format eines Security Hub CSPM-Schlüsselworts ist unterschiedlich. Informationen zur Genauigkeit finden Sie in der Liste von. Unterstützte Security Hub CSPM-Steuerelemente

`AuditManagerSecurityHubFindingsReceiver` EventBridge Amazon-Regel fehlt

Wenn Sie Audit Manager aktivieren, `AuditManagerSecurityHubFindingsReceiver` wird automatisch eine Regel mit dem Namen erstellt und in Amazon aktiviert EventBridge. Diese Regel ermöglicht es Audit Manager, die Ergebnisse des Security Hub CSPM als Beweismittel zu sammeln.

Wenn diese Regel in dem Bereich, in AWS-Region dem Sie Security Hub CSPM verwenden, nicht aufgeführt und aktiviert ist, kann Audit Manager keine Security Hub-CSPM-Ergebnisse für diese Region sammeln.

Um dieses Problem zu beheben, rufen Sie die EventBridge Konsole auf und vergewissern Sie sich, dass die `AuditManagerSecurityHubFindingsReceiver` Regel in Ihrem System existiert. AWS-Konto Wenn die Regel nicht existiert, empfehlen wir, Audit Manager zu deaktivieren und den Dienst danach erneut zu aktivieren. Wenn das Problem durch diese Aktion nicht behoben wird oder die Deaktivierung von Audit Manager keine Option ist, wenden Sie sich an Support, um Unterstützung zu erhalten.

Von Security Hub CSPM erstellte dienstbezogene AWS Config Regeln

Denken Sie daran, dass Audit Manager keine Beweise anhand der serviceverknüpften AWS Config Regeln sammelt, die Security Hub CSPM erstellt. Dies ist eine bestimmte Art von verwalteter AWS Config Regel, die vom Security Hub CSPM-Dienst aktiviert und gesteuert wird. Security Hub CSPM erstellt Instanzen dieser serviceverknüpften Regeln in Ihrer AWS Umgebung, auch wenn bereits andere Instanzen derselben Regeln existieren. Um doppelte Beweise zu verhindern, unterstützt Audit Manager daher die Erfassung von Beweisen anhand der servicebezogenen Regeln nicht.

Ich habe eine Sicherheitskontrolle in Security Hub CSPM deaktiviert. Sammelt Audit Manager Nachweise zur Konformitätsprüfung für diese Sicherheitskontrolle?

Audit Manager sammelt keine Beweise für deaktivierte Sicherheitskontrollen.

Wenn Sie den Status einer Sicherheitskontrolle in Security Hub CSPM auf deaktiviert setzen, werden für diese Kontrolle im aktuellen Konto und in der Region keine Sicherheitsprüfungen durchgeführt. Daher sind in Security Hub CSPM keine Sicherheitsfeststellungen verfügbar, und Audit Manager sammelt keine diesbezüglichen Nachweise.

Indem der Deaktivierungsstatus, den Sie in Security Hub CSPM festgelegt haben, respektiert, stellt Audit Manager sicher, dass Ihre Bewertung die aktiven Sicherheitskontrollen und Ergebnisse, die für Ihre Umgebung relevant sind, korrekt widerspiegelt, mit Ausnahme von Kontrollen, die Sie absichtlich deaktiviert haben.

Ich habe den Status eines Ergebnisses **`Suppressed`** in Security Hub CSPM auf gesetzt. Sammelt Audit Manager Beweise für die Konformitätsprüfung zu diesem Ergebnis?

Audit Manager sammelt Beweise für Sicherheitskontrollen, die Ergebnisse unterdrückt haben.

Wenn Sie den Workflow-Status eines Ergebnisses in Security Hub CSPM auf Unterdrückt setzen, bedeutet dies, dass Sie das Ergebnis überprüft haben und nicht der Meinung sind, dass Maßnahmen erforderlich sind. In Audit Manager werden diese unterdrückten Ergebnisse als Beweismittel gesammelt und Ihrer Bewertung beigefügt. Die Nachweisdetails zeigen den Bewertungsstatus, der direkt vom Security Hub CSPM `SUPPRESSED` gemeldet wurde.

Dieser Ansatz stellt sicher, dass Ihre Audit Manager Manager-Bewertung die Ergebnisse von Security Hub CSPM korrekt wiedergibt, und bietet gleichzeitig Einblick in alle unterdrückten Ergebnisse, die möglicherweise einer weiteren Überprüfung oder Berücksichtigung im Rahmen eines Audits bedürfen.

Bei meiner Bewertung werden keine Nachweise zur Konformitätsprüfung gesammelt von AWS Config

Wenn Sie für eine AWS Config Regel keine Nachweise zur Konformitätsprüfung finden, kann dies an einem der folgenden Probleme liegen.

Die Regel-ID wurde falsch in Ihr **`ControlMappingSource`** eingegeben

Wenn Sie die Audit Manager Manager-API verwenden, um ein benutzerdefiniertes Steuerelement zu erstellen, können Sie eine AWS Config Regel als Datenquellenzuordnung für die Beweiserhebung angeben. Der `keywordValue`, den Sie angeben, hängt vom Typ der Regel ab.

Wenn Sie keine Nachweise für die Konformitätsprüfung für eine AWS Config Regel sehen, kann es sein, dass die Regel falsch in Ihre Regel eingegeben `keywordValue` wurde`ControlMappingSource`. Bei der Angabe der `keywordValue` ist die Groß- und Kleinschreibung zu beachten. Wenn Sie sie falsch eingeben, erkennt Audit Manager die Regel möglicherweise nicht. Infolgedessen können Sie möglicherweise nicht wie vorgesehen Beweise für die Prüfung der Einhaltung dieser Regel sammeln.

Um dieses Problem zu beheben, aktualisieren Sie die benutzerdefinierte Kontrolle und überarbeiten Sie das `keywordValue`.

- Stellen Sie bei benutzerdefinierten Regeln sicher, dass im `keywordValue` das `Custom_`-Präfix gefolgt vom Namen der benutzerdefinierten Regel steht. Das Format des Namens der benutzerdefinierten Regel kann variieren. Überprüfen Sie die Namen Ihrer benutzerdefinierten Regeln in der AWS Config -Konsole, um seine Richtigkeit zu überprüfen.
- Stellen Sie bei verwalteten Regeln sicher, dass das `keywordValue` die Regel-ID in `ALL_CAPS_WITH_UNDERSCORES` ist. Beispiel, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Informationen zur Genauigkeit finden Sie in der Liste der unterstützten Schlüsselwörter für verwaltete Regeln.

> **Note**
>
> Bei einigen verwalteten Regeln unterscheidet sich die Regel-ID vom Regelnamen. Die Regel-ID für restricted-ssh lautet beispielsweise `INCOMING_SSH_DISABLED`. Stellen Sie sicher, dass Sie die Regel-ID verwenden, nicht den Regelnamen. Um eine Regel-ID zu finden, wählen Sie eine Regel aus der Liste der verwalteten Regeln aus und suchen Sie nach ihrem Identifikationswert.

Bei der Regel handelt es sich um eine servicebezogene AWS Config -Regel

Als Datenquellenzuordnung für die Beweiserhebung können Sie verwaltete Regeln und benutzerdefinierte Regeln verwenden. Audit Manager sammelt jedoch keine Beweise aus den meisten servicebezogenen Regeln.

Es gibt nur zwei Arten von servicebezogenen Regeln, anhand derer Audit Manager Beweise sammelt:

- Servicebezogene Regeln von Conformance Packs
- Mit Diensten verknüpfte Regeln von AWS Organizations

Audit Manager sammelt keine Beweise aus anderen servicebezogenen Regeln, insbesondere aus Regeln mit einem Amazon-Ressourcennamen (ARN), der das Präfix `arn:aws:config:*:*:config-rule/aws-service-rule/...` enthält.

Der Grund dafür, dass Audit Manager keine Beweise aus den meisten servicebezogenen AWS Config -Regeln sammelt, besteht darin, doppelte Beweise in Ihren Bewertungen zu vermeiden. Eine dienstgebundene Regel ist eine bestimmte Art von verwalteter Regel, die es anderen ermöglicht, AWS Config Regeln in Ihrem Konto AWS-Services zu erstellen. Beispielsweise verwenden einige Security Hub CSPM-Steuerelemente eine AWS Config serviceverknüpfte Regel, um Sicherheitsüberprüfungen durchzuführen. Für jedes Security Hub CSPM-Steuerelement, das eine serviceverknüpfte AWS Config Regel verwendet, erstellt Security Hub CSPM eine Instanz der erforderlichen AWS Config Regel in Ihrer Umgebung. AWS Dies geschieht auch dann, wenn die ursprüngliche Regel bereits in Ihrem Konto vorhanden ist. Um zu vermeiden, dass dieselben Beweise aus derselben Regel zweimal gesammelt werden, ignoriert Audit Manager daher die servicebezogene Regel und sammelt keine Beweise von ihr.

AWS Config ist nicht aktiviert

AWS Config muss in Ihrem aktiviert sein AWS-Konto. Nachdem Sie die Einrichtung auf diese AWS Config Weise vorgenommen haben, sammelt Audit Manager bei jeder Auswertung einer AWS Config Regel Nachweise. Stellen Sie sicher, dass Sie Ihre aktiviert AWS Config haben AWS-Konto. Anweisungen finden Sie unter Aktivieren und einrichten AWS Config.

Die AWS Config Regel hat eine Ressourcenkonfiguration bewertet, bevor Sie Ihre Bewertung eingerichtet haben

Wenn Ihre AWS Config Regel so eingerichtet ist, dass sie Konfigurationsänderungen für eine bestimmte Ressource auswertet, stellen Sie möglicherweise fest, dass die Bewertung in AWS Config und die Nachweise in Audit Manager nicht übereinstimmen. Dies ist der Fall, wenn die Regelauswertung stattgefunden hat, bevor Sie die Kontrolle in Ihrer Audit Manager-Bewertung eingerichtet haben. In diesem Fall generiert Audit Manager keine Beweise, bis die zugrunde liegende Ressource ihren Status erneut ändert und eine Neubewertung der Regel auslöst.

Um das Problem zu umgehen, können Sie in der AWS Config Konsole zu der Regel navigieren und die Regel manuell neu bewerten. Dadurch wird eine neue Bewertung aller Ressourcen veranlasst, die zu dieser Regel gehören.

In meiner Bewertung werden von AWS CloudTrail keine Beweise für Benutzeraktivitäten gesammelt

Wenn Sie die Audit Manager Manager-API verwenden, um ein benutzerdefiniertes Steuerelement zu erstellen, können Sie einen CloudTrail Ereignisnamen als Datenquellenzuordnung für die Beweiserhebung angeben. Geben Sie dazu den Namen des Ereignisses als den `keywordValue` ein.

Wenn Sie keine Belege für Benutzeraktivitäten für ein CloudTrail Ereignis sehen, kann es sein, dass das Ereignis falsch eingegeben `keywordValue` wurde`ControlMappingSource`. Bei der Angabe der `keywordValue` ist die Groß- und Kleinschreibung zu beachten. Wenn Sie sie falsch eingeben, erkennt Audit Manager den Ereignisnamen möglicherweise nicht. Infolgedessen sammeln Sie möglicherweise nicht wie geplant Beweise über Benutzeraktivitäten für dieses Ereignis.

Um dieses Problem zu beheben, aktualisieren Sie die benutzerdefinierte Kontrolle und überarbeiten Sie das `keywordValue`. Stellen Sie sicher, dass das Ereignis als `serviceprefix_ActionName` ausgewiesen ist. Beispiel, `cloudtrail_StartLogging`. Überprüfen Sie das AWS-Service -Präfix auf Richtigkeit und die Aktionsnamen in der Dienstberechtigungsreferenz.

In meiner Bewertung werden keine Beweise für Konfigurationsdaten für einen AWS API-Aufruf gesammelt

Wenn Sie die Audit Manager Manager-API verwenden, um ein benutzerdefiniertes Steuerelement zu erstellen, können Sie einen AWS API-Aufruf als Datenquellenzuordnung für die Beweiserhebung angeben. Geben Sie dazu den API-Aufruf als den `keywordValue` ein.

Wenn Sie keine Beweise für Konfigurationsdaten für einen AWS API-Aufruf sehen, könnte es sein, dass der in Ihrem falsch eingegeben `keywordValue` wurde`ControlMappingSource`. Bei der Angabe der `keywordValue` ist die Groß- und Kleinschreibung zu beachten. Wenn Sie sie falsch eingeben, erkennt Audit Manager den API-Aufruf möglicherweise nicht. Dies kann dazu führen, dass Sie die Konfigurationsdaten für diesen API-Aufruf nicht wie vorgesehen erfassen.

Um dieses Problem zu beheben, aktualisieren Sie die benutzerdefinierte Kontrolle und überarbeiten Sie das `keywordValue`. Stellen Sie sicher, dass der API-Aufruf als `serviceprefix_ActionName`

ausgewiesen ist. Beispiel, `iam_ListGroups`. Informationen zur Genauigkeit finden Sie in der Liste vonAWS API-Aufrufe werden unterstützt von AWS Audit Manager.

Eine übliche Kontrolle besteht darin, keine automatisierten Beweise zu sammeln

Wenn Sie eine gemeinsame Kontrolle überprüfen, wird Ihnen möglicherweise die folgende Meldung angezeigt: Diese gemeinsame Kontrolle sammelt keine automatisierten Beweise aus zentralen Kontrollen.

Das bedeutet, dass derzeit keine AWS verwalteten Beweisquellen diese gemeinsame Kontrolle unterstützen können. Daher ist die Registerkarte Evidenzquellen leer und es werden keine zentralen Steuerelemente angezeigt.

Wenn eine gemeinsame Kontrolle keine automatisierten Beweise sammelt, wird sie als manuelle gemeinsame Kontrolle bezeichnet. Manuelle gemeinsame Kontrollen erfordern in der Regel die Bereitstellung physischer Aufzeichnungen und Signaturen oder von Informationen über Ereignisse, die außerhalb Ihrer AWS Umgebung auftreten. Aus diesem Grund gibt es oft keine AWS Datenquellen, die Belege für die Erfüllung der Kontrollanforderungen liefern könnten.

Wenn es sich bei einem häufig verwendeten Steuerelement um ein manuelles Steuerelement handelt, können Sie es dennoch als Beweisquelle für ein benutzerdefiniertes Steuerelement verwenden. Der einzige Unterschied besteht darin, dass das gemeinsame Steuerelement nicht automatisch Beweise sammelt. Stattdessen müssen Sie Ihre eigenen Beweise manuell hochladen, um die Anforderungen der gemeinsamen Kontrolle zu erfüllen.

Um Nachweise zu einer manuellen gemeinsamen Kontrolle hinzuzufügen

1. Erstellen Sie ein benutzerdefiniertes Steuerelement
   - Folgen Sie den Schritten, um ein benutzerdefiniertes Steuerelement zu erstellen oder zu bearbeiten.
   - Wenn Sie in Schritt 2 Beweisquellen angeben, wählen Sie das manuelle Common Control als Beweisquelle aus.
2. Erstellen Sie ein benutzerdefiniertes Framework
   - Folgen Sie den Schritten, um ein benutzerdefiniertes Framework zu erstellen oder zu bearbeiten.
   - Wenn Sie in Schritt 2 einen Steuersatz angeben, fügen Sie Ihr neues benutzerdefiniertes Steuerelement hinzu.

3. Erstellen Sie eine Bewertung
   - Folgen Sie den Schritten, um eine Bewertung aus Ihrem benutzerdefinierten Framework zu erstellen.
   - Zu diesem Zeitpunkt ist die manuelle gemeinsame Kontrolle nun eine Evidenzquelle für eine aktive Bewertungskontrolle.
4. Laden Sie manuelle Beweise hoch
   - Folgen Sie den Schritten, um der Kontrolle in Ihrer Bewertung manuelle Nachweise hinzuzufügen.

> **Note**
>
> Da in AWS future mehr Datenquellen verfügbar werden, ist es möglich, dass die AWS gemeinsame Kontrolle aktualisiert wird, sodass Kernkontrollen als Beweisquellen aufgenommen werden. In diesem Fall profitieren Sie automatisch von diesen Aktualisierungen, wenn es sich bei der gemeinsamen Kontrolle um eine Evidenzquelle in einer oder mehreren Ihrer aktiven Bewertungskontrollen handelt. Es ist keine weitere Einrichtung Ihrerseits erforderlich, und Sie beginnen mit der automatischen Erfassung von Nachweisen, die die gemeinsame Kontrolle unterstützen.

Meine Beweise werden in unterschiedlichen Intervallen generiert, und ich bin mir nicht sicher, wie oft sie gesammelt werden.

Die Kontrollen in Audit Manager-Bewertungen sind verschiedenen Datenquellen zugeordnet. Jede Datenquelle verfügt über eine andere Häufigkeit der Datenerfassung. Daher gibt es keine one-size-fits-all Antwort darauf, wie oft Beweise gesammelt werden. Einige Datenquellen bewerten die Einhaltung der Vorschriften, während andere nur Daten zum Ressourcenstatus und zu Änderungen erfassen, ohne dass eine Konformitätsfeststellung vorliegt.

Im Folgenden finden Sie eine Zusammenfassung der verschiedenen Datenquellentypen und der Häufigkeit, mit der sie Beweise sammeln.

Datenquellentyp	Description	Häufigkeit der Beweissuche	Wenn diese Kontrolle in einer Bewertung aktiv ist
AWS CloudTrail	Verfolgt eine bestimmte Benutzeraktivität.	Kontinuierlich	Audit Manager filtert Ihre CloudTrail Protokolle anhand des von Ihnen ausgewählten Schlüsselworts. Die verarbeiteten Protokolle werden als Beweis für Benutzeraktivitäten importiert.
AWS Security Hub CSPM	Erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem Ergebnisse aus Security Hub CSPM gemeldet werden.	Basierend auf dem Zeitplan der Security Hub CSPM-Überprüfung (in der Regel etwa alle 12 Stunden)	Audit Manager ruft das Sicherheitsergebnis direkt vom Security Hub CSPM ab. Das Ergebnis wird als Beweis für die Konformitätsprüfung importiert.
AWS Config	Erfasst einen Überblick über die Sicherheitslage Ihrer Ressourcen, indem die Ergebnisse von gemeldet werden. AWS Config	Basierend auf den Einstellungen, die in der AWS Config Regel definiert sind	Audit Manager ruft die Regelauswertung direkt von ab AWS Config. Die Bewertung wird als Beweis für die Konformitätsprüfung importiert.
AWS API-Aufrufe	Erstellt einen Snapshot Ihrer Ressourcenkonfiguration direkt über einen API-Aufruf	Täglich, wöchentlich oder monatlich	Audit Manager führt den API-Aufruf auf der Grundlage der von Ihnen angegebenen Häufigkeit durch. Die Antwort wird als Beweis für Konfigurationsdaten importiert.

Datenquellentyp	Description	Häufigkeit der Beweissuche	Wenn diese Kontrolle in einer Bewertung aktiv ist
	an die angegebene Ressource AWS-Service.		

Unabhängig von der Häufigkeit der Beweiserhebung werden neue Beweise automatisch gesammelt, solange die Bewertung aktiv ist. Weitere Informationen finden Sie unter Häufigkeit der Beweissuche.

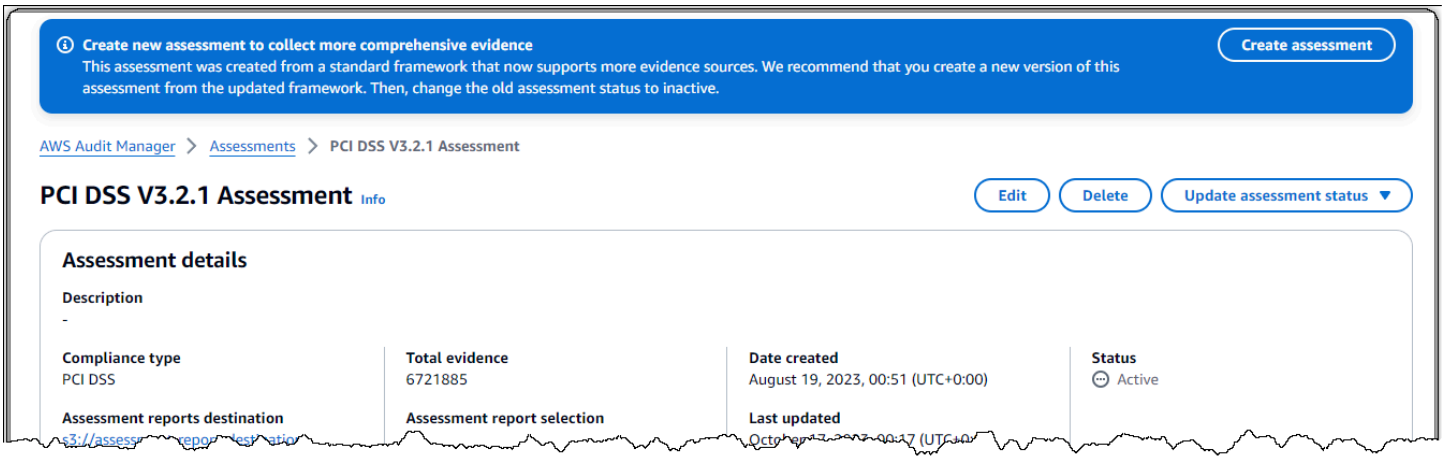
Weitere Informationen hierzu finden Sie unter Unterstützte Datenquellentypen für automatisierte Beweise und Ändern der Häufigkeit, mit der eine Kontrolle Beweise sammelt.

Ich habe Audit Manager deaktiviert und dann wieder aktiviert, und jetzt sammeln meine bereits vorhandenen Bewertungen keine Beweise mehr

Wenn Sie Audit Manager deaktivieren und sich dafür entscheiden, Ihre Daten nicht zu löschen, gehen Ihre vorhandenen Bewertungen in einen Ruhezustand über und es werden keine Beweise mehr gesammelt. Das bedeutet, dass die Bewertungen, die Sie zuvor erstellt haben, weiterhin verfügbar sind, wenn Sie Audit Manager erneut aktivieren. Sie setzen die Beweiserhebung jedoch nicht automatisch fort.

Um erneut mit der Erfassung von Nachweisen für eine bereits bestehende Bewertung zu beginnen, bearbeiten Sie die Bewertung und wählen Sie Speichern, ohne Änderungen vorzunehmen.

Auf meiner Seite mit den Bewertungsdetails werde ich aufgefordert, meine Bewertung erneut zu erstellen



Wenn Sie die Meldung Neue Bewertung erstellen, um umfassendere Nachweise zu sammeln, sehen, bedeutet dies, dass Audit Manager jetzt eine neue Definition des Standardrahmens bereitstellt, auf dessen Grundlage Ihre Bewertung erstellt wurde.

In der neuen Rahmendefinition können nun alle Standardkontrollen des Frameworks Nachweise aus AWS verwalteten Quellen sammeln. Das bedeutet, dass Audit Manager jedes Mal, wenn die zugrunde liegenden Datenquellen für eine gemeinsame oder zentrale Kontrolle aktualisiert werden, dieselbe Aktualisierung automatisch auf alle zugehörigen Standardkontrollen anwendet.

Um von diesen AWS verwalteten Quellen zu profitieren, empfehlen wir Ihnen, anhand des aktualisierten Frameworks eine neue Bewertung zu erstellen. Nachdem Sie dies getan haben, können Sie den alten Bewertungsstatus in inaktiv ändern. Diese Maßnahme trägt dazu bei, dass bei Ihrer neuen Bewertung die genauesten und umfassendsten Nachweise erfasst werden, die aus AWS verwalteten Quellen verfügbar sind. Wenn Sie keine Maßnahmen ergreifen, verwendet Ihre Bewertung weiterhin die alten Rahmen- und Kontrolldefinitionen, um Beweise genau wie zuvor zu sammeln.

Was ist der Unterschied zwischen einer Datenquelle und einer Evidenzquelle?

Eine Evidenzquelle bestimmt, woher Beweise gesammelt werden. Dabei kann es sich um eine einzelne Datenquelle oder um eine vordefinierte Gruppierung von Datenquellen handeln, die einem zentralen Steuerelement oder einem gemeinsamen Steuerelement zugeordnet ist.

Eine Datenquelle ist die detaillierteste Art von Beweisquelle. Eine Datenquelle enthält die folgenden Details, die Audit Manager darüber informieren, wo genau Beweisdaten gesammelt werden sollen:

- Datenquellentyp (zum Beispiel AWS Config)
- Datenquellenzuordnung (z. B. eine bestimmte AWS Config Regel wies`3-bucket-public-write-prohibited`)

Meine Bewertung konnte nicht erstellt werden

Wenn die Erstellung Ihrer Bewertung fehlschlägt, kann dies an einem der folgenden Probleme liegen.

Sie haben AWS-Konten in Ihrem Bewertungsbereich zu viele ausgewählt

Wenn Sie verwenden AWS Organizations, kann Audit Manager bis zu 200 Mitgliedskonten im Rahmen einer einzigen Bewertung unterstützen. Wenn Sie diese Anzahl überschreiten, schlägt die Erstellung der Bewertung fehl.

Um dieses Problem zu umgehen, können Sie für jede Bewertung mehrere Bewertungen mit unterschiedlichen Konten und bis zu 250 eindeutigen Mitgliedskonten für alle Bewertungen durchführen.

Ein Konto in Ihrem Geltungsbereich wird bereits im Rahmen eines anderen aktiven Assessments bewertet

Wenn Sie versuchen, eine Bewertung zu erstellen, die ein Konto umfasst, das bereits für eine andere aktive Bewertung gilt, schlägt die Erstellung der Bewertung fehl. Dies kann passieren, wenn mehrere Teams oder Organisationen versuchen, dasselbe Konto gleichzeitig zu bewerten.

Möglicherweise wird eine Fehlermeldung ähnlich der folgenden angezeigt:`Scope: AWS Account [account-id] has assessments in progress`.

Um dieses Problem zu beheben, können Sie eine der folgenden Maßnahmen ergreifen:

- Abstimmung mit anderen Teams — Erkundigen Sie sich bei anderen Teams in Ihrer Organisation, welche Assessments derzeit das betreffende Konto verwenden. Sie können sich dann abstimmen, um zu vermeiden, dass sich die Prüfungsumfänge überschneiden.
- Ändern Sie Ihren Bewertungsbereich — Entfernen Sie das widersprüchliche Konto aus Ihrem Bewertungsbereich und erstellen Sie die Bewertung mit den verbleibenden Konten. Sie können das widersprüchliche Konto separat bewerten, sobald die andere Bewertung abgeschlossen ist.

- Warten Sie, bis die andere Bewertung abgeschlossen ist — Wenn die andere Bewertung nur vorübergehend ist oder kurz vor dem Abschluss steht, können Sie warten, bis sie abgeschlossen ist, bevor Sie Ihre Bewertung mit dem gewünschten Umfang erstellen.

> **Note**
>
> Durch diese Einschränkung wird sichergestellt, dass es bei der Erfassung von Nachweisen nicht zu Konflikten zwischen mehreren Bewertungen kommt und dass die Prüfungsergebnisse korrekt und konsistent bleiben.

Was passiert, wenn ich ein in den Bewertungsumfang fallendes Konto aus meiner Organisation entferne?

Wenn ein in den Geltungsbereich fallender Account aus Ihrer Organisation entfernt wird, sammelt Audit Manager keine Belege mehr für dieses Konto und es wird aus allen Prüfungen entfernt, bei denen das Konto in den Geltungsbereich fällt. Wenn Sie ein Mitgliedskonto aus allen Bewertungen entfernen, wird auch die Gesamtzahl der einzelnen Konten im Geltungsbereich reduziert, sodass Sie ein neues Konto aus Ihrer Organisation hinzufügen können.

Ich kann nicht sehen, welche Dienste in den Geltungsbereich meiner Bewertung fallen

Wenn Sie die AWS-ServicesRegisterkarte nicht sehen, bedeutet dies, dass die im Leistungsumfang enthaltenen Dienste von Audit Manager für Sie verwaltet werden. Wenn Sie eine neue Bewertung erstellen, verwaltet Audit Manager ab diesem Zeitpunkt die im Leistungsumfang enthaltenen Dienstleistungen für Sie.

Wenn Sie eine ältere Bewertung haben, ist es möglich, dass Sie diese Registerkarte schon einmal in Ihrer Bewertung gesehen haben. Audit Manager entfernt diese Registerkarte jedoch automatisch aus Ihrer Bewertung und übernimmt die Verwaltung der Services im Umfang, wenn eines der folgenden Ereignisse eintritt:

- Sie bearbeiten Ihre Bewertung
- Sie bearbeiten eines der benutzerdefinierten Steuerelemente, die in Ihrer Bewertung verwendet werden

Audit Manager leitet den Umfang der Services ab, indem er Ihre Bewertungskontrollen und deren Datenquellen untersucht und diese Informationen dann den entsprechenden AWS-Services zuordnet. Wenn sich eine zugrunde liegende Datenquelle für Ihre Bewertung ändert, aktualisieren wir den Umfang bei Bedarf automatisch, um die richtigen Services widerzuspiegeln. Auf diese Weise wird sichergestellt, dass bei Ihrer Bewertung genaue und umfassende Daten zu allen relevanten Services in Ihrer AWS Umgebung gesammelt werden.

Ich kann die Services, die für meine Bewertung gelten, nicht bearbeiten

Der Eine Bewertung bearbeiten in AWS Audit Manager Workflow verfügt nicht mehr über den Schritt Dienste bearbeiten. Dies liegt daran, dass Audit Manager jetzt verwaltet, welche Bereiche von Ihrer Bewertung betroffen AWS-Services sind.

Wenn Sie über eine ältere Bewertung verfügen, ist es möglich, dass Sie bei der Erstellung der Bewertung die Services im Umfang manuell definiert haben. Sie können diese Dienste jedoch in Zukunft nicht mehr bearbeiten. Audit Manager übernimmt automatisch die Verwaltung der Dienstleistungen, die für Ihre Bewertung vorgesehen sind, wenn eines der folgenden Ereignisse eintritt:

- Sie bearbeiten Ihre Bewertung
- Sie bearbeiten eines der benutzerdefinierten Steuerelemente, die in Ihrer Bewertung verwendet werden

Audit Manager leitet den Umfang der Services ab, indem er Ihre Bewertungskontrollen und deren Datenquellen untersucht und diese Informationen dann den entsprechenden AWS-Services zuordnet. Wenn sich eine zugrunde liegende Datenquelle für Ihre Bewertung ändert, aktualisieren wir den Umfang bei Bedarf automatisch, um die richtigen Services widerzuspiegeln. Auf diese Weise wird sichergestellt, dass bei Ihrer Bewertung genaue und umfassende Daten zu allen relevanten Services in Ihrer AWS Umgebung gesammelt werden.

Was ist der Unterschied zwischen einem Service im Umfang und einem Datenquellentyp?

A service in scope ist ein AWS-Service Wert, der im Umfang Ihrer Bewertung enthalten ist. Wenn ein Service in den Bewertungsumfang fällt, sammelt Audit Manager Beweise über Ihre Nutzung dieses Dienstes und seiner Ressourcen.

> **Note**
>
> Der Audit Manager verwaltet, AWS-Services welche Punkte für Ihre Bewertungen gelten. Wenn Sie ein älteres Assessment haben, ist es möglich, dass Sie die in den Geltungsbereich fallenden Services in der Vergangenheit manuell festgelegt haben. In Zukunft können Sie die Services nicht mehr im Gültigkeitsbereich spezifizieren oder bearbeiten.

Ein Datenquellentyp gibt an, woher genau die Beweise gesammelt werden. Wenn Sie Ihre eigenen Beweise hochladen, ist der Datenquellentyp Manuell. Wenn Audit Manager die Beweise sammelt, kann es sich bei der Datenquelle um einen der folgenden vier Typen handeln:

1. AWS Security Hub CSPM — Erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem Ergebnisse aus Security Hub CSPM gemeldet werden.
2. AWS Config — Erfasst anhand von Berichten über die Ergebnisse von eine Momentaufnahme Ihrer Ressourcensicherheit. AWS Config
3. AWS CloudTrail — Verfolgt eine bestimmte Benutzeraktivität für eine Ressource.
4. AWS API-Aufrufe — Erstellt einen Snapshot Ihrer Ressourcenkonfiguration direkt über einen API-Aufruf an eine bestimmte Ressource AWS-Service.

Im Folgenden sind zwei Beispiele, die den Unterschied zwischen einem Service im Bewertungsumfang und einem Datenquellentyp verdeutlichen.

Beispiel 1

Nehmen wir an, Sie möchten Beweise für eine Kontrolle mit dem Namen 4.1.2 – Öffentlichen Schreibzugriff auf S3-Buckets verbieten sammeln. Diese Kontrolle überprüft die Zugriffsebenen Ihrer S3-Bucket-Richtlinien. Für diese Kontrolle verwendet Audit Manager eine bestimmte AWS Config Regel (s3- bucket-public-write-prohibited), um nach einer Bewertung Ihrer S3-Buckets zu suchen. In diesem Beispiel gilt Folgendes:

- Das service in scope ist Amazon S3
- Bei den Ressourcen, die bewertet werden, handelt es sich um Ihre S3-Buckets
- Der Datenquellentyp ist AWS Config
- Bei der Datenquellenzuordnung handelt es sich um eine bestimmte AWS Config Regel (`s3-bucket-public-write-prohibited`)

Beispiel 2

Nehmen wir an, Sie möchten Beweise für eine HIPAA-Kontrolle mit der Bezeichnung 164.308 (a) (5) (ii) (C) sammeln. Diese Kontrolle erfordert ein Überwachungsverfahren zur Erkennung unangemessener Anmeldungen. Für diese Steuerung verwendet Audit Manager CloudTrail Protokolle, um nach allen Anmeldeereignissen der AWS Management Console zu suchen. In diesem Beispiel gilt Folgendes:

- Das service in scope ist IAM
- Bei den Ressourcen, die bewertet werden, handelt es sich um Ihre Benutzer
- Der Datenquellentyp ist CloudTrail
- Die Datenquellenzuordnung ist ein bestimmtes CloudTrail Ereignis (`ConsoleLogin`)

Behebung von Bewertungsberichtfehlern

Mithilfe der Informationen auf dieser Seite können Sie häufig auftretende Probleme mit den Bewertungsberichten in Audit Manager lösen.

Themen

Mein Bewertungsbericht konnte nicht generiert werden

Ihr Bewertungsbericht kann aus verschiedenen Gründen nicht erstellt worden sein. Sie können mit der Behebung dieses Problems beginnen, indem Sie die häufigsten Ursachen überprüfen. Verwenden Sie die folgende Checkliste, um loszulegen.

1. Prüfen Sie, ob Ihre AWS-Region Informationen nicht übereinstimmen:
   a. Stimmt AWS-Region der Schlüssel Ihres vom Kunden verwalteten AWS-Region Schlüssels mit Ihrer Bewertung überein?

      Wenn Sie Ihren eigenen KMS-Schlüssel für die Audit Manager Manager-Datenverschlüsselung angegeben haben, muss der Schlüssel mit Ihrer Bewertung übereinstimmen. AWS-Region Um dieses Problem zu beheben, ändern Sie den KMS-Schlüssel in einen, der sich in derselben Region wie Ihre Bewertung befindet. Anweisungen zum Ändern des KMS-Schlüssels finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen.

   b. Stimmt AWS-Region der Schlüssel Ihres vom Kunden verwalteten Schlüssels mit dem AWS-Region Ihres S3-Buckets überein?

      Wenn Sie Ihren eigenen KMS-Schlüssel für die Audit Manager Manager-Datenverschlüsselung angegeben haben, muss sich der Schlüssel in demselben AWS-Region S3-Bucket befinden, den Sie als Ziel für Ihren Bewertungsbericht verwenden. Um dieses Problem zu beheben, können Sie entweder den KMS-Schlüssel oder den S3-Bucket so ändern, dass sich beide in der gleichen Region wie Ihre Bewertung befinden. Anweisungen zum Ändern des KMS-Schlüssels finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen. Anweisungen zum Ändern des S3-Buckets finden Sie unterKonfiguration Ihres Standardziels für Bewertungsberichte.

2. Überprüfen Sie die Berechtigungen des S3-Buckets, den Sie als Ziel für den Bewertungsbericht verwenden:
   a. Verfügt die IAM-Einheit, die den Bewertungsbericht generiert, über die erforderlichen Berechtigungen für den S3-Bucket?

      Die IAM-Einheit muss über die erforderlichen S3-Bucket-Berechtigungen verfügen, um Berichte in diesem Bucket zu veröffentlichen. Wir stellen Ihnen eine Beispielrichtlinie zur Verfügung, die Sie befolgen können.

   b. Hat der S3-Bucket eine Bucket-Richtlinie, die eine serverseitige Verschlüsselung (SSE) mit SSE-KMS erfordert?

Falls ja, muss der KMS-Schlüssel, der in dieser Bucket-Richtlinie verwendet wird, mit dem KMS-Schlüssel übereinstimmen, der in Ihren Audit Manager-Datenverschlüsselungseinstellungen angegeben ist. Wenn Sie in Ihren Audit Manager-Einstellungen keinen KMS-Schlüssel konfiguriert haben und Ihre S3-Bucket-Richtlinie SSE erfordert, stellen Sie sicher, dass die Bucket-Richtlinie SSE-S3 zulässt. Anweisungen zum Ändern des KMS-Schlüssels finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen. Anweisungen zum Ändern des S3-Buckets finden Sie unterKonfiguration Ihres Standardziels für Bewertungsberichte.

Wenn Sie immer noch nicht erfolgreich einen Bewertungsbericht erstellen können, überprüfen Sie die auf dieser Seite angegebenen Problemquellen.

Ich habe die obige Checkliste befolgt, und mein Bewertungsbericht konnte immer noch nicht erstellt werden

Audit Manager begrenzt, wie viele Beweise Sie einem Bewertungsbericht hinzufügen können. Das Limit basiert auf Ihrer Bewertung, der Region AWS-Region des S3-Buckets, der als Ziel für Ihren Bewertungsbericht verwendet wird, und darauf, ob Ihre Bewertung einen vom Kunden verwalteten Bereich verwendet AWS KMS key.

1. Die Obergrenze liegt bei 22.000 für Berichte in derselben Region (bei denen sich der S3-Bucket und die Bewertung im selben AWS-Region befinden).
2. Die Obergrenze liegt bei 3.500 für regionsübergreifende Berichte (bei denen sich der AWS-Regionen des S3-Bucket und der Bewertung unterscheiden).
3. Die Obergrenze liegt bei 3.500, wenn für die Bewertung ein vom Kunden verwalteter KMS-Schlüssel verwendet wird.

Wenn Sie versuchen, einen Bericht zu erstellen, der mehr Beweise enthält, schlägt der Vorgang möglicherweise fehl.

Um dieses Problem zu umgehen, können Sie mehrere kleinere Bewertungsberichte anstelle eines größeren Bewertungsberichts erstellen. Auf diese Weise können Sie Beweise aus Ihrer Bewertung in Stapeln exportieren, deren Größe leichter zu handhaben ist.

Ich erhalte die Fehlermeldung Zugriff verweigert, wenn ich versuche, einen Bericht zu erstellen

Sie erhalten eine `access denied`-Fehlermeldung, wenn Ihre Bewertung von einem delegierten Administratorkonto erstellt wurde, zu dem der in Ihren Audit Manager-Einstellungen angegebene KMS-Schlüssel nicht gehört. Um diesen Fehler zu vermeiden, stellen Sie bei der Benennung eines delegierten Administrators für Audit Manager sicher, dass das delegierte Administratorkonto Zugriff auf den KMS-Schlüssel hat, den Sie bei der Einrichtung von Audit Manager angegeben haben.

Möglicherweise erhalten Sie auch eine `access denied`-Fehlermeldung, wenn Sie keine Schreibberechtigungen für den S3-Bucket haben, den Sie als Ziel für Ihren Bewertungsbericht verwenden.

Wenn Sie eine `access denied`-Fehlermeldung erhalten, vergewissern Sie sich, dass Sie die folgenden Voraussetzungen erfüllen:

- Ihr KMS-Schlüssel in Ihren Audit Manager-Einstellungen gewährt dem delegierten Administrator Berechtigungen. Sie können dies konfigurieren, indem Sie den Anweisungen unter Zulassen, dass Benutzer mit anderen Konten einen KMS-Schlüssel verwenden können im AWS Key Management Service -Entwicklerhandbuch folgen. Anweisungen zum Überprüfen und Ändern Ihrer Verschlüsselungseinstellungen in Audit Manager finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen.
- Sie haben eine Berechtigungsrichtlinie, die Ihnen Schreibzugriff für den S3-Bucket gewährt, den Sie als Ziel für den Bewertungsbericht verwenden. Genauer gesagt enthält Ihre Berechtigungsrichtlinie eine `s3:PutObject`-Aktion, spezifiziert den ARN des S3-Buckets und beinhaltet den KMS-Schlüssel, der zur Verschlüsselung Ihrer Bewertungsberichte verwendet wird. Ein Beispiel für eine Richtlinie, die Sie verwenden können, finden Sie unterBeispiel 2 (Zielberechtigungen für den Bewertungsbericht).

> **Note**
>
> Wenn Sie Ihre Audit Manager-Datenverschlüsselungseinstellungen ändern, gelten diese Änderungen für die neuen Bewertungen, die Sie in Zukunft erstellen. Dies schließt alle Bewertungsberichte mit ein, die Sie anhand Ihrer neuen Bewertungen erstellen.
> Die Änderungen gelten nicht für bestehende Bewertungen, die Sie erstellt haben, bevor Sie Ihre Verschlüsselungseinstellungen geändert haben. Dazu gehören neben bestehenden Bewertungsberichten auch neue Bewertungsberichte, die Sie anhand vorhandener

Bewertungen erstellen. Bestehende Bewertungen – und all ihre Bewertungsberichte – verwenden weiterhin den alten KMS-Schlüssel. Wenn die IAM-Identität, die den Bewertungsbericht generiert, nicht berechtigt ist, den alten KMS-Schlüssel zu verwenden, können Sie Berechtigungen auf der Ebene der wichtigsten Richtlinien gewähren.

Ich kann den Bewertungsbericht nicht entpacken

Wenn Sie den Bewertungsbericht in Windows nicht entpacken können, kann Windows Explorer ihn wahrscheinlich nicht extrahieren, da sein Dateipfad mehrere verschachtelte Ordner oder lange Namen enthält. Das liegt daran, dass unter dem Windows-Dateibenennungssystem der Ordnerpfad, der Dateiname und die Dateierweiterung 259 Zeichen nicht überschreiten dürfen. Andernfalls führt dies zu einem `Destination Path Too Long`-Fehler.

Versuchen Sie, die ZIP-Datei in den übergeordneten Ordner ihres aktuellen Speicherorts zu verschieben, um dieses Problem zu beheben. Sie können dann erneut versuchen, die Datei von dort aus zu entpacken. Alternativ können Sie auch versuchen, den Namen der ZIP-Datei zu kürzen oder sie an einen anderen Speicherort mit einem kürzeren Dateipfad zu extrahieren.

Wenn ich in einem Bericht einen Beweisnamen auswähle, werde ich nicht zu den Beweisdetails weitergeleitet

Dieses Problem kann auftreten, wenn Sie mit dem Bewertungsbericht in einem Browser interagieren oder den standardmäßigen PDF-Reader verwenden, der auf Ihrem Betriebssystem installiert ist. Bei einigen Standard-PDF-Readern in Browsern und Systemen ist das Öffnen relativer Links nicht möglich. Das bedeutet, dass Hyperlinks zwar in der PDF mit der Zusammenfassung des Bewertungsberichts funktionieren können (z. B. mit Hyperlinks versehene Kontrollnamen im Inhaltsverzeichnis), dass Hyperlinks jedoch ignoriert werden, wenn Sie versuchen, von der PDF-Datei mit der Bewertungszusammenfassung zu einer separaten PDF-Datei mit Beweisdetails zu wechseln.

Wenn Sie auf dieses Problem stoßen, empfehlen wir Ihnen, einen speziellen PDF-Reader zu verwenden, um mit Ihren Bewertungsberichten zu interagieren. Für ein zuverlässiges Nutzererlebnis empfehlen wir Ihnen, Adobe Acrobat Reader zu installieren und zu verwenden, den Sie auf der Adobe-Website herunterladen können. Andere PDF-Reader sind ebenfalls verfügbar, aber Adobe Acrobat Reader funktioniert nachweislich konsistent und zuverlässig mit den Bewertungsberichten von Audit Manager.

Die Erstellung meines Bewertungsberichts befindet sich im Status In Bearbeitung und ich bin mir nicht sicher, wie sich das auf meine Abrechnung auswirkt

Die Erstellung des Bewertungsberichts hat keine Auswirkungen auf die Abrechnung. Ihnen wird nur auf der Grundlage der Nachweise in Rechnung gestellt, die im Rahmen Ihrer Bewertungen gesammelt wurden. Weitere Informationen über die Preise finden Sie unter AWS Audit Manager – Preise.

Weitere Ressourcen

Auf den folgenden Seiten finden Sie Anleitungen zur Fehlerbehebung bei der Erstellung eines Bewertungsberichts mit Evidence Finder:

- Ich kann aus meinen Suchergebnissen nicht mehrere Bewertungsberichte erstellen
- Ich kann keine spezifischen Beweise aus meinen Suchergebnissen hinzufügen
- Nicht alle meine Beweiserhebungsergebnisse sind im Bewertungsbericht enthalten
- Ich möchte aus meinen Suchergebnissen einen Bewertungsbericht erstellen, aber meine Anfrage schlägt fehl

Behebung von Problemen mit Kontrollen und Kontrollsätzen

Sie können die Informationen auf dieser Seite verwenden, um häufig auftretende Probleme mit Kontrollen in Audit Manager zu lösen.

Allgemeine Probleme

- Ich kann in meiner Bewertung keine Kontrollen oder Kontrollsätze sehen
- Ich kann keine manuellen Beweise in eine Kontrolle hochladen
- Was bedeutet es, wenn auf einer Kontrolle „Ersatz verfügbar“ angezeigt wird?

AWS Config -Integrationsprobleme

- Ich muss mehrere AWS Config Regeln als Datenquelle für ein einzelnes Steuerelement verwenden

- Die Option für benutzerdefinierte Regeln ist nicht verfügbar, wenn ich eine Kontrolldatenquelle konfiguriere
- Die Option für benutzerdefinierte Regeln ist zwar verfügbar, aber in der Dropdownliste werden keine Regeln angezeigt
- Einige benutzerdefinierte Regeln sind verfügbar, aber ich kann die Regel, die ich verwenden möchte, nicht sehen
- Ich kann die verwaltete Regel, die ich verwenden möchte, nicht sehen
- Ich möchte ein benutzerdefiniertes Framework teilen, aber es enthält Steuerelemente, die benutzerdefinierte AWS Config Regeln als Datenquelle verwenden. Kann der Empfänger Beweise für diese Kontrollen sammeln?
- Was passiert, wenn eine benutzerdefinierte Regel in AWS Config aktualisiert wird? Muss ich in Audit Manager irgendwelche Aktionen durchführen?

Ich kann in meiner Bewertung keine Kontrollen oder Kontrollsätze sehen

Kurz gesagt, um die Kontrollen für eine Bewertung anzeigen zu können, müssen Sie als Audit-Verantwortlichen für diese Bewertung angegeben sein. Darüber hinaus benötigen Sie die erforderlichen IAM-Berechtigungen, um die zugehörigen Audit Manager-Ressourcen anzuzeigen und zu verwalten.

Wenn Sie Zugriff auf die Kontrollen in einer Bewertung benötigen, bitten Sie einen der Audit-Verantwortlichen, Sie als Audit-Verantwortlichen anzugeben. Wenn Sie eine Bewertung erstellen oder bearbeiten, können Sie gleichzeitig auch die Audit-Verantwortlichen angeben.

Stellen Sie außerdem sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um die Bewertung zu verwalten. Wir empfehlen den Prüfinhabern, die AWSAuditManagerAdministratorAccessRichtlinie zu verwenden. Wenn Sie Hilfe zu IAM-Berechtigungen benötigen, wenden Sie sich an Ihren Administrator oder AWS -Support. Weitere Informationen darüber, wie Sie einer IAM-Identität eine Richtlinie zuordnen, finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer und Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

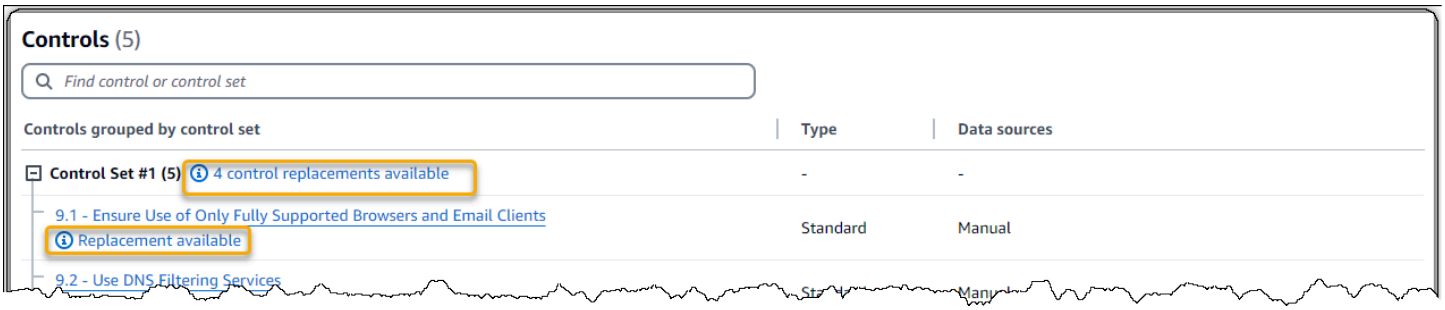
Ich kann keine manuellen Beweise in eine Kontrolle hochladen

Wenn Sie Beweise nicht manuell zu einer Kontrolle hochladen können, liegt das wahrscheinlich daran, dass sich die Kontrolle im Status Inaktiv befindet.

Um manuelle Beweise in eine Kontrolle hochzuladen, müssen Sie zunächst den Kontrollstatus entweder in Wird geprüft oder Geprüft ändern. Detaillierte Anweisungen finden Sie unter Den Status einer Bewertungskontrolle ändern in AWS Audit Manager.

> **Important**
>
> Jeder AWS-Konto kann täglich nur bis zu 100 Nachweisdateien manuell auf eine Kontrolle hochladen. Eine Überschreitung dieses täglichen Kontingents führt dazu, dass alle zusätzlichen manuellen Uploads für diese Kontrolle fehlschlagen. Wenn Sie eine große Menge manueller Beweise auf eine einzelne Kontrolle hochladen müssen, laden Sie Ihre Beweise stapelweise über mehrere Tage hinweg hoch.

Was bedeutet es, wenn auf einer Kontrolle „Ersatz verfügbar“ angezeigt wird?



Wenn Sie diese Meldung sehen, bedeutet dies, dass eine aktualisierte Kontrolldefinition für eine oder mehrere der Standardsteuerelemente in Ihrem benutzerdefinierten Framework verfügbar ist. Wir empfehlen Ihnen, diese Kontrollen zu ersetzen, damit Sie von den verbesserten Beweisquellen profitieren können, die Audit Manager jetzt bietet.

Anweisungen zum weiteren Vorgehen finden Sie unterAuf der Detailseite meines benutzerdefinierten Frameworks werde ich aufgefordert, mein benutzerdefiniertes Framework neu zu erstellen.

Ich muss mehrere AWS Config Regeln als Datenquelle für ein einzelnes Steuerelement verwenden

Sie können für eine einzelne Kontrolle eine Kombination aus verwalteten und benutzerdefinierten Regeln verwenden. Definieren Sie dazu mehrere Beweisquellen für das Steuerelement und wählen Sie für jede einzelne Ihren bevorzugten Regeltyp aus. Sie können bis zu 100 vom Kunden verwaltete Datenquellen für ein einzelnes benutzerdefiniertes Steuerelement definieren.

Die Option für benutzerdefinierte Regeln ist nicht verfügbar, wenn ich eine Kontrolldatenquelle konfiguriere

Das bedeutet, dass Sie nicht berechtigt sind, benutzerdefinierte Regeln für Ihre AWS-Konto oder Ihre Organisation einzusehen. Insbesondere sind Sie nicht berechtigt, den DescribeConfigRulesVorgang in der Audit Manager Manager-Konsole auszuführen.

Wenden Sie sich an Ihren AWS Administrator, um Hilfe zu erhalten, um dieses Problem zu beheben. Wenn Sie ein AWS -Administrator sind, können Sie Ihren Benutzern oder Gruppen Berechtigungen gewähren, indem Sie Ihre IAM-Richtlinien verwalten.

Die Option für benutzerdefinierte Regeln ist zwar verfügbar, aber in der Dropdownliste werden keine Regeln angezeigt

Das bedeutet, dass keine benutzerdefinierten Regeln aktiviert sind und für die Verwendung in Ihrer AWS-Konto oder Ihrer Organisation verfügbar sind.

Wenn Sie noch keine benutzerdefinierten Regeln eingerichtet haben AWS Config, können Sie eine erstellen. Anweisungen dazu finden Sie unter benutzerdefinierte AWS Config -Rollen im AWS Config -Entwicklerhandbuch.

Wenn Sie erwarten, dass eine benutzerdefinierte Regel angezeigt wird, überprüfen Sie den folgenden Punkt zur Fehlerbehebung.

Einige benutzerdefinierte Regeln sind verfügbar, aber ich kann die Regel, die ich verwenden möchte, nicht sehen

Wenn Sie die benutzerdefinierte Regel, die Sie voraussichtlich finden werden, nicht sehen können, könnte dies an einem der folgenden Probleme liegen.

Ihr Konto ist von der Regel ausgeschlossen

Es ist möglich, dass das von Ihnen verwendete delegierte Administratorkonto von der Regel ausgeschlossen ist.

Das Verwaltungskonto Ihrer Organisation (oder eines der AWS Config delegierten Administratorkonten) kann mithilfe von AWS Command Line Interface (AWS CLI) benutzerdefinierte Organisationsregeln erstellen. In diesem Fall können sie eine Liste von Konten

angeben, die von der Regel ausgeschlossen werden sollen. Wenn Ihr Konto auf dieser Liste steht, ist die Regel in Audit Manager nicht verfügbar.

Wenden Sie sich an Ihren AWS Config Administrator, um Hilfe zu erhalten, um dieses Problem zu beheben. Wenn Sie ein AWS Config Administrator sind, können Sie die Liste der ausgeschlossenen Konten aktualisieren, indem Sie den put-organization-config-ruleBefehl ausführen.

Die Regel wurde nicht erfolgreich erstellt und in AWS Config aktiviert

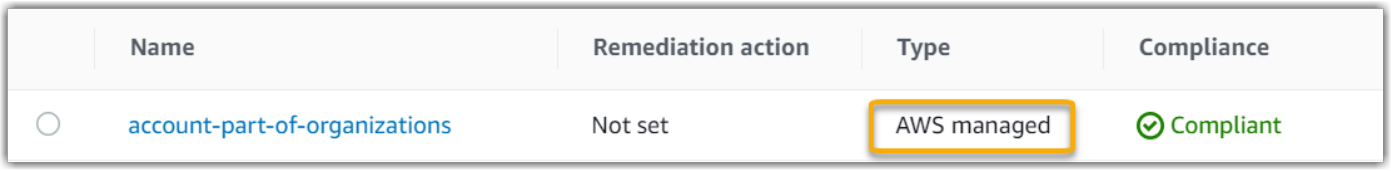
Es ist auch möglich, dass die benutzerdefinierte Regel nicht erfolgreich erstellt und aktiviert wurde. Wenn beim Erstellen der Regel ein Fehler aufgetreten ist oder die Regel nicht aktiviert ist, wird sie nicht in der Liste der verfügbaren Regeln in Audit Manager angezeigt.

Wir empfehlen, sich an Ihren AWS Config -Administrator zu wenden, um Hilfe bei diesem Problem zu erhalten.

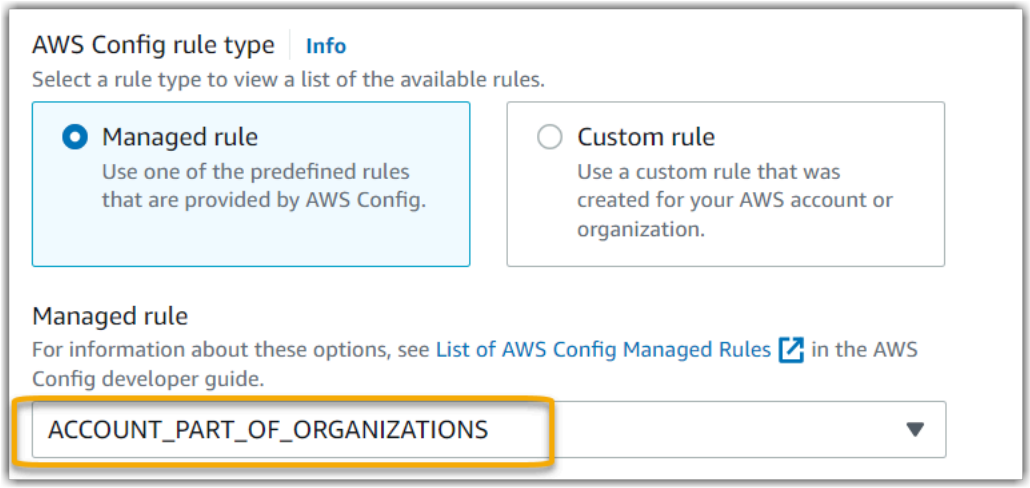
Die Regel ist eine verwaltete Regel

Wenn Sie die Regel, nach der Sie suchen, nicht in der Dropdownliste der benutzerdefinierten Regeln finden können, ist es möglich, dass es sich bei der Regel um eine verwaltete Regel handelt.

Sie können die AWS Config -Konsole verwenden, um zu überprüfen, ob es sich bei einer Regel um eine verwaltete Regel handelt. Wählen Sie dazu im linken Navigationsmenü Regeln aus und suchen Sie in der Tabelle nach der Regel. Wenn es sich bei der Regel um eine verwaltete Regel handelt, wird in der Spalte Typ der Eintrag AWS -verwaltet angezeigt.

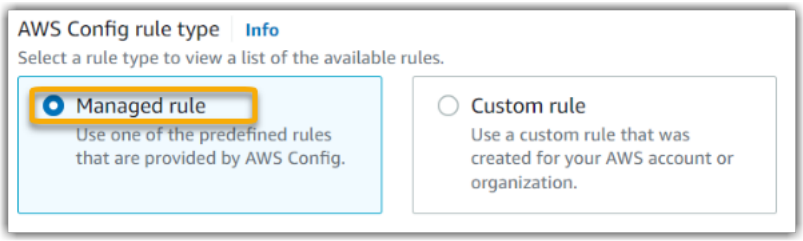


Nachdem Sie bestätigt haben, dass es sich um eine verwaltete Regel handelt, kehren Sie zu Audit Manager zurück und wählen als Regeltyp Verwaltete Regel aus. Suchen Sie dann in der Dropdownliste der verwalteten Regeln nach dem Schlüsselwort für die verwaltete Regel-ID.



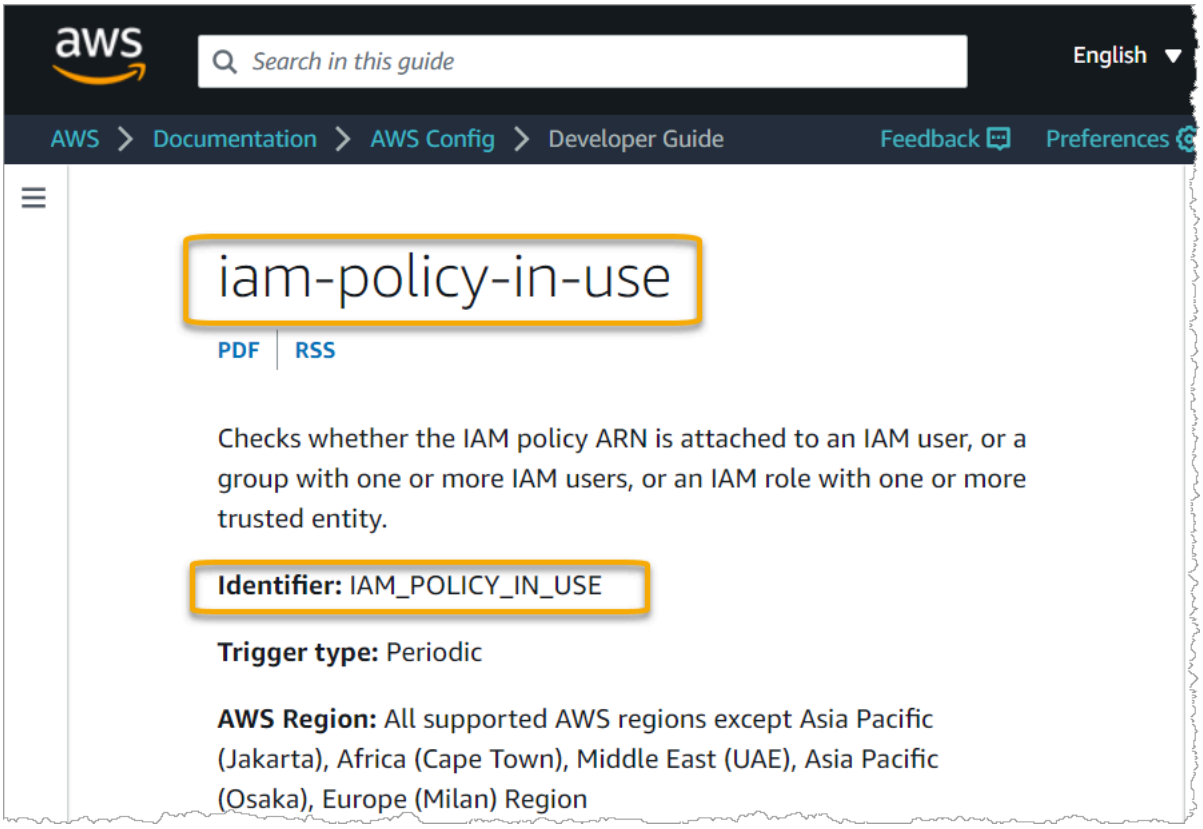
Ich kann die verwaltete Regel, die ich verwenden möchte, nicht sehen

Bevor Sie eine Regel aus der Dropdownliste in der Audit Manager-Konsole auswählen, stellen Sie sicher, dass Sie Verwaltete Regel als Regeltyp ausgewählt haben.

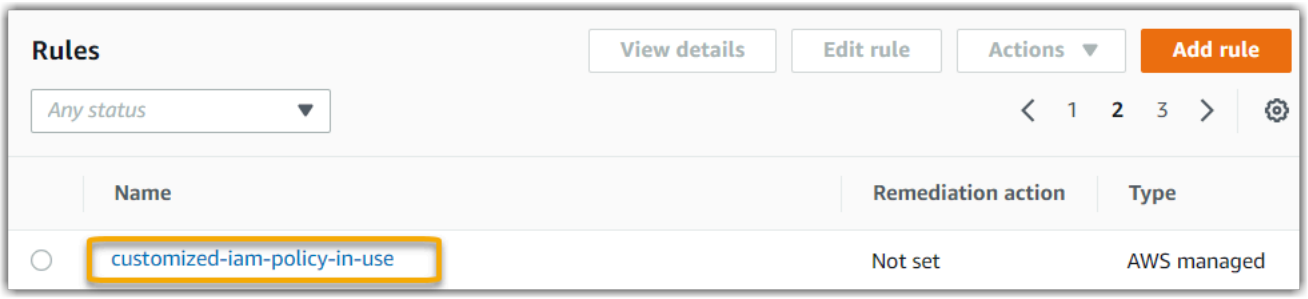


Wenn Sie die erwartete verwaltete Regel immer noch nicht sehen können, suchen Sie vielleicht nach dem Regelnamen. Stattdessen müssen Sie nach der Regel-ID suchen.

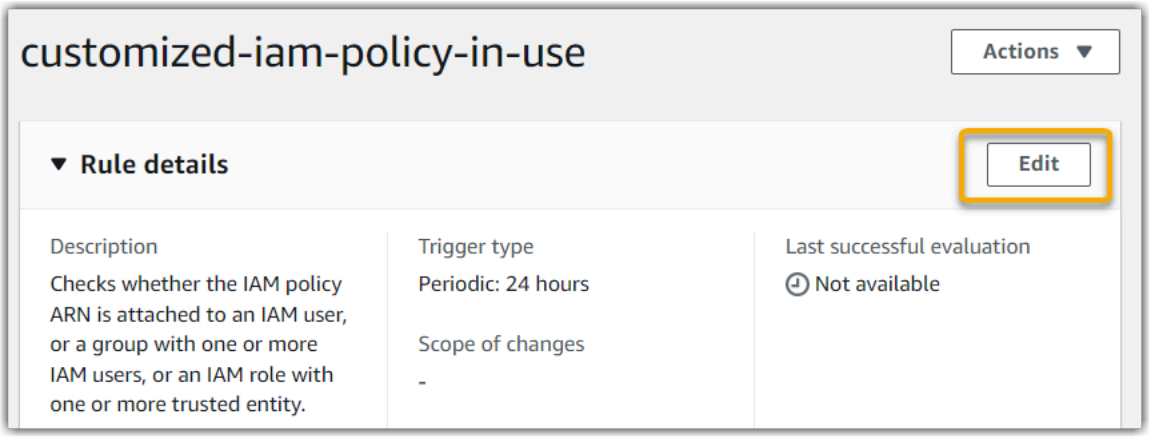
Wenn Sie eine verwaltete Standardregel verwenden, ähneln sich Name und ID. Der Name wird in Kleinbuchstaben geschrieben und verwendet Bindestriche (z. B. `iam-policy-in-use`). Die ID ist in Großbuchstaben geschrieben und verwendet Unterstriche (z. B. `IAM_POLICY_IN_USE`). Um den Bezeichner für eine verwaltete Standardregel zu finden, überprüfen Sie die Liste der unterstützten Schlüsselwörter für AWS Config verwaltete Regeln und folgen Sie dem Link für die Regel, die Sie verwenden möchten. Dadurch gelangen Sie zur AWS Config Dokumentation für diese verwaltete Regel. Von hier aus können Sie sowohl den Namen als auch die Kennung sehen. Suchen Sie in der Audit Manager-Dropdownliste nach der Schlüsselwort-ID.



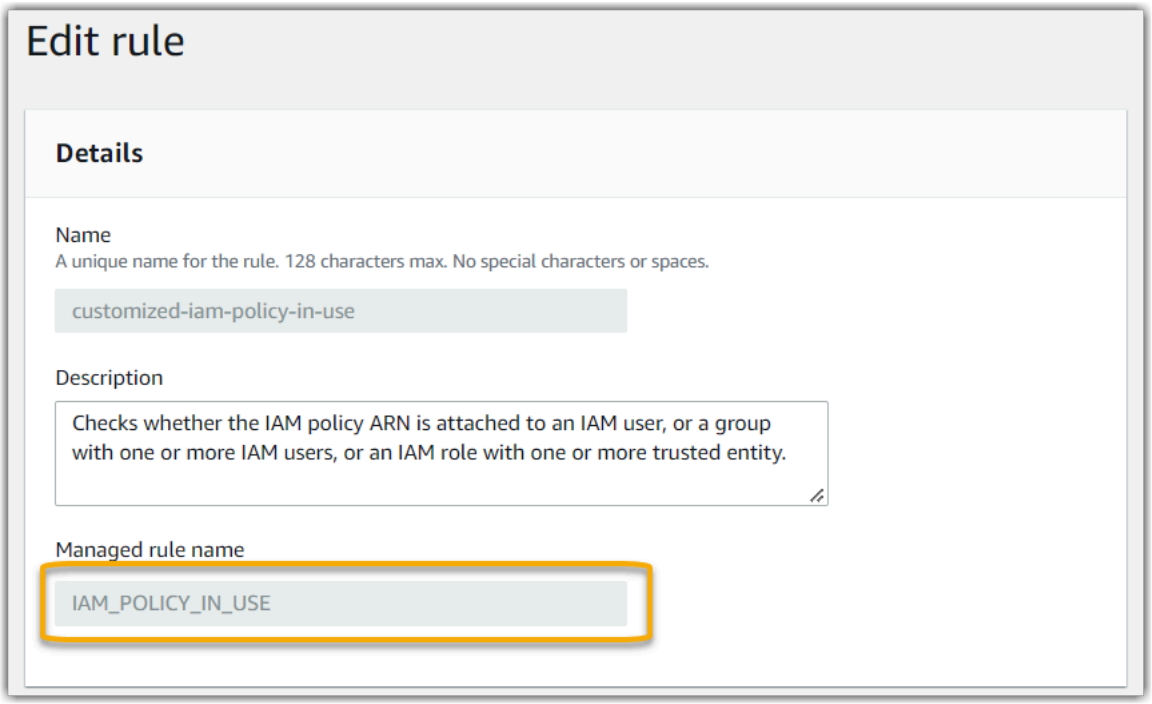
Wenn Sie eine benutzerdefinierte verwaltete Regel verwenden, können Sie die Regel-ID mithilfe der AWS Config Konsole suchen. Angenommen, Sie möchten die verwaltete Regel mit dem Namen `customized-iam-policy-in-use` verwenden. Um die ID für diese Regel zu finden, gehen Sie zur AWS Config Konsole, wählen Sie im linken Navigationsmenü Regeln und wählen Sie die Regel in der Tabelle aus.



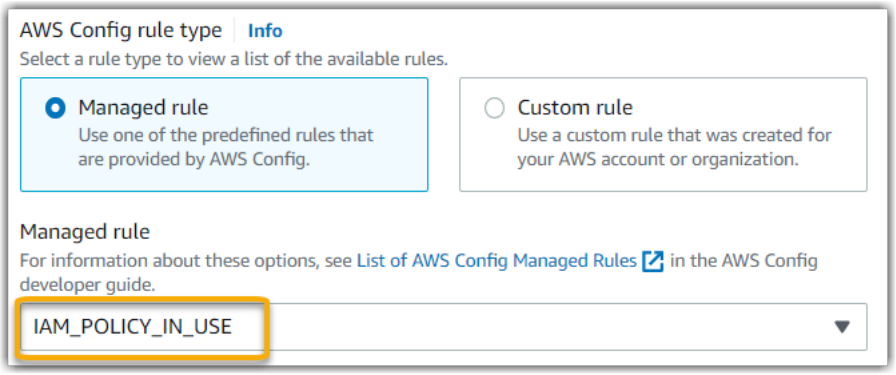
Wählen Sie Bearbeiten, um Details zur verwalteten Regel zu öffnen.



Im Abschnitt Details finden Sie die Quell-ID, aus der die verwaltete Regel erstellt wurde (`IAM_POLICY_IN_USE`).



Sie können jetzt zur Audit Manager-Konsole zurückkehren und dasselbe ID-Schlüsselwort aus der Dropdownliste auswählen.



Ich möchte ein benutzerdefiniertes Framework teilen, aber es enthält Steuerelemente, die benutzerdefinierte AWS Config Regeln als Datenquelle verwenden. Kann der Empfänger Beweise für diese Kontrollen sammeln?

Ja, der Empfänger kann Beweise für diese Kontrollen sammeln, aber dazu sind einige Schritte erforderlich.

Damit Audit Manager mithilfe einer AWS Config Regel als Datenquellenzuordnung Beweise sammeln kann, muss Folgendes zutreffen. Dies gilt sowohl für verwaltete als auch für benutzerdefinierte Regeln.

1. Die Regel muss in der AWS Umgebung des Empfängers vorhanden sein
2. Die Regel muss in der AWS Umgebung des Empfängers aktiviert sein

Denken Sie daran, dass die benutzerdefinierten AWS Config Regeln in Ihrem Konto wahrscheinlich nicht bereits in der AWS Umgebung des Empfängers existieren. Wenn der Empfänger die Freigabeanfrage akzeptiert, erstellt Audit Manager außerdem keine Ihrer benutzerdefinierten Regeln in seinem Konto neu. Damit der Empfänger anhand Ihrer benutzerdefinierten Regeln als Datenquellenzuordnung Beweise sammeln kann, muss er dieselben benutzerdefinierten Regeln in seiner Instanz von erstellen AWS Config. Nachdem der Empfänger die Regeln erstellt und anschließend aktiviert hat, kann Audit Manager Beweise aus dieser Datenquelle sammeln.

Wir empfehlen Ihnen, mit dem Empfänger zu kommunizieren, um ihn darüber zu informieren, ob in seiner Instance von AWS Config benutzerdefinierte Regeln erstellt werden müssen.

Was passiert, wenn eine benutzerdefinierte Regel in AWS Config aktualisiert wird? Muss ich in Audit Manager irgendwelche Aktionen durchführen?

Für Regelaktualisierungen in Ihrer AWS Umgebung

Wenn Sie eine benutzerdefinierte Regel in Ihrer AWS Umgebung aktualisieren, ist in Audit Manager keine Aktion erforderlich. Audit Manager erkennt und verarbeitet die Regelaktualisierungen wie in der folgenden Tabelle beschrieben. Audit Manager benachrichtigt Sie nicht, wenn ein Regel-Update erkannt wird.

Szenario	Was Audit Manager macht	Wichtige Informationen
Eine benutzerdefinierte Regel wird in Ihrer Instanz von aktualisiert AWS Config	Audit Manager berichtet weiterhin anhand der aktualisierten Regeldefinition über Ergebnisse für diese Regel.	Keine Aktion erforderlich.
Eine benutzerdefinierte Regel wird in Ihrer Instanz von gelöscht AWS Config	Audit Manager meldet keine Ergebnisse mehr für die gelöschte Regel.	Keine Aktion erforderlich. Wenn Sie möchten, können Sie die benutzerdefinierten Kontrollen bearbeiten, die die gelöschte Regel als Datenquellenzuordnung verwendet haben. Auf diese Weise, d. h. indem Sie die gelöschte Regel entfernen, können Sie Ihre Datenquelleneinstellungen bereinigen. Andernfalls bleibt der Name der gelöschten Regel als unbenutzte Datenquellenzuordnung erhalten.

Für Regelaktualisierungen außerhalb Ihrer AWS Umgebung

Wenn eine benutzerdefinierte Regel außerhalb Ihrer AWS Umgebung aktualisiert wird, erkennt Audit Manager die Regelaktualisierung nicht. Dies sollten Sie berücksichtigen, wenn Sie gemeinsam genutzte benutzerdefinierte Frameworks verwenden. Das liegt daran, dass in diesem Szenario der Absender und der Empfänger jeweils in unterschiedlichen AWS Umgebungen arbeiten. Die folgende Tabelle enthält empfohlene Aktionen für dieses Szenario.

Ihre Rolle	Szenario	Empfohlene Aktion
Absend	• Sie haben ein Framework geteilt, das benutzerdefinierte Regeln als Datenquel lenzuordnung verwendet. • Nachdem Sie das Framework freigegeb en haben, haben Sie eine dieser Regeln in aktualisiert oder gelöscht AWS Config.	Informieren Sie den Empfänger über Ihr Update. Auf diese Weise können sie dasselbe Update anwenden und mit der neuesten Regeldefinition synchron bleiben.
Empfär	• Sie haben ein gemeinsames Framework akzeptiert, das benutzerdefinierte Regeln als Datenquellenzuordnung verwendet. • Nachdem Sie die benutzerdefinierten Regeln in Ihrer Instanz von neu erstellt haben AWS Config, hat der Absender eine dieser Regeln aktualisiert oder gelöscht.	Führen Sie die entsprechende Regelaktualisierung in Ihrer eigenen Instance von AWS Config durch.

Fehlerbehebung bei Dashboard-Problemen

Sie können die Informationen auf dieser Seite verwenden, um häufig auftretende Probleme mit dem Dashboard in Audit Manager zu lösen.

Themen

- Ich sehe ähnliche oder doppelte Steuerelemente, die unter derselben Kontrolldomäne angezeigt werden
- Der tägliche Überblick zeigt jeden Tag unterschiedliche Mengen an Beweisen. Ist das normal?

Auf meinem Dashboard befinden sich keine Daten

Wenn die Zahlen im Tägliche Snapshots Widget einen Bindestrich (-) enthalten, bedeutet dies, dass keine Daten verfügbar sind. Sie müssen über mindestens eine aktive Bewertung verfügen, um die Daten im Dashboard zu sehen. Um loszulegen, erstellen Sie eine Bewertung. Nach einem Zeitraum von 24 Stunden werden Ihre Bewertungsdaten im Dashboard angezeigt.

> **Note**
>
> Wenn die Zahlen im täglichen Snapshot-Widget eine Null (0) anzeigen, bedeutet dies, dass Ihre aktiven Bewertungen (oder Ihre ausgewählte Bewertung) keine Hinweise auf Verstöße enthalten.

Die CSV-Download-Option ist nicht verfügbar

Diese Option steht nur für individuelle Bewertungen zu Verfügung. Stellen Sie sicher, dass Sie einen Bewertungsfilter auf das Dashboard angewendet haben, und versuchen Sie es dann erneut. Berücksichtigen Sie, dass Sie jeweils nur eine CSV-Datei herunterladen können.

Ich sehe die heruntergeladene Datei nicht, wenn ich versuche, eine CSV-Datei herunterzuladen

Wenn eine Kontrolldomain eine große Anzahl von Kontrollen enthält, kann es zu einer kurzen Verzögerung kommen, während Audit Manager die CSV-Datei generiert. Nachdem die Datei generiert wurde, wird sie automatisch heruntergeladen.

Wenn Sie die heruntergeladene Datei immer noch nicht sehen, stellen Sie sicher, dass Ihre Internetverbindung normal funktioniert und Sie die neueste Version Ihres Webbrowsers verwenden. Überprüfen Sie außerdem Ihren Ordner mit den letzten Downloads. Dateien werden in den von Ihrem Browser festgelegten Standardspeicherort heruntergeladen. Wenn das Problem dadurch nicht behoben wird, versuchen Sie, die Datei mit einem anderen Browser herunterzuladen.

Eine bestimmte Kontrolle oder Kontrolldomain fehlt im Dashboard

Dies bedeutet wahrscheinlich, dass Ihre aktiven Bewertungen (oder eine bestimmte Bewertung) keine relevanten Daten für diese Kontrolle oder Kontrolldomain enthalten.

Eine Kontrolldomain wird nur dann im Dashboard angezeigt, wenn die beiden folgenden Kriterien erfüllt sind:

- Ihre aktiven Bewertungen (oder die angegebene Bewertung) enthalten mindestens eine Kontrolle, die sich auf diese Domäne bezieht
- Mindestens eine Kontrolle innerhalb dieses Bereichs hat an dem oben im Dashboard angezeigten Datum Beweise gesammelt

Eine Kontrolle wird innerhalb einer Domain nur angezeigt, wenn sie an dem oben im Dashboard angegebenen Datum Beweise gesammelt hat.

Ich sehe ähnliche oder doppelte Steuerelemente, die unter derselben Kontrolldomäne angezeigt werden

Dieses Problem kann auftreten, wenn bei Ihren Prüfungen Beweise aus verschiedenen Versionen derselben Standardkontrolle gesammelt werden.

Dies passiert in folgenden Szenarien:

Szenario 1: Sie haben zwei Bewertungen, die auf demselben Standard-Framework basieren

- Sie haben vor dem Start der Common Controls Library eine Bewertung auf der Grundlage eines Standard-Frameworks erstellt.

  Bei dieser Bewertung werden Beweise anhand veralteter Standardkontrollen gesammelt.
- Nach der Einführung der Common Controls Library haben Sie außerdem eine Bewertung auf der Grundlage desselben Standard-Frameworks erstellt.

  Bei dieser Bewertung werden Beweise anhand der neuen Versionen der Standardkontrollen gesammelt.
- Daher werden bei Ihren Bewertungen Belege aus verschiedenen Versionen derselben Standardkontrollen gesammelt.

Szenario 2: Sie haben zwei Bewertungen auf der Grundlage eines benutzerdefinierten Frameworks erstellt, das Standardkontrollen verwendet

- Sie haben vor dem Start der Common Controls Library eine Bewertung anhand Ihres benutzerdefinierten Frameworks erstellt.

  Bei dieser Bewertung werden Beweise anhand veralteter Standardkontrollen gesammelt.
- Nach dem Start der Common Controls Library haben Sie auch eine Bewertung auf der Grundlage desselben benutzerdefinierten Frameworks erstellt.

  Bei dieser Bewertung werden Beweise anhand der neuen Versionen der Standardkontrollen gesammelt.
- Daher werden bei Ihren Bewertungen Belege aus verschiedenen Versionen derselben Standardkontrollen gesammelt.

Beispiel: Nehmen wir an, Sie haben bereits eine Bewertung, die Sie vor dem 6. Juni 2024 auf der Grundlage des PCI-DSS-Standard-Frameworks erstellt haben. Darüber hinaus haben Sie nach dem 6. Juni 2024 eine neue Bewertung auf der Grundlage des PCI DSS-Standard-Frameworks erstellt. Daher werden bei der ersten Bewertung Beweise anhand der veralteten Version der Standardkontrollen für PCI DSS gesammelt. Bei der zweiten Bewertung werden Beweise anhand der neuen Version der Standardkontrollen für PCI DSS gesammelt. Da beide Versionen der PCI-DSS-Kontrollen im Rahmen Ihrer Bewertungen aktiv Beweise sammeln, werden Sie wahrscheinlich feststellen, dass beide Kontrollgruppen im Dashboard unter derselben Kontrolldomäne angezeigt werden. In seltenen Fällen können das veraltete Steuerelement und das neue Steuerelement jedoch unter verschiedenen Kontrolldomänen auf dem Dashboard angezeigt werden.

Sie können weiterhin Beweise sammeln und Dashboard-Einblicke für veraltete Standardkontrollen und Frameworks einsehen. Wir empfehlen Ihnen jedoch, die neuen Kontrollen und Frameworks zu verwenden, die Audit Manager nach der Einführung der Common Controls Library am 6. Juni 2024 bereitstellt. Mit den neuen Standardkontrollen können AWS managed source Beweise von uns gesammelt werden. Das bedeutet, dass Audit Manager jedes Mal, wenn die zugrunde liegenden Datenquellen für eine gemeinsame oder zentrale Kontrolle aktualisiert werden, dieselbe Aktualisierung automatisch auf alle zugehörigen Standardkontrollen anwendet.

Der tägliche Überblick zeigt jeden Tag unterschiedliche Mengen an Beweisen. Ist das normal?

Nicht alle Beweise werden täglich gesammelt. Die Kontrollen in Audit Manager-Bewertungen sind unterschiedlichen Datenquellen zugeordnet, und für jede dieser Quellen kann ein anderer Zeitplan für die Beweiserhebung gelten. Daher ist zu erwarten, dass der tägliche Snapshot eine unterschiedliche Menge an Beweisen enthalten kann. Weitere Informationen finden Sie unter Häufigkeit der Beweissuche.

Behebung von Problemen mit delegierten AWS Organizations - Administratoren

Sie können die Informationen auf dieser Seite verwenden, um häufig auftretende Probleme mit delegierten Administratoren in Audit Manager zu lösen.

Themen

- Ich kann Audit Manager nicht mit meinem delegierten Administratorkonto einrichten
- Wenn ich eine Bewertung erstelle, kann ich die Konten meiner Organisation unter Konten im Bewertungsumfang nicht sehen
- Ich erhalte die Fehlermeldung Zugriff verweigert, wenn ich versuche, mit meinem delegierten Administratorkonto einen Bewertungsbericht zu erstellen
- Was passiert in Audit Manager, wenn ich die Verknüpfung eines Mitgliedskontos mit meiner Organisation aufhebe?
- Was passiert, wenn ich ein Mitgliedskonto erneut mit meiner Organisation verknüpfe?
- Was passiert, wenn ich ein Mitgliedskonto von einer Organisation zu einer anderen migriere?

Ich kann Audit Manager nicht mit meinem delegierten Administratorkonto einrichten

Obwohl mehrere delegierte Administratoren unterstützt werden AWS Organizations, erlaubt Audit Manager nur einen delegierten Administrator. Wenn Sie versuchen, mehrere delegierte Administratoren in Audit Manager zu benennen, erhalten Sie die folgende Fehlermeldung:

- Konsole: `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Wählen Sie das einzelne Konto aus, das Sie als Ihren delegierten Administrator in Audit Manager verwenden möchten. Stellen Sie sicher, dass Sie zuerst das delegierte Administratorkonto in Organizations registrieren und dann dasselbe Konto wie ein delegierter Administrator in Audit Manager hinzufügen.

Wenn ich eine Bewertung erstelle, kann ich die Konten meiner Organisation unter Konten im Bewertungsumfang nicht sehen

Wenn Sie möchten, dass Ihre Audit Manager-Bewertung mehrere Konten aus Ihrer Organisation umfasst, müssen Sie einen delegierten Administrator angeben.

Stellen Sie sicher, dass Sie ein delegiertes Administratorkonto für Audit Manager konfiguriert haben. Detaillierte Anweisungen finden Sie unter Hinzufügen eines delegierten Administrators.

Einige Probleme, die Sie berücksichtigen sollten:

- Sie können Ihr AWS Organizations Verwaltungskonto nicht als delegierter Administrator in Audit Manager verwenden.
- Wenn Sie Audit Manager in mehr als einer Region aktivieren möchten AWS-Region, müssen Sie in jeder Region separat ein delegiertes Administratorkonto einrichten. Geben Sie in Ihren Audit Manager-Einstellungen für alle Regionen dasselbe delegierte Administratorkonto an.
- Wenn Sie einen delegierten Administrator benennen, stellen Sie sicher, dass das delegierte Administratorkonto Zugriff auf den KMS-Schlüssel hat, den Sie bei der Einrichtung von Audit Manager angeben. Informationen zum Überprüfen und Ändern Ihrer Verschlüsselungseinstellungen finden Sie unter. Konfiguration Ihrer Datenverschlüsselungseinstellungen

Ich erhalte die Fehlermeldung Zugriff verweigert, wenn ich versuche, mit meinem delegierten Administratorkonto einen Bewertungsbericht zu erstellen

Sie erhalten eine `access denied`-Fehlermeldung, wenn Ihre Bewertung von einem delegierten Administratorkonto erstellt wurde, zu dem der in Ihren Audit Manager-Einstellungen angegebene KMS-Schlüssel nicht gehört. Um diesen Fehler zu vermeiden, stellen Sie bei der Benennung eines delegierten Administrators für Audit Manager sicher, dass das delegierte Administratorkonto Zugriff auf den KMS-Schlüssel hat, den Sie bei der Einrichtung von Audit Manager angegeben haben.

Möglicherweise erhalten Sie auch eine `access denied`-Fehlermeldung, wenn Sie keine Schreibberechtigungen für den S3-Bucket haben, den Sie als Ziel für Ihren Bewertungsbericht verwenden.

Wenn Sie eine `access denied`-Fehlermeldung erhalten, vergewissern Sie sich, dass Sie die folgenden Voraussetzungen erfüllen:

- Ihr KMS-Schlüssel in Ihren Audit Manager-Einstellungen gewährt dem delegierten Administrator Berechtigungen. Sie können dies konfigurieren, indem Sie den Anweisungen unter Zulassen, dass Benutzer mit anderen Konten einen KMS-Schlüssel verwenden können im AWS Key Management Service -Entwicklerhandbuch folgen. Anweisungen zum Überprüfen und Ändern Ihrer Verschlüsselungseinstellungen in Audit Manager finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen.
- Sie verfügen über eine Berechtigungsrichtlinie, die Ihnen Schreibzugriff für das Ziel des Bewertungsberichts gewährt. Genauer gesagt enthält Ihre Berechtigungsrichtlinie eine `s3:PutObject`-Aktion, spezifiziert den ARN des S3-Buckets und beinhaltet den KMS-Schlüssel, der zur Verschlüsselung Ihrer Bewertungsberichte verwendet wird. Ein Beispiel für eine Richtlinie, die Sie verwenden können, finden Sie unterBeispiel 2 (Zielberechtigungen für den Bewertungsbericht).

> **Note**
>
> Wenn Sie Ihre Audit Manager-Datenverschlüsselungseinstellungen ändern, gelten diese Änderungen für die neuen Bewertungen, die Sie in Zukunft erstellen. Dies schließt alle Bewertungsberichte mit ein, die Sie anhand Ihrer neuen Bewertungen erstellen.
> Die Änderungen gelten nicht für bestehende Bewertungen, die Sie erstellt haben, bevor Sie Ihre Verschlüsselungseinstellungen geändert haben. Dazu gehören neben bestehenden

Bewertungsberichten auch neue Bewertungsberichte, die Sie anhand vorhandener Bewertungen erstellen. Bestehende Bewertungen – und all ihre Bewertungsberichte – verwenden weiterhin den alten KMS-Schlüssel. Wenn die IAM-Identität, die den Bewertungsbericht generiert, nicht berechtigt ist, den alten KMS-Schlüssel zu verwenden, können Sie Berechtigungen auf der Ebene der wichtigsten Richtlinien gewähren.

Was passiert in Audit Manager, wenn ich die Verknüpfung eines Mitgliedskontos mit meiner Organisation aufhebe?

Wenn Sie die Verknüpfung eines Mitgliedskontos mit einer Organisation aufheben, erhält Audit Manager eine Benachrichtigung über dieses Ereignis. Audit Manager entfernt dieses AWS-Konto dann automatisch aus den Konten im Bewertungsumfang. Wenn Sie den Umfang neuer Bewertungen für die Zukunft angeben, wird das nicht verknüpfte Konto nicht mehr in der Liste der in Frage kommenden AWS-Konten-Konten angezeigt.

Wenn Audit Manager ein nicht verknüpftes Mitgliedskonto aus den Konten im Bewertungsumfang entfernt, werden Sie nicht über diese Änderung informiert. Darüber hinaus wird das nicht verknüpfte Mitgliedskonto nicht darüber informiert, dass Audit Manager für sein Konto nicht mehr aktiviert ist.

Was passiert, wenn ich ein Mitgliedskonto erneut mit meiner Organisation verknüpfe?

Wenn Sie ein Mitgliedskonto erneut mit Ihrer Organisation verknüpfen, wird dieses Konto nicht automatisch zum Umfang Ihrer bestehenden Audit Manager-Bewertungen hinzugefügt. Das erneut verknüpfte Mitgliedskonto wird jetzt jedoch als berechtigtes Konto angezeigt AWS-Konto , wenn Sie die Konten im Rahmen Ihrer Bewertungen angeben.

- Bei bestehenden Bewertungen können Sie den Bewertungsbereich manuell bearbeiten, um das erneut verknüpfte Mitgliedskonto hinzuzufügen. Detaillierte Anweisungen finden Sie unter Schritt 2: Den Umfang bearbeiten AWS-Konten.
- Für neue Bewertungen können Sie das erneut verknüpfte Konto bei der Einrichtung des Tests hinzufügen. Detaillierte Anweisungen finden Sie unter Schritt 2: Geben Sie den Geltungsbereich AWS-Konten an.

Was passiert, wenn ich ein Mitgliedskonto von einer Organisation zu einer anderen migriere?

Wenn für ein Mitgliedskonto Audit Manager in Organisation 1 aktiviert ist und dann zu Organisation 2 migriert wird, ist Audit Manager damit für Organisation 2 nicht aktiviert.

Behebung von Problemen mit der Beweiserhebung

Verwenden Sie die Informationen auf dieser Seite, um häufig auftretende Probleme mit der Beweiserhebung in Audit Manager zu lösen.

Allgemeine Probleme mit der Beweiserhebung

- Ich kann die Beweiserhebung nicht aktivieren
- Ich habe die Beweiserhebung aktiviert, sehe aber in meinen Suchergebnissen keine Beweise aus der Vergangenheit
- Ich kann die Beweiserhebung nicht deaktivieren
- Meine Suchanfrage schlägt fehl
- Ich sehe, dass eine Kontrolldomäne als „veraltet“ markiert ist. Was bedeutet das?

Probleme mit dem Beweiserhebungs-Bewertungsbericht

- Ich kann aus meinen Suchergebnissen nicht mehrere Bewertungsberichte erstellen
- Ich kann keine spezifischen Beweise aus meinen Suchergebnissen hinzufügen
- Nicht alle meine Beweiserhebungsergebnisse sind im Bewertungsbericht enthalten
- Ich möchte aus meinen Suchergebnissen einen Bewertungsbericht erstellen, aber meine Anfrage schlägt fehl
- Weitere Ressourcen

Probleme mit dem CSV-Export der Beweiserhebung

- Mein CSV-Export ist fehlgeschlagen
- Ich kann keine bestimmten Beweise aus meinen Suchergebnissen exportieren

- Ich kann nicht mehrere CSV-Dateien gleichzeitig exportieren

Ich kann die Beweiserhebung nicht aktivieren

Häufige Gründe, warum Sie die Beweiserhebung nicht aktivieren können, bestehen in den folgenden Situationen:

Ihnen fehlen Berechtigungen

Wenn Sie zum ersten Mal versuchen, Evidence Finder zu aktivieren, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um Evidence Finder zu aktivieren. Diese Berechtigungen ermöglichen es Ihnen, einen Ereignisdatenspeicher in CloudTrail Lake zu erstellen und zu verwalten, der zur Unterstützung von Suchanfragen im Evidence Finder erforderlich ist. Mit den Berechtigungen können Sie dann Beweiserhebungsanfragen durchführen.

Wenn Sie Hilfe mit den Berechtigungen benötigen, wenden Sie sich an Ihren AWS Administrator. Wenn Sie ein AWS Administrator sind, können Sie die erforderliche Berechtigungserklärung kopieren und an eine IAM-Richtlinie anhängen.

Sie verwenden Ihr Organizations-Verwaltungskonto

Berücksichtigen Sie, dass Sie Ihr Verwaltungskonto nicht verwenden können, um die Beweiserhebung zu aktivieren. Melden Sie sich als delegiertes Administratorkonto an, und versuchen Sie es erneut.

Sie haben die Beweiserhebung zuvor deaktiviert

Die erneute Aktivierung der Beweiserhebung wird derzeit nicht unterstützt. Wenn Sie die Beweiserhebung zuvor deaktiviert haben, können Sie sie nicht erneut aktivieren.

Ich habe die Beweiserhebung aktiviert, sehe aber in meinen Suchergebnissen keine Beweise aus der Vergangenheit

Wenn Sie die Beweiserhebung aktivieren, dauert es bis zu 7 Tage, bis all Ihre Daten zu früheren Beweisen verfügbar sind.

Während dieses Zeitraums von 7 Tagen wird ein Ereignisdatenspeicher mit Beweisdaten aus den letzten zwei Jahren aufgefüllt. Das bedeutet, dass, wenn Sie die Beweiserhebung unmittelbar nach der Aktivierung verwenden, nicht alle Ergebnisse verfügbar sind, bis der Vorgang abgeschlossen ist.

Anweisungen, wie Sie den Status des Daten-Backfills überprüfen können, finden Sie unter. Bestätigung des Status von Evidence Finder

Ich kann die Beweiserhebung nicht deaktivieren

Dies kann durch einen der folgenden Gründe bedingt sein.

Ihnen fehlen Berechtigungen

Wenn Sie versuchen, Evidence Finder zu deaktivieren, vergewissern Sie sich, dass Sie über die erforderlichen Berechtigungen verfügen, um Evidence Finder zu deaktivieren. Mit diesen Berechtigungen können Sie einen Ereignisdatenspeicher in CloudTrail Lake aktualisieren und löschen. Dies ist erforderlich, um den Evidence Finder zu deaktivieren.

Wenn Sie Hilfe mit den Berechtigungen benötigen, wenden Sie sich an Ihren AWS Administrator. Wenn Sie ein AWS Administrator sind, können Sie die erforderliche Berechtigungserklärung kopieren und an eine IAM-Richtlinie anhängen.

Eine Anfrage zur Aktivierung der Beweiserhebung ist noch in Bearbeitung

Wenn Sie die Aktivierung der Beweiserhebung beantragen, erstellen wir einen Ereignisdatenspeicher, der Anfragen zur Beweiserhebung unterstützt. Sie können die Beweiserhebung nicht deaktivieren, während der Ereignisdatenspeicher erstellt wird.

Warten Sie, bis der Ereignisdatenspeicher erstellt wurde, und versuchen Sie es erneut, um fortzufahren. Weitere Informationen finden Sie unter Bestätigung des Status von Evidence Finder .

Sie haben bereits beantragt, die Beweiserhebung zu deaktivieren

Wenn Sie die Deaktivierung der Beweiserhebung beantragen, löschen wir den Ereignisdatenspeicher, der für Beweiserhebungsanfragen verwendet wird. Wenn Sie erneut versuchen, die Beweiserhebung zu deaktivieren, während der Ereignisdatenspeicher gelöscht wird, erhalten Sie eine Fehlermeldung.

In diesem Fall ist keine Aktion erforderlich. Warten Sie, bis der Ereignisdatenspeicher gelöscht ist. Sobald dieser Vorgang abgeschlossen ist, ist die Beweiserhebung deaktiviert. Weitere Informationen finden Sie unter Bestätigung des Status von Evidence Finder .

Meine Suchanfrage schlägt fehl

Eine fehlgeschlagene Suchanfrage kann einen der folgenden Gründe haben:

Ihnen fehlen Berechtigungen

Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, um Suchanfragen auszuführen und auf die Suchergebnisse zuzugreifen. Insbesondere benötigen Sie Berechtigungen für die folgenden CloudTrail Aktionen:

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Wenn Sie Hilfe mit Berechtigungen benötigen, wenden Sie sich an Ihren AWS Administrator. Wenn Sie ein AWS Administrator sind, können Sie die erforderliche Berechtigungserklärung kopieren und an eine IAM-Richtlinie anhängen.

Sie führen die maximale Anzahl von Anfragen aus

Sie können bis zu 5 Anfragen gleichzeitig ausführen. Wenn Sie die maximale Anzahl gleichzeitiger Anfragen ausführen, führt dies zu einem `MaxConcurrentQueriesException`-Fehler. Wenn Sie diese Fehlermeldung erhalten, warten Sie eine Minute, bis einige Anfragen abgeschlossen sind, und führen Sie die Anfrage dann erneut aus.

Ihre Anfrageanweisung weist einen Validierungsfehler auf

Wenn Sie die API oder CLI verwenden, um den CloudTrail StartQueryLake-Vorgang auszuführen, stellen Sie sicher, dass Ihre gültig `queryStatement` ist. Wenn die Anfrageanweisung Validierungsfehler, falsche Syntax oder nicht unterstützte Schlüsselwörter enthält, führt dies zu einem `InvalidQueryStatementException`.

Weitere Informationen zum Schreiben einer Anfrage finden Sie unter Erstellen oder Bearbeiten einer Anfrage im AWS CloudTrail -Benutzerhandbuch.

Beispiele für gültige Syntax finden Sie in den folgenden Beispielen für Anfrageanweisungen, die zur Anfrage eines Audit Manager-Ereignisdatenspeichers verwendet werden können.

Beispiel 1: Untersuchen Sie Beweise und deren Konformitätsstatus

In diesem Beispiel werden Beweise mit beliebigem Konformitätsstatus in allen Bewertungen innerhalb eines bestimmten Zeitraums gefunden.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Beispiel 2: Ermitteln Sie die Nichtkonformität von Beweisen für eine Kontrolle

In diesem Beispiel werden alle nicht konformen Beweise in einem angegebenen Datumsbereich für eine bestimmte Bewertung und Kontrolle gefunden.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Beispiel 3: Zählen Sie Beweise nach Namen

In diesem Beispiel werden die gesamten Beweise für eine Bewertung in einem bestimmten Zeitraum aufgeführt, gruppiert nach Namen und sortiert nach Anzahl der Beweise.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Beispiel 4: Untersuchen Sie die Beweise nach Datenquelle und Dienst

In diesem Beispiel werden alle Beweise in einem angegebenen Datumsbereich für eine bestimmte Datenquelle und einen bestimmten Dienst gefunden.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Beispiel 5: Untersuchen Sie konforme Beweise nach Datenquelle und Kontrolldomain

In diesem Beispiel werden konforme Beweise für bestimmte Kontrolldomain gefunden, wobei die Beweise aus einer Datenquelle stammen, die nicht AWS Config ist.

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
```

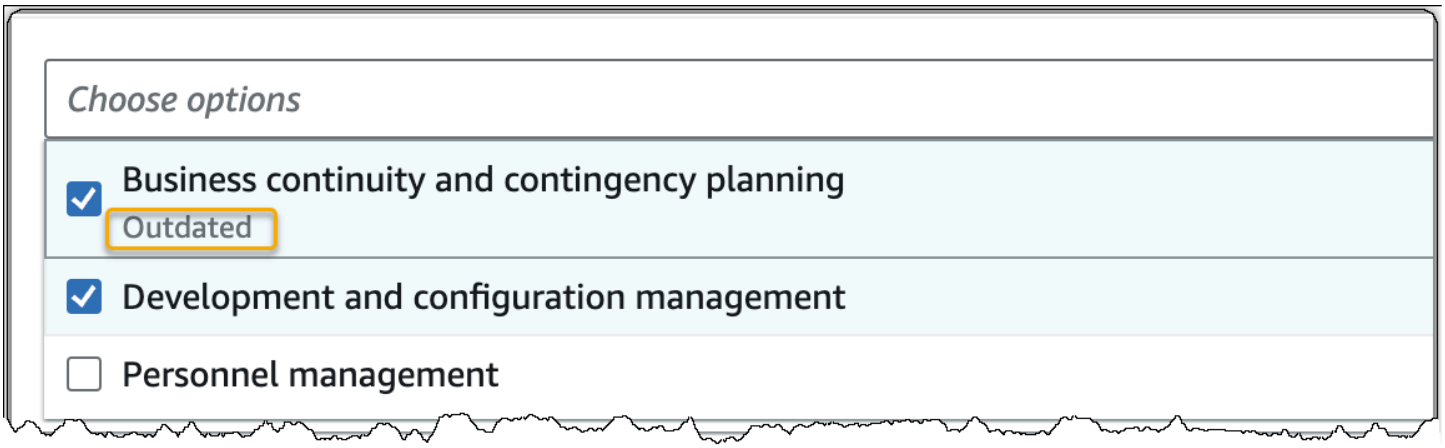
```
monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
Config')
```

Andere API-Ausnahmen

Die StartQueryAPI kann aus verschiedenen anderen Gründen fehlschlagen. Eine vollständige Liste möglicher Fehler und Beschreibungen finden Sie unter StartQuery Fehler in der AWS CloudTrail API-Referenz.

Ich sehe, dass eine Kontrolldomäne als „veraltet“ markiert ist. Was bedeutet das?

Wenn Sie im Evidence Finder einen Kontrolldomänenfilter anwenden, stellen Sie möglicherweise fest, dass einige verfügbare Kontrolldomänen als veraltet beschrieben werden.



Ab dem 6. Juni 2024 unterstützt Audit Manager eine neue Reihe von Kontrolldomänen, die von AWS Control Catalog bereitgestellt werden. Eine Liste dieser Kontrolldomänen finden Sie ListDomainsin der AWS Control Catalog API-Referenz.

Wenn eine Kontrolldomäne als veraltet markiert ist, bedeutet dies, dass es sich bei der angezeigten Kontrolldomäne nicht um eine der neuen Kontrolldomänen handelt, die von AWS Control Catalog bereitgestellt werden. Audit Manager unterstützt diese veralteten Kontrolldomänen weiterhin, sodass Sie sie weiterhin als Kriterien für die Suche nach Beweisen verwenden können.

Wir unterstützen zwar weiterhin die veralteten Kontrolldomänen, empfehlen Ihnen jedoch, stattdessen die neuen Kontrolldomänen zu verwenden. Die neuen Kontrolldomänen sind den aktualisierten Standardsteuerungen zugeordnet, die am 6. Juni 2024 als Teil der Common Controls Library eingeführt wurden. An diesem Tag haben wir aktualisierte Standardkontrollen veröffentlicht, mit

denen Beweise aus AWS verwalteten Quellen gesammelt werden können. Das bedeutet, dass Audit Manager jedes Mal, wenn die zugrunde liegenden Datenquellen für eine gemeinsame oder zentrale Kontrolle aktualisiert werden, dieselbe Aktualisierung automatisch auf alle zugehörigen Standardkontrollen anwendet.

Ich kann aus meinen Suchergebnissen nicht mehrere Bewertungsberichte erstellen

Dieser Fehler wird dadurch verursacht, dass zu viele CloudTrail Lake-Abfragen gleichzeitig ausgeführt werden.

Dieser Fehler kann auftreten, wenn Sie Ihre Suchergebnisse gruppieren und versuchen, sofort Bewertungsberichte für jeden einzelnen Eintrag in Ihren gruppierten Ergebnissen zu erstellen. Wenn Sie Ihre Suchergebnisse abrufen und einen Bewertungsbericht erstellen, ruft jede Aktion eine Anfrage auf. Sie können nur bis zu fünf Anfragen gleichzeitig ausführen. Wenn Sie die maximale Anzahl gleichzeitiger Anfragen ausführen, wird ein `MaxConcurrentQueriesException`-Fehler zurückgegeben.

Um diesen Fehler zu vermeiden, stellen Sie sicher, dass Sie nicht zu viele Bewertungsberichte gleichzeitig generieren. Wenn Sie die maximale Anzahl gleichzeitiger Anfragen ausführen, wird ein `MaxConcurrentQueriesException`-Fehler zurückgegeben. Wenn Sie diese Fehlermeldung erhalten, warten Sie einige Minuten, bis Ihre in Bearbeitung befindlichen Bewertungsberichte abgeschlossen sind.

Sie können den Status Ihrer Bewertungsberichte auf der Download-Center-Seite in der Audit Manager-Konsole überprüfen. Wenn Ihre Berichte fertig sind, kehren Sie zu Ihren gruppierten Ergebnissen in der Beweiserhebung zurück. Anschließend können Sie mit dem Abrufen der Ergebnisse fortfahren und für jede Position einen Bewertungsbericht erstellen.

Ich kann keine spezifischen Beweise aus meinen Suchergebnissen hinzufügen

Alle Ihre Suchergebnisse sind im Bewertungsbericht enthalten. Sie können einzelne Zeilen aus Ihren Suchergebnissen nicht selektiv hinzufügen.

Wenn Sie nur bestimmte Suchergebnisse in den Bewertungsbericht aufnehmen möchten, empfehlen wir Ihnen, Ihre aktuellen Suchfilter zu bearbeiten. Auf diese Weise können Sie Ihre Ergebnisse so eingrenzen, dass sie nur auf die Beweise abzielen, die Sie in den Bericht aufnehmen möchten.

Nicht alle meine Beweiserhebungsergebnisse sind im Bewertungsbericht enthalten

Wenn Sie einen Bewertungsbericht erstellen, ist die Anzahl der Beweise, die Sie hinzufügen können, begrenzt. Das Limit basiert auf Ihrer Bewertung, der Region AWS-Region des S3-Buckets, der als Ziel für Ihren Bewertungsbericht verwendet wird, und darauf, ob für Ihre Bewertung ein vom Kunden verwaltetes System verwendet wird AWS KMS key.

1. Die Obergrenze liegt bei 22.000 für Berichte in derselben Region (bei denen sich der S3-Bucket und die Bewertung im selben AWS-Region befinden).
2. Die Obergrenze liegt bei 3.500 für regionsübergreifende Berichte (bei denen sich der AWS-Regionen des S3-Bucket und der Bewertung unterscheiden).
3. Die Obergrenze liegt bei 3.500, wenn für die Bewertung ein vom Kunden verwalteter KMS-Schlüssel verwendet wird.

Wenn Sie diese Grenze überschreiten, wird der Bericht trotzdem erstellt. Audit Manager fügt dem Bericht jedoch nur die ersten 3.500 oder 22.000 Beweiselemente hinzu.

Um dieses Problem zu vermeiden, empfehlen wir Ihnen, Ihre aktuellen Suchfilter zu bearbeiten. Auf diese Weise können Sie Ihre Suchergebnisse reduzieren, indem Sie auf eine geringere Anzahl von Beweisen abzielen. Bei Bedarf können Sie diese Methode wiederholen und mehrere kleinere Bewertungsberichte anstelle eines größeren Berichts erstellen.

Ich möchte aus meinen Suchergebnissen einen Bewertungsbericht erstellen, aber meine Anfrage schlägt fehl

Wenn Sie die CreateAssessmentReportAPI verwenden und Ihre Abfrageanweisung eine Validierungsausnahme zurückgibt, finden Sie in der folgenden Tabelle Anleitungen zur Behebung des Problems.

> **Note**
>
> Selbst wenn eine Abfrageanweisung funktioniert CloudTrail, ist dieselbe Abfrage möglicherweise nicht für die Erstellung von Bewertungsberichten in Audit Manager gültig. Dies liegt an einigen Unterschieden bei der Anfragevalidierung zwischen den beiden Diensten.

Klausel	Problem	Lösung	Hinweise
`SELECT`	Die `SELECT`-Klausel enthält einen Spaltennamen	Entfernen Sie die `SELECT`-Klausel und ersetzen Sie sie durch `SELECT eventJson .`	Nur `SELECT eventJson` wird unterstützt. Diese Validierung wird von Audit Manager durchgeführt.
`FROM`	Die `FROM`-Klausel enthält eine ungültige ID für den Ereignisdatenspeicher oder Die angegebene Ereignisdatenspeicher-ID stimmt nicht mit der Ereignisdatenspeicher-ID in Ihren Audit Manager-Einstellungen überein	Entfernen Sie die `FROM`-Klausel und ersetzen Sie sie durch `FROM edsID`, wobei der Wert von `edsID` der ID des Ereignisdatenspeichers entspricht, die in Ihren Audit Manager-Einstellungen angegeben ist. Sie können den ARN des Ereignisdatenspeichers über Ihre Audit Manager-Einstellungen abrufen. Weitere Informationen finden Sie unter GetSettings in der AWS Audit Manager - API-Referenz.	Diese Validierung wird von Audit Manager durchgeführt.
`GROUP BY`	In der Anfrage ist eine `GROUP BY`-Klausel vorhanden	Entfernen Sie die `GROUP BY`-Klausel.	Diese Validierung wird von Audit Manager durchgeführt.
`HAVING`	In der Anfrage ist eine `HAVING`-Klausel vorhanden	Entfernen Sie die `HAVING`-Klausel.	Diese Validierung wird von Audit Manager durchgeführt.
`LIMIT`	Die `LIMIT`-Klausel enthält einen Wert, der den maximal zulässigen	Wenn die `LIMIT`-Klausel existiert, stellen Sie sicher, dass ihr Wert gleich oder kleiner als der maximal unterstützte Grenzwert ist:	In der Konsole gibt es keine Beschränkungen in Bezug auf die Anzahl der Beweisergebnisse, die zurückgegeben werden

Klausel	Problem	Lösung	Hinweise
	Grenzwert überschreitet	• Für Berichte aus derselben Region liegt der Grenzwert bei 22.000; • Für regionsübergreifende Berichte liegt der Grenzwert bei 3.500; • Für Berichte, bei denen für die zugehörige Bewertung ein vom Kunden verwalteter Benutzer verwendet wird AWS KMS key, liegt der Grenzwert bei 3.500	können. Bei der Erstellung eines Bewertungsberichts gilt jedoch eine Obergrenze für die Anzahl der Beweise, die Sie hinzufügen können. Wenn in Ihrer Anfragean weisung kein `LIMIT`-Wert angegeben ist, werden die standardmäßigen Höchstgrenzen angewendet. Diese Validierung wird von Audit Manager durchgeführt.
`ORDER BY`	Die `ORDER BY`-Klausel enthält Aggregat-Funktionen oder Aliase, die in der `SELECT`-Klausel nicht enthalten sind	Stellen Sie sicher, dass die `ORDER BY`-Klausel keine Bedingungen enthält, die Aggregat-Funktionen oder Aliase verwenden.	Diese Validierung wird von der CloudTrail StartQuery API abgewickelt.

Klausel	Problem	Lösung	Hinweise
`WHERE`	Die `WHERE`-Klausel enthält mehr als eine `assessmentId` oder Die `WHERE`-Klausel enthält eine `assessmentId` , die nicht mit der `assessmentId` in Ihrer `createAssessmentReport` Anfrage übereinstimmt oder Die `WHERE`-Klausel enthält einen Spaltennamen, der nicht unterstützt wird	Stellen Sie sicher, dass nur eine Bewertungs-ID angegeben ist und dass diese mit dem Bewertungs-ID-Parameter übereinstimmt, den Sie in der `createAssessmentReport` API-Anforderung angegeben haben. Entfernen Sie alle nicht unterstützten Spaltennamen.	Diese Validierung wird von der CloudTrail StartQuery API abgewickelt.

Beispiele

Die folgenden Beispiele zeigen, wie Sie den `queryStatement` Parameter beim Aufrufen der CreateAssessmentReportOperation verwenden können. Bevor Sie diese Abfragen verwenden, ersetzen Sie die *`placeholder text`* durch Ihre eigenen `assessmentId` Werte `edsId` und.

Beispiel 1: Einen Bericht erstellen (es gilt das Limit für dieselbe Region)

In diesem Beispiel wird ein Bericht erstellt, der Ergebnisse für S3-Buckets enthält, die zwischen dem 22. und 23. Januar 2022 erstellt wurden.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Beispiel 2: Einen Bericht erstellen (es gilt ein regionsübergreifendes Limit)

In diesem Beispiel wird ein Bericht erstellt, der alle Ergebnisse für den angegebenen Ereignisdatenspeicher und die angegebene Bewertung enthält, ohne dass ein Datumsbereich angegeben ist.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Beispiel 3: Erstellen eines Berichts (unter dem Standardlimit)

In diesem Beispiel wird ein Bericht erstellt, der alle Ergebnisse für den angegebenen Ereignisdatenspeicher und die angegebene Bewertung enthält, wobei der Grenzwert unter dem Standardmaximum liegt.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Weitere Ressourcen

Die folgende Seite enthält allgemeine Anleitungen zur Fehlerbehebung bei Bewertungsberichten:

- Behebung von Bewertungsberichtfehlern

Mein CSV-Export ist fehlgeschlagen

Ihr CSV-Export kann aus verschiedenen Gründen fehlschlagen. Sie können dieses Problem beheben, indem Sie die häufigsten Ursachen überprüfen.

Stellen Sie zunächst sicher, dass Sie die Voraussetzungen für die Verwendung der CSV-Export-Funktion erfüllen:

Sie haben die Beweiserhebung erfolgreich aktiviert

> Wenn Sie die Beweiserhebung nicht aktiviert haben, können Sie keine Suchanfrage ausführen und Ihre Suchergebnisse nicht exportieren.

Das Auffüllen Ihres Ereignisdatenspeichers ist abgeschlossen

Wenn Sie die Beweiserhebung unmittelbar nach der Aktivierung verwenden und das Auffüllen von Beweisen noch nicht abgeschlossen ist, kann es sein, dass einige Ergebnisse nicht verfügbar sind. Informationen zum Überprüfen des Auffüllstatus finden Sie unterBestätigung des Status von Evidence Finder .

Ihre Suchanfrage war erfolgreich

Audit Manager kann die Ergebnisse einer fehlgeschlagenen Anfrage nicht exportieren. Informationen zur Behebung einer fehlgeschlagenen Anfrage finden Sie unter Meine Suchanfrage schlägt fehl.

Nachdem Sie bestätigt haben, dass Sie die Voraussetzungen erfüllen, können Sie anhand der folgenden Checkliste nach potenziellen Problemen suchen:

1. Überprüfen Sie den Status der Suchanfrage:
   a. Wurde die Anfrage storniert? Die Beweiserhebung zeigt Teilergebnisse an, die vor dem Abbruch der Anfrage verarbeitet wurden. Audit Manager exportiert jedoch keine Teilergebnisse in Ihren S3-Bucket oder das Download-Center.
   b. Läuft die Anfrage seit über einer Stunde? Abfragen, die länger als eine Stunde laufen, können ablaufen. Die Beweiserhebung zeigt Teilergebnisse an, die vor dem Timeout der Anfrage verarbeitet wurden. Audit Manager exportiert jedoch keine Teilergebnisse. Um eine Zeitüberschreitung zu vermeiden, können Sie die Anzahl der gescannten Beweise reduzieren, indem Bearbeiten von Suchfiltern Sie einen engeren Zeitraum angeben.
2. Überprüfen Sie den Namen und die URI Ihres S3-Buckets für das Exportziel:
   a. Existiert der von Ihnen angegebene Bucket? Wenn Sie eine Bucket-URI manuell eingegeben haben, stellen Sie sicher, dass Sie nichts falsch eingegeben haben. Ein Tippfehler oder eine falsche URI können zu einem `RESOURCE_NOT_FOUND`-Fehler führen, wenn Audit Manager versucht, die CSV-Datei nach Amazon S3 zu exportieren.
3. Überprüfen Sie die Berechtigungen Ihres S3-Buckets für Ihr Exportziel:
   a. Verfügen Sie über Schreibberechtigungen für den S3-Bucket? Sie müssen über Schreibberechtigungen für den S3-Bucket verfügen, der als Exportziel verwendet wird. Insbesondere muss die IAM-Berechtigungsrichtlinie eine `s3:PutObject` Aktion und den Bucket-ARN enthalten und CloudTrail als Dienstprinzipal auflisten. Wir stellen Ihnen eine Beispielrichtlinie zur Verfügung, die Sie befolgen können.
4. Prüfen Sie, ob Ihre AWS-Region Informationen nicht übereinstimmen:

a. Stimmt AWS-Region der Schlüssel Ihres vom Kunden verwalteten AWS-Region Schlüssels mit Ihrer Bewertung überein? Wenn Sie einen vom Kunden verwalteten Schlüssel für die Datenverschlüsselung angegeben haben, muss dieser im selben AWS-Region hinterlegt sein, wie Ihre Bewertung. Anweisungen zum Ändern des KMS-Schlüssels finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen.

5. Überprüfen Sie die Berechtigungen Ihres delegierten Administratorkontos:

a. Erteilt der vom Kunden verwaltete Schlüssel in Ihren Audit Manager-Einstellungen Ihrem delegierten Administrator Berechtigungen? Wenn Sie ein delegiertes Administratorkonto verwenden und einen vom Kunden verwalteten Schlüssel für die Datenverschlüsselung angegeben haben, stellen Sie sicher, dass der delegierte Administrator Zugriff auf diesen KMS-Schlüssel hat. Weitere Informationen finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service -Entwicklerhandbuch. Informationen zum Überprüfen und Ändern Ihrer Verschlüsselungseinstellungen in Audit Manager finden Sie unterKonfiguration Ihrer Datenverschlüsselungseinstellungen.

> **Note**
>
> Wenn Sie Ihre Audit Manager-Datenverschlüsselungseinstellungen ändern, gelten diese Änderungen für neue Bewertungen, die Sie in Zukunft erstellen. Dies schließt alle CSV-Dateien mit ein, die Sie aus Ihren neuen Bewertungen exportieren.
> Die Änderungen gelten nicht für bestehende Bewertungen, die Sie erstellt haben, bevor Sie Ihre Verschlüsselungseinstellungen geändert haben. Dazu gehören neue CSV-Exporte aus bestehenden Bewertungen, zusätzlich zu den bereits vorhandenen CSV-Exporten. Bestehende Bewertungen – und alle ihre CSV-Exporte – verwenden weiterhin den alten KMS-Schlüssel. Wenn die IAM-Identität, die die CSV-Datei exportiert, nicht berechtigt ist, den alten KMS-Schlüssel zu verwenden, können Sie Berechtigungen auf der Ebene der wichtigsten Richtlinien gewähren.

Ich kann keine bestimmten Beweise aus meinen Suchergebnissen exportieren

Alle Ihre Suchergebnisse sind in den Ergebnissen enthalten.

Wenn Sie nur bestimmte Beweise in die CSV-Datei aufnehmen möchten, empfehlen wir Ihnen, Ihre aktuellen Suchfilter zu bearbeiten. Auf diese Weise können Sie Ihre Ergebnisse einschränken, sodass nur die Beweise angezeigt werden, die Sie exportieren möchten.

Ich kann nicht mehrere CSV-Dateien gleichzeitig exportieren

Dieser Fehler wird dadurch verursacht, dass zu viele CloudTrail Lake-Abfragen gleichzeitig ausgeführt werden.

Dies kann passieren, wenn Sie Ihre Suchergebnisse gruppieren und versuchen, für jeden Zeileneintrag in Ihren gruppierten Ergebnissen sofort eine CSV-Datei zu exportieren. Wenn Sie Ihre Suchergebnisse abrufen und eine CSV-Datei exportieren, ruft jede dieser Aktionen eine Anfrage auf. Sie können nur bis zu fünf Anfragen gleichzeitig ausführen. Wenn Sie die maximale Anzahl gleichzeitiger Anfragen ausführen, wird ein `MaxConcurrentQueriesException`-Fehler zurückgegeben.

Um diesen Fehler zu vermeiden, stellen Sie sicher, dass Sie nicht zu viele CSV-Dateien gleichzeitig exportieren.

Um diesen Fehler zu beheben, warten Sie, bis Ihre laufenden CSV-Exporte abgeschlossen sind. Die meisten Exporte dauern nur wenige Minuten. Wenn Sie jedoch eine sehr große Datenmenge exportieren, kann es bis zu einer Stunde dauern, bis der Export abgeschlossen ist. Sie können die Beweiserhebung jederzeit verlassen, während der Export läuft.

Sie können dabei den Exportstatus jederzeit im Download-Center in der Audit Manager-Konsole überprüfen. Wenn Ihre exportierten Dateien fertig sind, kehren Sie zu Ihren gruppierten Ergebnissen in der Beweiserhebung zurück. Sie können dann mit dem Abrufen der Ergebnisse fortfahren und für jeden Einzelposten eine CSV-Datei exportieren.

Behebung von Framework-Problemen

Sie können die Informationen auf dieser Seite verwenden, um häufig auftretende Framework-Probleme in Audit Manager zu lösen.

Allgemeine Probleme mit dem Framework

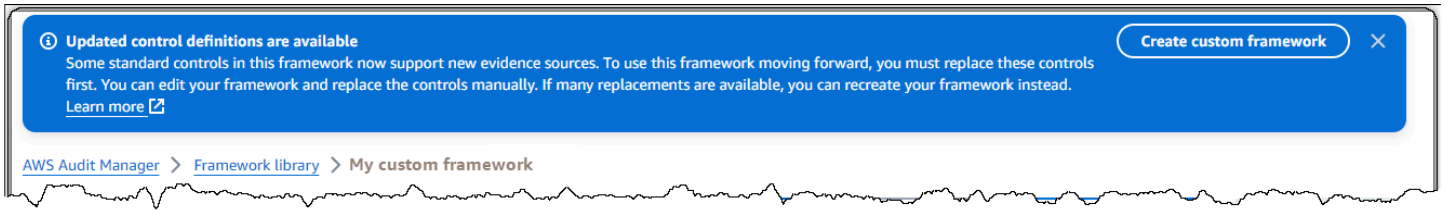
- Auf der Detailseite meines benutzerdefinierten Frameworks werde ich aufgefordert, mein benutzerdefiniertes Framework neu zu erstellen

- Ich kann keine Kopie meines benutzerdefinierten Frameworks erstellen

Probleme bei der gemeinsamen Nutzung von Rahmenbedingungen

- Der Status meiner gesendeten Freigabeanfrage wird als Fehlgeschlagen angezeigt
- Neben meiner Anfrage zum Teilen ist ein blauer Punkt zu sehen. Was bedeutet das?
- Mein gemeinsames Framework verfügt über Steuerelemente, die benutzerdefinierte AWS Config Regeln als Datenquelle verwenden. Kann der Empfänger Beweise für diese Kontrollen sammeln?
- Ich habe eine benutzerdefinierte Regel aktualisiert, die in einem freigegebenen Framework verwendet wird. Muss ich irgendwelche Aktion durchführen?

Auf der Detailseite meines benutzerdefinierten Frameworks werde ich aufgefordert, mein benutzerdefiniertes Framework neu zu erstellen



Wenn Sie eine Meldung mit dem Hinweis sehen, dass aktualisierte Kontrolldefinitionen verfügbar sind, bedeutet dies, dass Audit Manager jetzt neuere Definitionen für einige der Standardsteuerelemente bereitstellt, die sich in Ihrem benutzerdefinierten Framework befinden.

Standardsteuerungen können jetzt Beweise sammeln vonAWS managed source. Das bedeutet, dass jedes Mal, wenn Audit Manager die zugrunde liegenden Datenquellen für eine gemeinsame oder zentrale Kontrolle aktualisiert, dasselbe Update automatisch auf die zugehörigen Standardkontrollen angewendet wird. Auf diese Weise können Sie die kontinuierliche Einhaltung der Vorschriften sicherstellen, wenn sich die Cloud-Compliance-Umgebung ändert. Um sicherzustellen, dass Sie von diesen AWS verwalteten Quellen profitieren, empfehlen wir Ihnen, die Kontrollen in Ihrem benutzerdefinierten Framework zu ersetzen.

In Ihrem benutzerdefinierten Framework gibt Audit Manager an, für welche Kontrollen Ersatz verfügbar ist. Sie müssen diese Steuerelemente ersetzen, bevor Sie eine Kopie Ihres benutzerdefinierten Frameworks erstellen können. Wenn Sie Ihr benutzerdefiniertes Framework das nächste Mal bearbeiten, werden Sie aufgefordert, diese Steuerelemente zusammen mit allen anderen Änderungen, die Sie vornehmen möchten, zu ersetzen.

Es gibt zwei Möglichkeiten, die Steuerelemente in Ihrem benutzerdefinierten Framework zu ersetzen:

1. Erstellen Sie Ihr benutzerdefiniertes Framework neu

Wenn für eine große Anzahl von Steuerelementen Ersatzprodukte verfügbar sind, empfehlen wir Ihnen, Ihr benutzerdefiniertes Framework neu zu erstellen. Dies ist wahrscheinlich die beste Option, wenn Ihr benutzerdefiniertes Framework auf einem Standard-Framework basiert.

- Nehmen wir zum Beispiel an, Sie haben Ihr benutzerdefiniertes Framework NIST SP 800-53 Rev. 5 als Ausgangspunkt erstellt. Dieses Standard-Framework hat 1007 Standardsteuerelemente, und Sie haben 20 benutzerdefinierte Steuerelemente hinzugefügt.
- In diesem Fall besteht die effizienteste Option darin, `NIST 800-53 (Rev. 5) Low-Moderate-High` in der Framework-Bibliothek nach einer bearbeitbaren Kopie dieses Frameworks zu suchen und zu erstellen. Während dieses Vorgangs können Sie dieselben 20 benutzerdefinierten Steuerelemente hinzufügen, die Sie zuvor verwendet haben. Da Sie jetzt die neueste Definition des Standard-Frameworks als Ausgangspunkt verwenden, erbt Ihr benutzerdefiniertes Framework automatisch die neuesten Definitionen für alle 1007 Standardsteuerelemente.

2. Bearbeiten Sie Ihr benutzerdefiniertes Framework

Wenn für eine kleine Anzahl von Steuerelementen Ersatz verfügbar ist, empfehlen wir Ihnen, Ihr benutzerdefiniertes Framework zu bearbeiten und die Steuerelemente manuell zu ersetzen.

- Nehmen wir zum Beispiel an, Sie haben Ihr benutzerdefiniertes Framework von Grund auf neu erstellt. In Ihrem benutzerdefinierten Framework haben Sie 20 benutzerdefinierte Steuerelemente, die Sie selbst erstellt haben, und acht Standardsteuerelemente aus dem ACSC Essential Eight Standard-Framework hinzugefügt.
- Da in diesem Fall Updates für maximal acht Steuerelemente verfügbar wären, besteht die effizienteste Option darin, Ihr benutzerdefiniertes Framework zu bearbeiten und diese Steuerelemente nacheinander zu ersetzen. Detaillierte Informationen finden Sie in der Anleitung unten.

Um Steuerelemente in Ihrem benutzerdefinierten Framework manuell zu ersetzen

Um Steuerelemente in Ihrem benutzerdefinierten Framework manuell zu ersetzen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.

2. Wählen Sie im linken Navigationsbereich die Framework-Bibliothek und dann die Registerkarte Benutzerdefinierte Frameworks aus.
3. Wählen Sie das zu bearbeitende Framework aus, klicken Sie auf Aktionen und dann auf Bearbeiten.
4. Wählen Sie auf der Seite „Framework-Details bearbeiten“ die Option Weiter aus.
5. Überprüfen Sie auf der Seite „Kontrollsätze bearbeiten“ die Namen der einzelnen Kontrollsätze, um festzustellen, ob für die zugehörigen Steuerelemente Ersatzprodukte verfügbar sind.
6. Wählen Sie einen betroffenen Kontrollsatz aus, um ihn zu erweitern und festzustellen, welche seiner Steuerelemente ersetzt werden müssen.

   > **Tip**
   >
   > Geben Sie **`Replacement available`** in das Suchfeld ein, um Steuerelemente schneller zu identifizieren.

7. Entfernen Sie die betroffenen Steuerelemente, indem Sie das Kontrollkästchen aktivieren und dann Aus dem Steuersatz entfernen wählen.
8. Fügen Sie dieselben Steuerelemente erneut hinzu. Diese Aktion ersetzt die Steuerelemente, die Sie gerade entfernt haben, durch die neueste Steuerelementdefinition.

   a. Verwenden Sie unter Steuerelemente hinzufügen die Dropdownliste Steuerelementtyp und wählen Sie Standardsteuerelemente aus.

   b. Suchen Sie den Ersatz für das Steuerelement, das Sie gerade entfernt haben.

      > **Tip**
      >
      > In einigen Fällen entspricht der Name des Ersatzsteuerelements möglicherweise nicht exakt dem Namen des Originals. In diesem Fall ist der Name des Ersatzsteuerelements dem Original wahrscheinlich sehr ähnlich. In seltenen Fällen kann ein Steuerelement durch zwei Steuerelemente ersetzt werden (oder umgekehrt).
      > Wenn Sie kein Ersatzsteuerelement finden können, empfehlen wir Ihnen, eine Teilsuche durchzuführen. Geben Sie dazu einen Teil des Namens des ursprünglichen Steuerelements oder ein Schlüsselwort ein, das dem entspricht, wonach Sie suchen. Sie können auch nach Konformitätstyp suchen, um die Ergebnisliste weiter einzugrenzen.

c. Aktivieren Sie das Kontrollkästchen neben einem Steuerelement und wählen Sie Zum Kontrollsatz hinzufügen aus.

d. Wählen Sie im daraufhin angezeigten Popup-Fenster zur Bestätigung die Option Hinzufügen aus.

9. Wiederholen Sie die Schritte 6-8 nach Bedarf, bis Sie alle Bedienelemente ausgetauscht haben.
10. Wählen Sie Weiter aus.
11. Wählen Sie auf der Seite Überprüfen und speichern die Option Änderungen speichern aus.

Ich kann keine Kopie meines benutzerdefinierten Frameworks erstellen

Wenn die Schaltfläche „Kopie erstellen“ auf der Framework-Detailseite nicht verfügbar ist, bedeutet dies, dass Sie einige der Steuerelemente in Ihrem benutzerdefinierten Framework ersetzen müssen.

Anweisungen zum weiteren Vorgehen finden Sie unterAuf der Detailseite meines benutzerdefinierten Frameworks werde ich aufgefordert, mein benutzerdefiniertes Framework neu zu erstellen.

Der Status meiner gesendeten Freigabeanfrage wird als Fehlgeschlagen angezeigt

Wenn Sie versuchen, ein benutzerdefiniertes Framework zu teilen und der Vorgang fehlschlägt, empfehlen wir Ihnen, Folgendes zu überprüfen:

1. Stellen Sie sicher, dass Audit Manager in der Empfängerregion AWS-Konto und in der angegebenen Region aktiviert ist. Eine Liste der unterstützten AWS Audit Manager Regionen finden Sie unter AWS Audit Manager Endpunkte und Kontingente in der Amazon Web Services General Reference.
2. Vergewissern Sie sich, dass Sie bei der Angabe des Empfängerkontos die richtige AWS-Konto ID eingegeben haben.
3. Stellen Sie sicher, dass Sie kein AWS Organizations Verwaltungskonto als Empfänger angegeben haben. Sie können ein benutzerdefiniertes Framework mit einem delegierten Administrator teilen, aber wenn Sie versuchen, ein benutzerdefiniertes Framework mit einem Verwaltungskonto zu teilen, schlägt der Vorgang fehl.
4. Wenn Sie einen vom Kunden verwalteten Schlüssel zur Verschlüsselung Ihrer Audit Manager-Daten verwenden, stellen Sie sicher, dass Ihr KMS-Schlüssel aktiviert ist. Wenn Ihr KMS-Schlüssel deaktiviert ist und Sie versuchen, ein benutzerdefiniertes Framework gemeinsam zu nutzen,

schlägt der Vorgang fehl. Anweisungen zum Aktivieren eines deaktivierten KMS-Schlüssels finden Sie unter Aktivieren und Deaktivieren von Schlüsseln im AWS Key Management Service - Entwicklerhandbuch.

Neben meiner Anfrage zum Teilen ist ein blauer Punkt zu sehen. Was bedeutet das?

Eine Benachrichtigung mit einem blauen Punkt weist darauf hin, dass eine Freigabeanfrage Ihre Aufmerksamkeit erfordert.

Benachrichtigungen mit blauem Punkt für Absender

Ein blauer Benachrichtigungspunkt erscheint neben gesendeten Freigabeanfragen mit dem Status Läuft ab. Audit Manager zeigt die Benachrichtigung mit dem blauen Punkt an, sodass Sie den Empfänger daran erinnern können, Maßnahmen zur Freigabeanfrage zu ergreifen, bevor sie abläuft.

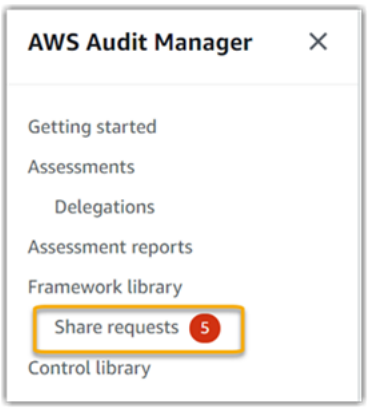
Damit der blaue Benachrichtigungspunkt verschwindet, muss der Empfänger die Anfrage annehmen oder ablehnen. Der blaue Punkt verschwindet auch, wenn Sie die Freigabeanfrage widerrufen.

Sie können das folgende Verfahren verwenden, um nach ablaufenden Freigabeanfragen zu suchen und dem Empfänger eine optionale Erinnerung zu senden, damit er Maßnahmen ergreifen kann.

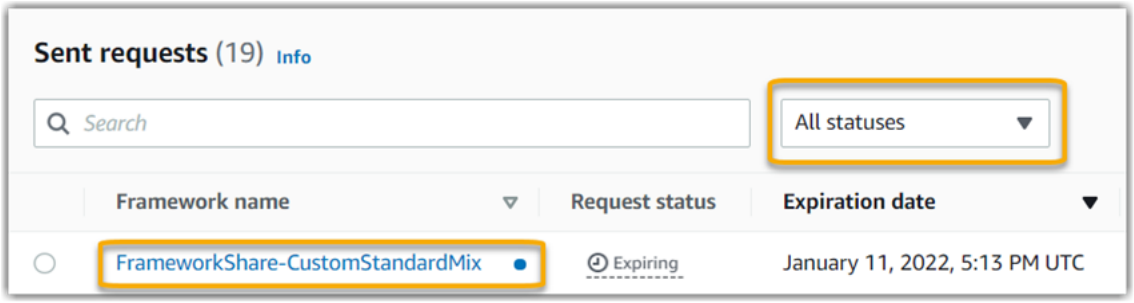
Um Benachrichtigungen für gesendete Anfragen einzusehen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wenn Sie eine Benachrichtigung über eine Freigabeanfrage haben, sehen Sie in Audit Manager einen roten Punkt neben dem Navigationssymbol.

3. Erweitern Sie den Navigationsbereich und suchen Sie nach Freigabeanfragen. Ein Benachrichtigungssymbol gibt die Anzahl der Freigabeanfragen an, die Aufmerksamkeit erfordern.



4. Wählen Sie Freigabeanfragen und dann die Registerkarte Gesendete Anfragen aus.
5. Halten Sie nach dem blauen Punkt Ausschau, um Freigabeanfragen zu kennzeichnen, die innerhalb der nächsten 30 Tage ablaufen. Alternativ dazu können Sie sich auch ablaufende Freigabeanträge anzeigen lassen, indem Sie aus dem Dropdown-Menü des Filters Alle Status die Option Läuft ab wählen.



6. (Optional) Erinnern Sie den Empfänger daran, dass er auf die Freigabeanfrage reagieren muss, bevor sie abläuft. Dieser Schritt ist optional, da Audit Manager eine Benachrichtigung in der Konsole sendet, um den Empfänger zu informieren, wenn eine Freigabeanfrage aktiv ist oder abläuft. Sie können dem Empfänger jedoch auch Ihre eigene Erinnerung über Ihren bevorzugten Kommunikationskanal senden.

Benachrichtigungen mit blauem Punkt für Empfänger

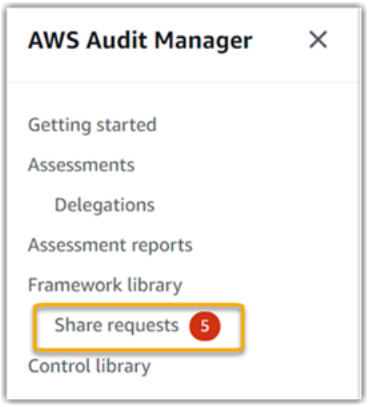
Neben eingegangenen Freigabeanfragen mit dem Status Aktiv oder Läuft ab wird ein blauer Benachrichtigungspunkt angezeigt. Audit Manager zeigt die Benachrichtigung mit dem blauen Punkt an, um Sie daran zu erinnern, Maßnahmen zur Freigabeanfrage zu ergreifen, bevor sie abläuft. Damit der blaue Benachrichtigungspunkt verschwindet, müssen Sie die Anfrage annehmen oder ablehnen. Der blaue Punkt verschwindet auch, wenn der Absender die Freigabeanfrage widerruft.

Mit dem folgenden Verfahren können Sie nach aktiven und ablaufenden Freigabeanfragen suchen.

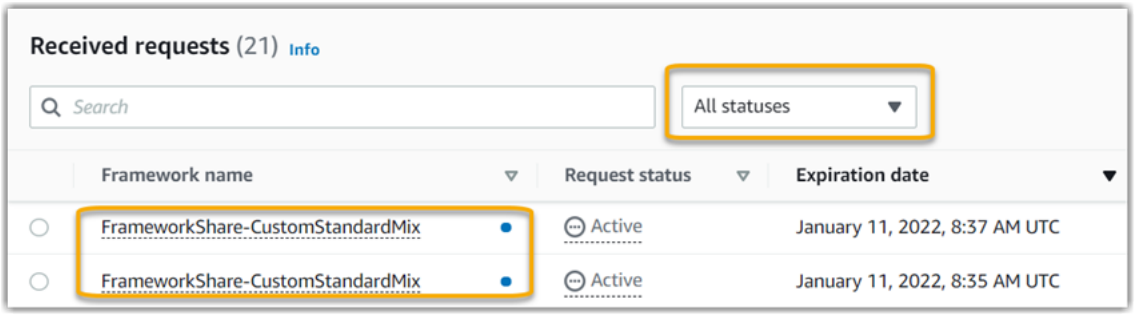
Um Benachrichtigungen für eingegangene Anfragen einzusehen

1. Öffnen Sie die AWS Audit Manager Manager-Konsole https://console.aws.amazon.com/auditmanager/zu Hause.
2. Wenn Sie eine Benachrichtigung über eine Freigabeanfrage haben, sehen Sie in Audit Manager einen roten Punkt neben dem Navigationssymbol.

3. Erweitern Sie den Navigationsbereich und suchen Sie nach Freigabeanfragen. Ein Benachrichtigungssymbol gibt die Anzahl der Freigabeanfragen an, die Ihre Aufmerksamkeit erfordern.



4. Wählen Sie Freigabeanfragen aus. Standardmäßig wird diese Seite auf der Registerkarte Empfangene Anfragen geöffnet.
5. Identifizieren Sie die Freigabeanfrage, die Sie bearbeiten müssen, indem Sie nach Elementen mit einem blauen Punkt suchen.



6. Um (optional) nur Anfragen anzuzeigen, die in den nächsten 30 Tagen ablaufen, suchen Sie in der Dropdownliste Alle Status nach und wählen Sie Läuft ab.

Mein gemeinsames Framework verfügt über Steuerelemente, die benutzerdefinierte AWS Config Regeln als Datenquelle verwenden. Kann der Empfänger Beweise für diese Kontrollen sammeln?

Ja, Ihr Empfänger kann Beweise für diese Kontrollen sammeln, aber dazu sind einige Schritte erforderlich.

Damit Audit Manager mithilfe einer AWS Config Regel als Datenquellenzuordnung Beweise sammeln kann, muss Folgendes zutreffen. Diese Kriterien gelten sowohl für verwaltete Regeln als auch für benutzerdefinierte Regeln.

- Die Regel muss in der AWS Umgebung des Empfängers vorhanden sein.
- Die Regel muss in der AWS Umgebung des Empfängers aktiviert sein.

Denken Sie daran, dass die AWS Config Regeln in Ihrem Konto wahrscheinlich nicht bereits in der AWS Umgebung des Empfängers existieren. Wenn der Empfänger die Freigabeanfrage akzeptiert, erstellt Audit Manager außerdem keine Ihrer benutzerdefinierten Regeln in seinem Konto neu. Damit der Empfänger anhand Ihrer benutzerdefinierten Regeln als Datenquellenzuordnung Beweise sammeln kann, muss er dieselben benutzerdefinierten Regeln in seiner Instanz von erstellen AWS Config. Nachdem der Empfänger die Regeln erstellt und anschließend aktiviert hat AWS Config, kann Audit Manager Beweise aus dieser Datenquelle sammeln.

Wir empfehlen Ihnen, mit dem Empfänger zu kommunizieren, um ihn darüber zu informieren, ob in seiner Instanz von benutzerdefinierte AWS Config Regeln erstellt werden sollen AWS Config.

Ich habe eine benutzerdefinierte Regel aktualisiert, die in einem freigegebenen Framework verwendet wird. Muss ich irgendwelche Aktion durchführen?

Für Regelaktualisierungen in Ihrer AWS Umgebung

Wenn Sie eine benutzerdefinierte Regel in Ihrer AWS Umgebung aktualisieren, sind keine Maßnahmen in Audit Manager erforderlich. Audit Manager erkennt und verarbeitet Regelaktualisierungen auf die in der folgenden Tabelle beschriebene Weise. Audit Manager benachrichtigt Sie nicht, wenn ein Regel-Update erkannt wird.

Szenario	Was Audit Manager macht	Wichtige Informationen
Eine benutzerdefinierte Regel wird in Ihrer Instanz von aktualisiert AWS Config.	Audit Manager berichtet weiterhin anhand der aktualisierten Regeldefinition über Ergebnisse für diese Regel.	Keine Aktion erforderlich.
Eine benutzerdefinierte Regel wird in Ihrer Instanz von gelöscht AWS Config.	Audit Manager meldet keine Ergebnisse mehr für die gelöschte Regel.	Keine Aktion erforderlich. Wenn Sie möchten, können Sie die benutzerdefinierten Kontrollen bearbeiten, die die gelöschte Regel als Datenquellenzuordnung verwendet haben. Anschließend können Sie die gelöschte Regel entfernen, um die Datenquelleneinstellungen Ihrer Kontrolle zu bereinigen. Andernfalls bleibt der Name der gelöschten Regel als unbenutzte Datenquellenzuordnung erhalten.

Für Regelaktualisierungen außerhalb Ihrer AWS Umgebung

In der AWS Umgebung des Empfängers erkennt Audit Manager das Regelupdate nicht. Das liegt daran, dass Absender und Empfänger jeweils in unterschiedlichen AWS Umgebungen arbeiten. Die folgende Tabelle enthält empfohlene Aktionen für dieses Szenario.

Ihre Rolle	Szenario	Empfohlene Aktion
Absend	• Sie haben ein Framework geteilt, das benutzerdefinierte Regeln als Datenquellenzuordnung verwendet.	Wenden Sie sich an den Empfänger, um ihn über das Update zu informieren. Auf diese Weise können sie dasselbe Update durchführen und mit der

Ihre Rolle	Szenario	Empfohlene Aktion
	• Nachdem Sie das Framework freigegeb en haben, haben Sie eine dieser Regeln in AWS Config aktualisiert oder gelöscht.	neuesten Regeldefinition synchron bleiben.
Empfär	• Sie haben ein gemeinsames Framework akzeptiert, das benutzerdefinierte Regeln als Datenquellenzuordnung verwendet. • Nachdem Sie die benutzerdefinierten Regeln in Ihrer Instanz von neu erstellt haben AWS Config, hat der Absender eine dieser Regeln aktualisiert oder gelöscht.	Führen Sie die entsprechende Regelaktualisierung in Ihrer eigenen Instance von AWS Config durch.

Fehlerbehebung bei Benachrichtigungsproblemen

Sie können die Informationen auf dieser Seite verwenden, um häufig auftretende Benachrichtigungsprobleme in Audit Manager zu lösen.

Themen

Ich habe in Audit Manager ein Amazon SNS-Thema angegeben, erhalte aber keine Benachrichtigungen

Wenn Ihr Amazon SNS SNS-Thema AWS KMS serverseitige Verschlüsselung (SSE) verwendet, fehlen Ihnen möglicherweise die erforderlichen Berechtigungen für Ihre AWS KMS Schlüsselrichtlinie. Möglicherweise erhalten Sie auch keine Benachrichtigungen, wenn Sie für Ihr Thema keinen Endpunkt abonniert haben.

Wenn Sie keine Benachrichtigungen erhalten, stellen Sie sicher, dass Sie folgende Schritte ausgeführt haben:

- Sie haben die erforderliche Berechtigungsrichtlinie an Ihren KMS-Schlüssel angehängt. Ein Beispiel für eine Richtlinie, die Sie verwenden können, finden Sie unter. Beispiel 2 (Berechtigungen für den KMS-Schlüssel, der mit dem SNS-Thema verknüpft ist)
- Sie haben einen Endpunkt für das Thema abonniert, über das die Benachrichtigungen gesendet werden. Wenn Sie einen E-Mail-Endpunkt für ein Thema abonnieren, erhalten Sie eine E-Mail, in der Sie aufgefordert werden, Ihr Abonnement zu bestätigen. Sie müssen Ihr Abonnement bestätigen, um E-Mail-Benachrichtigungen empfangen zu können. Weitere Informationen finden Sie unter Erste Schritte im Amazon SNS-Entwicklerhandbuch.

Ich habe ein FIFO-Thema angegeben, erhalte aber keine Benachrichtigungen in der erwarteten Reihenfolge

Audit Manager unterstützt das Senden von Benachrichtigungen an FIFO-SNS-Themen. Die Reihenfolge, in der Audit Manager Benachrichtigungen zu Ihren FIFO-Themen sendet, ist jedoch nicht garantiert.

Behebung von Berechtigungs- und Zugriffsproblemen

Sie können die Informationen auf dieser Seite verwenden, um häufig auftretende Berechtigungsprobleme in Audit Manager zu lösen.

Themen

Ich habe das Audit Manager-Einrichtungsverfahren befolgt, habe aber nicht genügend IAM-Rechte

Der Benutzer, die Rolle oder die Gruppe, die Sie für den Zugriff auf Audit Manager verwenden, muss über die erforderlichen Berechtigungen verfügen. Darüber hinaus sollte Ihre identitätsbasierte Richtlinie nicht zu restriktiv sein. Andernfalls funktioniert die Konsole nicht wie vorgesehen. Dieses Handbuch enthält ein Beispiel für eine Richtlinie, die Sie verwenden könnenErlauben Sie die Mindestberechtigungen, die zur Aktivierung von Audit Manager erforderlich sind. Je nach Anwendungsfall benötigen Sie möglicherweise umfassendere, weniger restriktive Berechtigungen. Wir empfehlen beispielsweise, dass Audit-Verantwortliche Administratorrechte haben. Auf diese Weise können sie die Audit Manager-Einstellungen ändern und Ressourcen wie Bewertungen, Frameworks, Kontrollen und Bewertungsberichte verwalten. Andere Benutzer, z. B. Delegierte, benötigen möglicherweise nur einen Verwaltungszugriff oder Lesezugriff.

Stellen Sie sicher, dass Sie die entsprechenden Berechtigungen für Ihren Benutzer, Ihre Rolle oder Ihre Gruppe hinzufügen. Für Prüfungsverantwortliche lautet die empfohlene Richtlinie AWSAuditManagerAdministratorAccess. Für Delegierte können Sie die Beispielrichtlinie für den Verwaltungszugriff verwenden, die auf der Seite mit den Beispielen für IAM-Richtlinien bereitgestellt wird. Sie können diese Beispielrichtlinien als Ausgangspunkt verwenden und nach Bedarf Änderungen vornehmen, um Ihren Anforderungen zu entsprechen.

Wir empfehlen Ihnen, sich Zeit zu nehmen, um Ihre Berechtigungen an Ihre spezifischen Anforderungen anzupassen. Wenn Sie Hilfe zu IAM-Berechtigungen benötigen, wenden Sie sich an Ihren Administrator oder AWS -Support.

Ich habe jemanden als Audit-Verantwortlichen angegeben, aber dieser hat immer noch keinen vollen Zugriff auf die Bewertung. Warum ist das so?

Die Angabe einer Person als Audit-Verantwortlicher allein gewährt dieser Person keinen vollen Zugriff auf eine Bewertung. Audit-Verantwortliche müssen außerdem über die erforderlichen IAM-Berechtigungen für den Zugriff auf und die Verwaltung von Audit Manager-Ressourcen verfügen. Mit anderen Worten, Sie müssen nicht nur einen Benutzer als Audit-Verantwortliche angeben, sondern diesem Benutzer auch die erforderlichen IAM-Richtlinien zuteilen. Die Idee dahinter ist, dass Audit Manager durch beides sicherstellt, dass Sie die volle Kontrolle über alle Einzelheiten jeder Bewertung haben.

> **Note**
>
> Für Prüfungsverantwortliche empfehlen wir, die AWSAuditManagerAdministratorAccessRichtlinie zu verwenden. Weitere Informationen finden Sie unter Empfohlene Richtlinien für Benutzerrollen in AWS Audit Manager.

Ich kann eine Aktion in Audit Manager nicht ausführen

Wenn Sie nicht über die erforderlichen Berechtigungen verfügen, um die AWS Audit Manager Konsolen- oder Audit Manager Manager-API-Operationen zu verwenden, wird wahrscheinlich ein `AccessDeniedException` Fehler auftreten.

Um dieses Problem zu lösen, müssen Sie Ihren Administrator um Hilfe bitten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Audit Manager Manager-Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen 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 dazu, ob Audit Manager diese Funktionen unterstützt, finden Sie unter Wie AWS Audit Manager funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen in AWS-Konten Ihrem Besitz gewähren können, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , dem Sie gehören.
- 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.

Ich erhalte die Fehlermeldung „Zugriff verweigert“, obwohl ich über die erforderlichen Audit Manager Manager-Berechtigungen verfüge

Wenn Ihr Konto Teil einer Organisation ist, ist es möglich, dass der `Access Denied` Fehler durch eine Service Control Policy (SCP) verursacht wird. SCPs sind Richtlinien, die zur Verwaltung von Berechtigungen für eine Organisation verwendet werden. Wenn ein SCP eingerichtet ist, kann es allen Mitgliedskonten, einschließlich des delegierten Administratorkontos, das Sie in Audit Manager verwenden, bestimmte Berechtigungen verweigern.

Wenn Ihre Organisation beispielsweise über einen SCP verfügt, der Berechtigungen für AWS Control Catalog verweigert APIs, können Sie die von Control Catalog bereitgestellten Ressourcen nicht einsehen. Dies gilt auch dann, wenn Sie anderweitig über die erforderlichen Berechtigungen für Audit Manager verfügen, z. B. die AWSAuditManagerAdministratorAccessRichtlinie. Der SCP setzt die verwalteten Richtlinienberechtigungen außer Kraft, indem er den Zugriff auf den Kontrollkatalog ausdrücklich verweigert. APIs

Hier ist ein Beispiel für ein solches SCP. Wenn dieser SCP eingerichtet ist, wird Ihrem delegierten Administratorkonto der Zugriff auf die allgemeinen Kontrollen, Kontrollziele und Kontrolldomänen verweigert, die für die Verwendung der allgemeinen Kontrollfunktion in Audit Manager erforderlich sind.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "controlcatalog:ListCommonControls",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListDomains"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Um dieses Problem zu beheben, empfehlen wir Ihnen, die folgenden Schritte durchzuführen:

1. Bestätigen Sie, ob Ihrer Organisation ein SCP zugeordnet ist. Anweisungen finden Sie im AWS Organizations User Guide unter Informationen zu den Richtlinien Ihrer Organisation abrufen.
2. Stellen Sie fest, ob der SCP den `Access Denied` Fehler verursacht.
3. Aktualisieren Sie den SCP, um sicherzustellen, dass Ihr delegiertes Administratorkonto über den erforderlichen Zugriff für Audit Manager verfügt. Anweisungen finden Sie unter Aktualisieren eines SCP im AWS Organizations User Guide.

Weitere Ressourcen

Die folgenden Seiten enthalten Anleitungen zur Behebung anderer Probleme, die durch fehlende Berechtigungen verursacht werden können:

- Ich kann in meiner Bewertung keine Kontrollen oder Kontrollsätze sehen
- Die Option für benutzerdefinierte Regeln ist nicht verfügbar, wenn ich eine Kontrolldatenquelle konfiguriere
- Ich erhalte die Fehlermeldung Zugriff verweigert, wenn ich versuche, einen Bericht zu erstellen
- Ich erhalte die Fehlermeldung Zugriff verweigert, wenn ich versuche, mit meinem delegierten Administratorkonto einen Bewertungsbericht zu erstellen
- Ich kann die Beweiserhebung nicht aktivieren
- Ich kann die Beweiserhebung nicht deaktivieren
- Meine Suchanfrage schlägt fehl
- Ich habe in Audit Manager ein Amazon SNS-Thema angegeben, erhalte aber keine Benachrichtigungen

Ressourcen taggen AWS Audit Manager

Ein Tag ist ein Metadaten-Label, das Sie einer Ressource zuweisen oder das einer AWS Ressource AWS zugewiesen wird. Jedes Tag besteht aus einem Schlüssel und einem Wert. Für Tags, die Sie zuweisen, definieren Sie einen Schlüssel und einen Wert. So können Sie beispielsweise den Schlüssel als `stage` und den Wert für eine Ressource als `test` definieren.

Tags sind für folgende Aktivitäten nützlich:

- Einfaches Auffinden Ihrer Audit Manager-Ressourcen. Sie können Tags als Suchkriterien verwenden, wenn Sie die Framework-Bibliothek und die Steuerungsbibliothek durchsuchen.
- Zuordnen Ihrer Ressource zu einem Compliance-Typ. Sie können mehrere Ressourcen mit einem Compliance-spezifischen Tag kennzeichnen, um diese Ressourcen einem bestimmten Framework zuzuordnen.
- Identifizieren und organisieren Sie Ihre AWS Ressourcen. Viele AWS-Services unterstützen Tagging, sodass Sie Ressourcen aus verschiedenen Diensten dasselbe Tag zuweisen können, um anzuzeigen, dass die Ressourcen miteinander verknüpft sind.
- Verfolgen Sie Ihre AWS Kosten. Sie aktivieren diese Tags auf dem AWS Fakturierung und Kostenmanagement Dashboard. AWS verwendet die Tags, um Ihre Kosten zu kategorisieren und Ihnen einen monatlichen Kostenverteilungsbericht zu senden. Weitere Informationen finden Sie unter Use cost allocation tags (Verwendung von Kostenzuordnungs-Tags) im AWS Fakturierung und Kostenmanagement -Benutzerhandbuch.

In den folgenden Abschnitten finden Sie weitere Informationen zu Tags für AWS Audit Manager.

Inhalt

In Audit Manager unterstützte Ressourcen

Die folgenden Ressourcen in Audit Manager unterstützen das Tagging:

- Bewertungen

- Steuerungen
- Frameworks

Tag-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags auf Audit Manager-Ressourcen:

- Die maximale Anzahl der Tags, die Sie einer Ressource zuweisen können beträgt 50.
- Maximale Schlüssellänge: 128 Unicode-Zeichen
- Maximale Wertlänge: 256 Unicode-Zeichen
- Gültige Zeichen für Schlüssel und Werte: – A-Z, 0-9, Leerzeichen sowie die folgenden Zeichen _ . : / = + - ind @
- Schlüssel und Werte unterscheiden zwischen Groß- und Kleinschreibung.
- Verwenden Sie es nicht `aws:` als Präfix für Schlüssel; es ist für die AWS Verwendung reserviert

Weitere Ressourcen

Sie können Tags als Eigenschaften festlegen, wenn Sie eine Bewertung, ein Framework oder ein Kontrollelement erstellen. Sie können Tags über die Audit Manager-Konsole, die AWS Command Line Interface (AWS CLI) und die Audit Manager-API hinzufügen, bearbeiten und löschen. Weitere Informationen finden Sie unter den folgenden Links:

- Um Bewertungen mit Tags zu versehen:
  - Erstellen Sie eine Bewertung in AWS Audit Manager und Eine Bewertung bearbeiten in AWS Audit Manager im Abschnitt Assessments dieses Handbuchs
  - Registerkarte „Tags“auf der Seite Bewertung überprüfen in diesem Leitfaden
  - CreateAssessmentund UpdateAssessmentin der AWS Audit Manager API-Referenz
  - TagResourceund UntagResourcein der AWS Audit Manager API-Referenz
- Zum Taggen von Frameworks:
  - Erstellen Sie ein benutzerdefiniertes Framework in AWS Audit Manager und Bearbeiten eines benutzerdefinierten Frameworks in AWS Audit Manager im Abschnitt Framework-Bibliothek dieses Handbuchs
  - Die Tags tab Seite mit den Framework-Details anzeigen in diesem Handbuch

  - CreateAssessmentFrameworkund UpdateAssessmentFrameworkin der AWS Audit Manager API-Referenz
  - TagResourceund UntagResourcein der AWS Audit Manager API-Referenz
- Zum Markieren von Steuerelementen:
  - Erstellen eines benutzerdefinierten Steuerelements in AWS Audit Manager und Bearbeiten eines benutzerdefinierten Steuerelements in AWS Audit Manager im Abschnitt Kontrollen-Bibliothek dieses Handbuchs
  - Der Tags Abschnitt auf der Seite „Ein benutzerdefiniertes Steuerelement überprüfen“ in diesem Handbuch
  - Der Tags Abschnitt auf der Seite Ein Standardsteuerelement überprüfen in diesem Handbuch
  - CreateControlund UpdateControlin der AWS Audit Manager API-Referenz
  - TagResourceund UntagResourcein der AWS Audit Manager API-Referenz

Grundlegendes zu Kontingenten und Einschränkungen für AWS Audit Manager

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Grenzwerte bezeichnet wurden AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Die meisten Audit Manager Manager-Kontingente, aber nicht alle, sind unter dem AWS Audit Manager Namespace in der Service Quotas Quotas-Konsole aufgeführt. Informationen zum Anfordern einer Kontingenterhöhung finden Sie unter Verwaltung Ihrer Audit Manager-Kontingente.

Inhalt

Audit Manager-Standardkontingente

Die folgenden AWS Audit Manager Kontingente gelten AWS-Konto pro Region.

Ressource	Kontingent
Bewertungen	Anzahl der aktiven Bewertungen pro Konto: 100
Bewertungsberichte	Anzahl der Beweise, die Sie einem Bewertungsbericht hinzufügen können: • Für Berichte aus derselben Region (bei denen sich die Bewertung und der Ziel-S3-Bucket des Bewertungsberichts im selben AWS-Region befinden): 22.000 • Für regionsübergreifende Berichte (bei denen sich die Bewertung und der Ziel-S3-Bereich in Hinblick auf den AWS-Regionen unterscheiden): 3.500

Ressource	Kontingent
	• Für Berichte, bei denen für die zugehörige Bewertung ein vom Kunden verwalteter Kunde verwendet wird AWS KMS key: 3.500
Kontrollen	Anzahl von benutzerdefinierten Kontrollen pro Konto: 500
Beweise	Maximale Größe einer Datei mit manuellen Beweisen: 100 MB Anzahl der täglichen Uploads manueller Beweise pro Kontrolle: 100 **Tip** Wenn Sie eine große Menge manueller Beweise auf eine einzelne Kontrolle hochladen müssen, empfehlen wir Ihnen, Ihre Beweise stapelweise über mehrere Tage hochzuladen.
Frameworks	Anzahl von benutzerdefinierten Frameworks pro Konto: 100 **Note** Framework-Kontingente gelten für alle gemeinsam genutzten benutzerdefinierten Frameworks in Ihrer Framework-Bibliothek, unabhängig davon, wer das Framework erstellt hat.
Empfänger gemeinsam genutzter benutzerdefinierter Frameworks	Anzahl der aktiven Empfängerkonten: 100
API-Zugriff	Gesamtzahl der Transaktionen pro Sekunde (TPS) APIs: 20 TPS

Verwaltung Ihrer Audit Manager-Kontingente

AWS Audit Manager ist in Service Quotas integriert, AWS-Service sodass Sie Ihre Kontingente von einem zentralen Ort aus einsehen und verwalten können. Mit Service Quotas können Sie den Wert Ihrer Audit Manager-Kontingente einfach ermitteln.

So zeigen Sie Audit Manager-Service Quotas mit der Konsole an

1. Öffnen Sie die Service Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/.
2. Wählen Sie im Navigationsbereich AWS-Services aus.
3. Suchen Sie in der AWS-Services-Liste und wählen Sie AWS Audit Manager aus.
4. In der Liste der Servicekontingente finden Sie den Namen des Servicekontingents, den angewendeten Kontingentwert (falls verfügbar), den AWS Standardkontingentwert und ob das Kontingent anpassbar ist.
5. Wählen Sie den Kontingentnamen, um zusätzliche Informationen zu einem Service Quota anzuzeigen, z. B. seine Beschreibung.
6. (Optional) Um eine Kontingenterhöhung zu beantragen, wählen Sie das Kontingent, das Sie erhöhen möchten, und dann Request quota increase (Kontingenterhöhung beantragen) aus, geben Sie die erforderlichen Informationen ein, und wählen Sie dann Request (Beantragen) aus.

Weitere Ressourcen

Weitere Informationen zur Verwaltung Ihrer Kontingente finden Sie unter Beantragung einer Kontingenterhöhung im Servicekontingents-Benutzerhandbuch.

Weitere Informationen zu Servicekontingenten finden Sie unter Was sind Servicekontingente im Benutzerhandbuch für Servicekontingente.

Codebeispiele für Audit Manager mit AWS SDKs

Die folgenden Codebeispiele zeigen, wie Audit Manager mit einem AWS Software Development Kit (SDK) verwendet wird.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie bestimmte Aufgaben ausführen, indem Sie mehrere Funktionen innerhalb eines Service aufrufen oder mit anderen AWS-Services kombinieren.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS Audit Manager mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele

- Szenarien für die Verwendung von Audit Manager AWS SDKs
  - Erstellen Sie mithilfe eines SDK ein benutzerdefiniertes Audit Manager Manager-Framework aus einem AWS ConfigAWS Conformance Pack
  - Erstellen Sie mithilfe eines SDK ein benutzerdefiniertes Audit Manager Manager-Framework, das Security Hub CSPM-Steuerelemente enthält AWS
  - Erstellen Sie mithilfe eines AWS SDK einen Audit Manager Manager-Bewertungsbericht, der Beweise für einen Tag enthält

Szenarien für die Verwendung von Audit Manager AWS SDKs

Die folgenden Codebeispiele zeigen Ihnen, wie Sie allgemeine Szenarien in Audit Manager mit implementieren AWS SDKs. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben durch den Aufruf mehrerer Funktionen innerhalb von Audit Manager oder in Kombination mit anderen AWS-Services ausführen können. Jedes Szenario enthält einen Link zum vollständigen Quell-Code, wo Sie Anleitungen zum Einrichten und Ausführen des Codes finden.

Szenarien zielen auf eine mittlere Erfahrungsebene ab, um Ihnen zu helfen, Service-Aktionen im Kontext zu verstehen.

Beispiele

- Erstellen Sie mithilfe eines SDK ein benutzerdefiniertes Audit Manager Manager-Framework aus einem AWS ConfigAWS Conformance Pack

- Erstellen Sie mithilfe eines SDK ein benutzerdefiniertes Audit Manager Manager-Framework, das Security Hub CSPM-Steuerelemente enthält AWS
- Erstellen Sie mithilfe eines AWS SDK einen Audit Manager Manager-Bewertungsbericht, der Beweise für einen Tag enthält

Erstellen Sie mithilfe eines SDK ein benutzerdefiniertes Audit Manager Manager-Framework aus einem AWS ConfigAWS Conformance Pack

Wie das aussehen kann, sehen Sie am nachfolgenden Beispielcode:

- Holen Sie sich eine Liste der AWS Config Konformitätspakete.
- Erstellen eines benutzerdefinierten Audit-Manager-Steuerelements für jede verwaltete Regel in einem Konformitätspaket
- Erstellen eines benutzerdefinierten Audit-Manager-Frameworks, das die Steuerelemente enthält

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


class ConformancePack:
    def __init__(self, config_client, auditmanager_client):
        self.config_client = config_client
        self.auditmanager_client = auditmanager_client

    def get_conformance_pack(self):
```

```
        """
        Return a selected conformance pack from the list of conformance packs.

        :return: selected conformance pack
        """
        try:
            conformance_packs = self.config_client.describe_conformance_packs()
            print(
                "Number of conformance packs fetched: ",
                len(conformance_packs.get("ConformancePackDetails")),
            )
            print("Fetched the following conformance packs: ")
            all_cpack_names = {
                cp["ConformancePackName"]
                for cp in conformance_packs.get("ConformancePackDetails")
            }
            for pack in all_cpack_names:
                print(f"\t{pack}")
            cpack_name = input(
                "Provide ConformancePackName that you want to create a custom "
                "framework for: "
            )
            if cpack_name not in all_cpack_names:
                print(f"{cpack_name} is not in the list of conformance packs!")
                print(
                    "Provide a conformance pack name from the available list of "
                    "conformance packs."
                )
                raise Exception("Invalid conformance pack")
            print("-" * 88)
        except ClientError:
            logger.exception("Couldn't select conformance pack.")
            raise
        else:
            return cpack_name

    def create_custom_controls(self, cpack_name):
        """
        Create custom controls for all managed AWS Config rules in a conformance
pack.

        :param cpack_name: The name of the conformance pack to create controls
for.
        :return: The list of custom control IDs.
```

```
        """
        try:
            rules_in_pack =
self.config_client.describe_conformance_pack_compliance(
                ConformancePackName=cpack_name
            )
            print(
                "Number of rules in the conformance pack: ",
                len(rules_in_pack.get("ConformancePackRuleComplianceList")),
            )
            for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
                print(f"\t{rule.get('ConfigRuleName')}")
            print("-" * 88)
            print(
                "Creating a custom control for each rule and a custom framework "
                "consisting of these rules in Audit Manager."
            )
            am_controls = []
            for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
                config_rule = self.config_client.describe_config_rules(
                    ConfigRuleNames=[rule.get("ConfigRuleName")]
                )
                source_id = (
                    config_rule.get("ConfigRules")[0]
                    .get("Source", {})
                    .get("SourceIdentifier")
                )
                custom_control = self.auditmanager_client.create_control(
                    name="Config-" + rule.get("ConfigRuleName"),
                    controlMappingSources=[
                        {
                            "sourceName": "ConfigRule",
                            "sourceSetUpOption": "System_Controls_Mapping",
                            "sourceType": "AWS_Config",
                            "sourceKeyword": {
                                "keywordInputType": "SELECT_FROM_LIST",
                                "keywordValue": source_id,
                            },
                        }
                    ],
                ).get("control", {})
                am_controls.append({"id": custom_control.get("id")})
            print("Successfully created a control for each config rule.")
            print("-" * 88)
```

```
        except ClientError:
            logger.exception("Failed to create custom controls.")
            raise
        else:
            return am_controls

    def create_custom_framework(self, cpack_name, am_control_ids):
        """
        Create a custom Audit Manager framework from a selected AWS Config
 conformance
        pack.

        :param cpack_name: The name of the conformance pack to create a framework
 from.
        :param am_control_ids: The IDs of the custom controls created from the
                               conformance pack.
        """
        try:
            print("Creating custom framework...")
            custom_framework =
 self.auditmanager_client.create_assessment_framework(
                name="Config-Conformance-pack-" + cpack_name,
                controlSets=[{"name": cpack_name, "controls": am_control_ids}],
            )
            print(
                f"Successfully created the custom framework: ",
                f"{custom_framework.get('framework').get('name')}: ",
                f"{custom_framework.get('framework').get('id')}",
            )
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom framework.")
            raise


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager custom framework demo!")
    print("-" * 88)
    print(
        "You can use this sample to select a conformance pack from AWS Config and
 "
        "use AWS Audit Manager to create a custom control for all the managed "
        "rules under the conformance pack. A custom framework is also created "
```

```
            "with these controls."
        )
        print("-" * 88)
        conf_pack = ConformancePack(boto3.client("config"),
    boto3.client("auditmanager"))
        cpack_name = conf_pack.get_conformance_pack()
        am_controls = conf_pack.create_custom_controls(cpack_name)
        conf_pack.create_custom_framework(cpack_name, am_controls)


if __name__ == "__main__":
    run_demo()
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - CreateAssessmentFramework
  - CreateControl

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS Audit Manager mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen Sie mithilfe eines SDK ein benutzerdefiniertes Audit Manager Manager-Framework, das Security Hub CSPM-Steuerelemente enthält AWS

Wie das aussehen kann, sehen Sie am nachfolgenden Beispielcode:

- Rufen Sie eine Liste aller Standardsteuerelemente ab, deren Datenquelle Security Hub CSPM ist.
- Erstellen eines benutzerdefinierten Audit-Manager-Frameworks, das die Steuerelemente enthält

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


class SecurityHub:
    def __init__(self, auditmanager_client):
        self.auditmanager_client = auditmanager_client

    def get_sechub_controls(self):
        """
        Gets the list of controls that use Security Hub as their data source.

        :return: The list of Security Hub controls.
        """
        print("-" * 88)
        next_token = None
        page = 1
        sechub_control_list = []
        while True:
            print("Page [" + str(page) + "]")
            if next_token is None:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", maxResults=100
                )
            else:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", nextToken=next_token, maxResults=100
                )
```

```
            print("Total controls found:",
 len(control_list.get("controlMetadataList")))
            for control in control_list.get("controlMetadataList"):
                control_details = self.auditmanager_client.get_control(
                    controlId=control.get("id")
                ).get("control", {})
                if "AWS Security Hub" in control_details.get("controlSources"):
                    sechub_control_list.append({"id": control_details.get("id")})
            next_token = control_list.get("nextToken")
            if not next_token:
                break
            page += 1
        print("Number of Security Hub controls found: ",
 len(sechub_control_list))
        return sechub_control_list

    def create_custom_framework(self, am_controls):
        """
        Create a custom framework with a list of controls.

        :param am_controls: The list of controls to include in the framework.
        """
        try:
            print("Creating custom framework...")
            custom_framework =
 self.auditmanager_client.create_assessment_framework(
                name="All Security Hub Controls Framework",
                controlSets=[{"name": "Security-Hub", "controls": am_controls}],
            )
            print(
                f"Successfully created the custom framework: "
                f"{custom_framework.get('framework').get('name')}: "
                f"{custom_framework.get('framework').get('id')}"
            )
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom framework.")
            raise


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager Security Hub demo!")
    print("-" * 88)
```

```
    print(" This script creates a custom framework with all Security Hub
 controls.")
    print("-" * 88)
    sechub = SecurityHub(boto3.client("auditmanager"))
    am_controls = sechub.get_sechub_controls()
    sechub.create_custom_framework(am_controls)


if __name__ == "__main__":
    run_demo()
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - CreateAssessmentFramework
  - GetControl
  - ListControls

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS Audit Manager mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen Sie mithilfe eines AWS SDK einen Audit Manager Manager-Bewertungsbericht, der Beweise für einen Tag enthält

Das folgende Codebeispiel zeigt, wie Sie einen Audit-Manager-Bewertungsbericht mit eintägigen Nachweisen erstellen.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import dateutil.parser
```

```
import logging
import time
import urllib.request
import uuid
import boto3
from botocore.exceptions import ClientError


logger = logging.getLogger(__name__)


class AuditReport:
    def __init__(self, auditmanager_client):
        self.auditmanager_client = auditmanager_client

    def get_input(self):
        print("-" * 40)
        try:
            assessment_id = input("Provide assessment id [uuid]: ").lower()
            try:
                assessment_uuid = uuid.UUID(assessment_id)
            except ValueError:
                logger.error("Assessment Id is not a valid UUID: %s",
 assessment_id)
                raise
            evidence_folder = input("Provide evidence date [yyyy-mm-dd]: ")
            try:
                evidence_date = dateutil.parser.parse(evidence_folder).date()
            except ValueError:
                logger.error("Invalid date : %s", evidence_folder)
                raise
            try:
                self.auditmanager_client.get_assessment(
                    assessmentId=str(assessment_uuid)
                )
            except ClientError:
                logger.exception("Couldn't get assessment %s.", assessment_uuid)
                raise
        except (ValueError, ClientError):
            return None, None
        else:
            return assessment_uuid, evidence_date

    def clear_staging(self, assessment_uuid, evidence_date):
```

```
        """
        Find all the evidence in the report and clear it.
        """
        next_token = None
        page = 1
        interested_folder_id_list = []
        while True:
            print(f"Page [{page}]")
            if next_token is None:
                folder_list = (
                    self.auditmanager_client.get_evidence_folders_by_assessment(
                        assessmentId=str(assessment_uuid), maxResults=1000
                    )
                )
            else:
                folder_list = (
                    self.auditmanager_client.get_evidence_folders_by_assessment(
                        assessmentId=str(assessment_uuid),
                        nextToken=next_token,
                        maxResults=1000,
                    )
                )
            folders = folder_list.get("evidenceFolders")
            print(f"Got {len(folders)} folders.")
            for folder in folders:
                folder_id = folder.get("id")
                if folder.get("name") == str(evidence_date):
                    interested_folder_id_list.append(folder_id)
                if folder.get("assessmentReportSelectionCount") == folder.get(
                    "totalEvidence"
                ):
                    print(
                        f"Removing folder from report selection :
{folder.get('name')} "
                        f"{folder_id} {folder.get('controlId')}"
                    )

self.auditmanager_client.disassociate_assessment_report_evidence_folder(
                        assessmentId=str(assessment_uuid),
evidenceFolderId=folder_id
                    )
                elif folder.get("assessmentReportSelectionCount") > 0:
                    # Get all evidence in the folder and
                    # add selected evidence in the selected_evidence_list.
```

```
                    evidence_list = (
                        self.auditmanager_client.get_evidence_by_evidence_folder(
                            assessmentId=str(assessment_uuid),
                            controlSetId=folder_id,
                            evidenceFolderId=folder_id,
                            maxResults=1000,
                        )
                    )
                    selected_evidence_list = []
                    for evidence in evidence_list.get("evidence"):
                        if evidence.get("assessmentReportSelection") == "Yes":
                            selected_evidence_list.append(evidence.get("id"))
                    print(
                        f"Removing evidence report selection :
{folder.get('name')} "
                        f"{len(selected_evidence_list)}"
                    )

self.auditmanager_client.batch_disassociate_assessment_report_evidence(
                        assessmentId=str(assessment_uuid),
                        evidenceFolderId=folder_id,
                        evidenceIds=selected_evidence_list,
                    )
            next_token = folder_list.get("nextToken")
            if not next_token:
                break
            page += 1
        return interested_folder_id_list

    def add_folder_to_staging(self, assessment_uuid, folder_id_list):
        print(f"Adding folders to report : {folder_id_list}")
        for folder in folder_id_list:
            self.auditmanager_client.associate_assessment_report_evidence_folder(
                assessmentId=str(assessment_uuid), evidenceFolderId=folder
            )

    def get_report(self, assessment_uuid):
        report = self.auditmanager_client.create_assessment_report(
            name="ReportViaScript",
            description="testing",
            assessmentId=str(assessment_uuid),
        )
        if self._is_report_generated(report.get("assessmentReport").get("id")):
            report_url = self.auditmanager_client.get_assessment_report_url(
```

```
                assessmentReportId=report.get("assessmentReport").get("id"),
                assessmentId=str(assessment_uuid),
            )
            print(report_url.get("preSignedUrl"))
            urllib.request.urlretrieve(
                report_url.get("preSignedUrl").get("link"),
                report_url.get("preSignedUrl").get("hyperlinkName"),
            )
            print(
                f"Report saved as
 {report_url.get('preSignedUrl').get('hyperlinkName')}."
            )
        else:
            print("Report generation did not finish in 15 minutes.")
            print(
                "Failed to download report. Go to the console and manually
 download "
                "the report."
            )

    def _is_report_generated(self, assessment_report_id):
        max_wait_time = 0
        while max_wait_time < 900:
            print(f"Checking status of the report {assessment_report_id}")
            report_list =
 self.auditmanager_client.list_assessment_reports(maxResults=1)
            if (
                report_list.get("assessmentReports")[0].get("id")
                == assessment_report_id
                and report_list.get("assessmentReports")[0].get("status") ==
 "COMPLETE"
            ):
                return True
            print("Sleeping for 5 seconds...")
            time.sleep(5)
            max_wait_time += 5


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager samples demo!")
    print("-" * 88)
    print(
```

```
        "This script creates an assessment report for an assessment with all the
 "
        "evidence collected on the provided date."
    )
    print("-" * 88)

    report = AuditReport(boto3.client("auditmanager"))
    assessment_uuid, evidence_date = report.get_input()
    if assessment_uuid is not None and evidence_date is not None:
        folder_id_list = report.clear_staging(assessment_uuid, evidence_date)
        report.add_folder_to_staging(assessment_uuid, folder_id_list)
        report.get_report(assessment_uuid)


if __name__ == "__main__":
    run_demo()
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - AssociateAssessmentReportEvidenceFolder
  - BatchDisassociateAssessmentReportEvidence
  - CreateAssessmentReport
  - DisassociateAssessmentReportEvidenceFolder
  - GetAssessment
  - GetAssessmentReportUrl
  - GetEvidenceByEvidenceFolder
  - GetEvidenceFoldersByAssessment
  - ListAssessmentReports

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS Audit Manager mit einem SDK AWS. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verständnis von Sicherheit und Datenschutz in AWS Audit Manager

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-Services in der AWS Cloud läuft. 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 gelten AWS Audit Manager, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können AWS Audit Manager. Die folgenden Themen veranschaulichen, wie Sie Audit Manager zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie lernen auch, wie Sie andere verwenden können AWS-Services , die Ihnen helfen, Ihre Audit Manager Manager-Ressourcen zu überwachen und zu sichern.

Topics

Datenschutz in AWS Audit Manager

Das AWS Modell der gilt für den Datenschutz in AWS Audit Manager. 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 Audit Manager 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.

Zusätzlich zu der obigen Empfehlung empfehlen wir Audit Manager-Kunden ausdrücklich, bei der Erstellung von Bewertungen, benutzerdefinierten Kontrollen, benutzerdefinierten Frameworks und Delegationskommentaren keine sensiblen Identifizierungsdaten in Freiformfeldern anzugeben.

Löschung von Audit Manager-Daten

Audit Manager-Daten können auf verschiedene Arten gelöscht werden.

Datenlöschung bei Deaktivierung von Audit Manager

Wenn Sie Audit Manager deaktivieren, können Sie entscheiden, ob Sie alle Ihre Audit Manager-Daten löschen möchten. Wenn Sie sich dafür entscheiden, Ihre Daten zu löschen, werden sie innerhalb von sieben (7) Tagen nach Deaktivierung von Audit Manager gelöscht. Nachdem Ihre Daten gelöscht wurden, können Sie sie nicht wiederherstellen.

Automatische Datenlöschung

Einige Audit Manager-Daten werden nach einem bestimmten Zeitraum automatisch gelöscht. Audit Manager speichert Kundendaten wie folgt:

Datentyp	Aufbewahrungszeitraum	Hinweise
Beweise	Daten werden ab dem Zeitpunkt der Erstellung zwei (2) Jahre lang aufbewahrt.	Beinhaltet automatisierte Beweise und manuelle Beweise
Vom Kunden erstellte Ressourcen	Daten werden auf unbestimmte Zeit aufbewahrt	Beinhaltet Bewertungen, Bewertungsberichte, benutzerdefinierte Kontrollen und benutzerdefinierte Frameworks

Manuelles Löschen von Daten

Sie können einzelne Audit Manager-Ressourcen jederzeit löschen. Detaillierte Informationen finden Sie hier:

- Löschen einer Bewertung in AWS Audit Manager
  - Siehe auch: DeleteAssessmentin der AWS Audit Manager API-Referenz
- Löschen eines benutzerdefinierten Frameworks in AWS Audit Manager
  - Siehe auch: DeleteAssessmentFrameworkin der AWS Audit Manager API-Referenz
- Löschen von Anfragen zum Teilen in AWS Audit Manager
  - Siehe auch: DeleteAssessmentFrameworkSharein der AWS Audit Manager API-Referenz
- Löschen eines Bewertungsberichts
  - Siehe auch: DeleteAssessmentReportin der AWS Audit Manager API-Referenz
- Löschen eines benutzerdefinierten Steuerelements in AWS Audit Manager
  - Siehe auch: DeleteControlin der AWS Audit Manager API-Referenz

Informationen zum Löschen anderer Ressourcendaten, die Sie möglicherweise mit Audit Manager erstellt haben, finden Sie im folgenden Abschnitt:

- Löschen Sie einen Ereignisdatenspeicher im AWS CloudTrail -Benutzerhandbuch
- Löschen eines Bucket im Benutzerhandbuch für Amazon Simple Storage Service (Amazon S3).

Verschlüsselung im Ruhezustand

Um Daten im Ruhezustand zu verschlüsseln, verwendet Audit Manager serverseitige Verschlüsselung mit Von AWS verwaltete Schlüssel für alle Datenspeicher und Protokolle.

Ihre Daten werden mit einem vom Kunden verwalteten Schlüssel oder einem AWS-eigener Schlüssel, je nach den von Ihnen ausgewählten Einstellungen, verschlüsselt. Wenn Sie keinen vom Kunden verwalteten Schlüssel bereitstellen, verwendet Audit Manager einen, AWS-eigener Schlüssel um Ihre Inhalte zu verschlüsseln. Alle Dienst-Metadaten in DynamoDB und Amazon S3 in Audit Manager werden mit einem AWS-eigener Schlüssel verschlüsselt.

Audit Manager verschlüsselt Daten wie folgt:

- In Amazon S3 gespeicherte Service-Metadaten werden unter AWS-eigener Schlüssel Verwendung von SSE-KMS verschlüsselt.
- In DynamoDB gespeicherte Dienst-Metadaten werden serverseitig mit KMS und einem AWS-eigener Schlüssel verschlüsselt.

- Ihre in DynamoDB gespeicherten Inhalte werden clientseitig entweder mit einem vom Kunden verwalteten Schlüssel oder einem AWS-eigener Schlüssel verschlüsselt. Der KMS-Schlüssel basiert auf den von Ihnen ausgewählten Einstellungen.
- Ihre in Amazon S3 in Audit Manager gespeicherten Inhalte werden mit SSE-KMS verschlüsselt. Der KMS-Schlüssel basiert auf Ihrer Auswahl und kann entweder ein vom Kunden verwalteter Schlüssel oder ein AWS-eigener Schlüssel sein.
- Die in Ihrem S3-Bucket veröffentlichten Bewertungsberichte sind wie folgt verschlüsselt:
  - Wenn Sie einen vom Kunden verwalteten Schlüssel bereitgestellt haben, werden Ihre Daten mit SSE-KMS verschlüsselt.
  - Wenn Sie das verwendet haben AWS-eigener Schlüssel, werden Ihre Daten mit SSE-S3 verschlüsselt.

Verschlüsselung während der Übertragung

Audit Manager bietet für die Verschlüsselung von Daten während der Übertragung sichere und private Endpunkte. Die sicheren und privaten Endpunkte ermöglichen es AWS , die Integrität von API-Anfragen an Audit Manager zu schützen.

Dienstübergreifender Transit

Standardmäßig wird die gesamte serviceübergreifende Kommunikation durch die Verwendung von Transport Layer Security (TLS)-Verschlüsselung geschützt.

Schlüsselverwaltung

Audit Manager unterstützt AWS-eigene Schlüssel sowohl vom Kunden verwaltete Schlüssel zur Verschlüsselung aller Audit Manager Manager-Ressourcen (Bewertungen, Kontrollen, Frameworks, Nachweise und Bewertungsberichte, die in S3-Buckets in Ihren Konten gespeichert sind).

Es wird empfohlen, einen vom Kunden verwalteten Schlüssel zu verwenden. Auf diese Weise können Sie die Verschlüsselungsschlüssel, die Ihre Daten schützen, anzeigen und verwalten, einschließlich der Anzeige von Protokollen über ihre Verwendung in AWS CloudTrail. Wenn Sie einen kundenverwalteten Schlüssel auswählen, erstellt der Audit Manager eine Genehmigung für den KMS-Schlüssel, damit der KMS-Schlüssel zur Verschlüsselung Ihrer Inhalte verwendet werden kann.

> **Warning**
>
> Nachdem Sie einen KMS-Schlüssel, der zur Verschlüsselung von Audit Manager-Ressourcen verwendet wird, gelöscht oder deaktiviert haben, können Sie die unter diesem KMS-Schlüssel verschlüsselte Ressource nicht mehr entschlüsseln, was bedeutet, dass die Daten nicht mehr wiederherstellbar sind.
> Das Löschen eines KMS-Schlüssels in AWS Key Management Service (AWS KMS) ist destruktiv und potenziell gefährlich. Weitere Informationen zum Löschen von KMS-Schlüsseln finden Sie unter Löschen AWS KMS keys im AWS Key Management Service - Benutzerhandbuch.

Sie können Ihre Verschlüsselungseinstellungen angeben, wenn Sie Audit Manager mithilfe der AWS-Managementkonsole, der Audit Manager Manager-API oder der AWS Command Line Interface (AWS CLI) aktivieren. Detaillierte Anweisungen finden Sie unter Aktiviert AWS Audit Manager.

Sie können Ihre Verschlüsselungseinstellungen jederzeit überprüfen und ändern. Detaillierte Anweisungen finden Sie unter Konfiguration Ihrer Datenverschlüsselungseinstellungen.

Weitere Informationen zur Einrichtung von kundenverwalteten Schlüsseln finden Sie im AWS Key Management Service -Benutzerhandbuch unter Schlüssel erstellen.

Identitäts- und Zugriffsmanagement für AWS Audit Manager

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren steuern, wer für die Nutzung von Audit Manager-Ressourcen authentifiziert (angemeldet) und autorisiert (über Berechtigungen verfügen) werden kann. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Serviceübergreifende Confused-Deputy-Prävention
- Beispiele für ressourcenbasierte Richtlinien AWS Audit Manager
- AWS verwaltete Richtlinien für AWS Audit Manager
- Fehlerbehebung bei AWS Audit Manager Identität und Zugriff
- Verwenden von serviceverknüpften Rollen für AWS Audit Manager

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Funktionen zugreifen können (siehe Fehlerbehebung bei AWS Audit Manager Identität und Zugriff)
- Dienstadministrator – bestimmen Sie den Benutzerzugriff und reichen Sie Berechtigungsanfragen ein (siehe Wie AWS Audit Manager funktioniert mit IAM)
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für AWS Audit Manager)

Authentifizierung mit Identitäten

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

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir

raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Verwenden Sie möglichst temporäre Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für Verbundbenutzerzugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, dienstübergreifenden Zugriff und Anwendungen, die auf Amazon ausgeführt werden. EC2 Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an Identitäten oder Ressourcen anhängen. AWS Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten 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 Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen 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. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

Wie AWS Audit Manager funktioniert mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Audit Manager verwenden, erfahren Sie, welche IAM-Funktionen Sie mit Audit Manager verwenden können.

IAM-Funktionen, die Sie mit verwenden können AWS Audit Manager

IAM-Feature	Audit Manager – Support
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Teilweise
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Audit Manager und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für AWS Audit Manager

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

AWS Audit Manager erstellt eine verwaltete Richtlinie, die `AWSAuditManagerAdministratorAccess` nach Audit Manager Manager-Administratoren benannt ist. Diese Richtlinie gewährt vollen Administratorzugriff in Audit Manager. Administratoren können diese Richtlinie mit jeder bestehenden Rolle bzw. jedem bestehenden Benutzer verknüpfen oder eine neue Rolle anlegen.

Empfohlene Richtlinien für Benutzerrollen in AWS Audit Manager

AWS Audit Manager ermöglicht es Ihnen, die Aufgabentrennung zwischen verschiedenen Benutzern und für verschiedene Audits aufrechtzuerhalten, indem Sie unterschiedliche IAM-Richtlinien verwenden. Die beiden Personas in Audit Manager und ihre empfohlenen Richtlinien werden wie folgt definiert:

Persona	Beschreibung und empfohlene Richtlinie
Audit-Verantwortlicher	• Diese Persona muss über die erforderlichen Berechtigungen verfügen, um Bewertungen in zu verwalten. AWS Audit Manager • Die empfohlene Richtlinie für diese Persona ist die verwaltete Richtlinie mit dem Namen. AWSAuditManagerAdministratorAccess Sie können diese Richtlinie als Ausgangspunkt verwenden und ihre Berechtigungen nach Bedarf einschränken.
Delegierter	• Diese Persona kann im Rahmen einer Bewertung auf die delegierten Kontrollsätze zugreifen. Sie kann den Kontrollstatus aktualisieren, Kommentare hinzufügen, ein Kontrollset zur Überprüfung einreichen und dem Bewertungsbericht Nachweise hinzufügen. • Die empfohlene Richtlinie für diese Persona hat sich nach der Beispielrichtlinie Erlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager zu richten. Sie können diese Richtlinie als Ausgangspunkt verwenden und bei Bedarf Änderungen vornehmen, um sie an Ihre Anforderungen anzupassen.

Beispiele für identitätsbasierte Richtlinien für AWS Audit Manager

Beispiele für identitätsbasierte Audit Manager-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Audit Manager.

Ressourcenbasierte Richtlinien innerhalb AWS Audit Manager

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. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Obwohl Sie ressourcenbasierte Richtlinien AWS Audit Manager nicht über IAM verwalten können, implementiert und verwaltet der Service intern ressourcenbasierte Richtlinien für die folgenden beiden Szenarien:

- Wenn Prüfungsverantwortliche einer Bewertung zugewiesen werden, wird der Bewertung eine ressourcenbasierte Richtlinie beigefügt, wobei der Schulleiter der Prüfungsverantwortliche ist. Weitere Informationen erhalten Sie unter Schritt 3: Geben Sie die Audit-Verantwortlichen an und Schritt 3: Audit-Inhaber bearbeiten.
- Wenn ein Kontrollsatz einer Bewertung delegiert wird, wird dem Kontrollsatz eine ressourcenbasierte Richtlinie beigefügt, wobei der Schulleiter der Delegierte ist. Weitere Informationen finden Sie unter Delegieren eines Kontrollsatzes zur Überprüfung in AWS Audit Manager.

Politische Maßnahmen für AWS Audit Manager

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was 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. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS Audit Manager Aktionen finden Sie unter Von AWS Audit Manager definierte Aktionen in der Service Authorization Reference.

Bei den AWS Audit Manager verwendeten Richtlinienaktionen wird das folgende Präfix vor der Aktion verwendet.

```
auditmanager
```

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

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

Sie können auch Platzhalter (*) verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Get` beginnen, einschließlich der folgenden Aktion:

```
"Action": "auditmanager:Get*"
```

Beispiele für identitätsbasierte Audit Manager-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Audit Manager.

Politische Ressourcen für AWS Audit Manager

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was 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. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS Audit Manager Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von AWS Audit Manager definierte Ressourcen in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Audit Manager definierte Aktionen.

Eine Audit Manager-Bewertung hat das folgende Amazon-Ressourcenname (ARN)-Format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Ein Audit Manager-Kontrollset verfügt über das folgende ARN-Format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Ein Audit Manager-Kontrollelement verfügt über das folgende ARN-Format:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs).

Um beispielsweise die `i-1234567890abcdef0`-Bewertung in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Um alle Instances anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Einige Audit Manager-Aktionen, z. B. zum Erstellen von Ressourcen, können auf bestimmten Ressourcen nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

```
"Resource": "*"
```

Viele Audit Manager-API-Aktionen umfassen mehrere Ressourcen. `ListAssessments`Gibt beispielsweise eine Liste von Bewertungs-Metadaten zurück, auf die die aktuell angemeldeten Benutzer zugreifen können AWS-Konto. Ein Benutzer muss daher über Berechtigungen zum Anzeigen der Bewertungen verfügen. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie ARNs durch Kommas.

```
"Resource": [
      "resource1",
      "resource2"
```

Eine Liste der Audit Manager Manager-Ressourcentypen und ihrer Eigenschaften ARNs finden Sie AWS Audit Manager im IAM-Benutzerhandbuch unter Defined by (Ressourcen definiert von). Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Audit Manager definierte Aktionen.

Einige API-Aktionen von Audit Manager unterstützen mehrere Ressourcen. Zum Beispiel greift `GetChangeLogs` auf ein `assessmentID`, `controlID` und `controlSetId` zu, so dass ein Prinzipal über die Berechtigung zum Zugriff auf jede dieser Ressourcen verfügen muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie ARNs durch Kommas.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Schlüssel zur Richtlinienbedingung für AWS Audit Manager

Unterstützt dienstspezifische Richtlinien-Bedingungsschlüssel: Teilweise

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

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

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

Wenn der Prinzipal in einer Richtlinien-Anweisung ein AWS -Service-Prinzipal ist, empfehlen wir dringend, die `aws:SourceArn`- oder globalen `aws:SourceAccount`-Bedingungsschlüssel in der Richtlinie zu verwenden. Sie können diese globalen Bedingungskontextschlüssel verwenden, um das Szenario eines verwirrten Stellvertreters zu verhindern. Die folgenden dokumentierten Richtlinien zeigen, wie Sie die `aws:SourceArn`- und globalen `aws:SourceAccount`-Bedingungskontextschlüssel in Audit Manager verwenden können, um das Problem des verwirrten Stellvertreters zu vermeiden.

- Beispielrichtlinie für ein SNS-Thema, das für Audit Manager-Benachrichtigungen verwendet wird
- Beispielrichtlinie für einen KMS-Schlüssel, der mit einem SNS-Thema verwendet wird

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

Audit Manager stellt keine servicespezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Zugriffskontrolllisten (ACLs) in AWS Audit Manager

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.

Attributbasierte Zugriffskontrolle (ABAC) mit AWS Audit Manager

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

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.

Weitere Informationen zum Markieren von AWS Audit Manager Ressourcen finden Sie unter. Ressourcen taggen AWS Audit Manager

Verwenden temporärer Anmeldeinformationen mit AWS Audit Manager

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Zugriffssitzungen weiterleiten für AWS Audit Manager

Unterstützt Forward Access Sessions (FAS): Ja

Forward-Access-Sitzungen (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Audit Manager

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 Rollen zum Delegieren von Berechtigungen an einen AWS-Service erstellen im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die AWS Audit Manager - Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Audit Manager dazu Anleitungen gibt.

Mit Diensten verknüpfte Rollen für AWS Audit Manager

Unterstützt serviceverknüpfte Rollen: Ja

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. 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 zu dienstbezogenen Rollen für finden Sie AWS Audit Manager unter. Verwenden von serviceverknüpften Rollen für AWS Audit Manager

Beispiele für identitätsbasierte Richtlinien für AWS Audit Manager

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, Audit Manager-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

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 AWS Audit Manager definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen,

Ressourcen und Bedingungsschlüssel für AWS Audit Manager in der Service Authorization Reference.

Inhalt

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Audit Manager-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads 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 Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen 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. 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 Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Erlauben Sie die Mindestberechtigungen, die zur Aktivierung von Audit Manager erforderlich sind

In diesem Beispiel wird gezeigt, wie Sie Konten ohne Administratorrolle zur Aktivierung von AWS Audit Manager zulassen können.

> **Note**
>
> Was wir hier anbieten, ist eine Basisrichtlinie, die die Mindestberechtigungen gewährt, die zur Aktivierung von Audit Manager erforderlich sind. Dabei sind alle in der folgenden Richtlinie genannten Berechtigungen erforderlich. Wenn Sie einen Teil dieser Richtlinie weglassen, können Sie Audit Manager nicht aktivieren.
> Wir empfehlen Ihnen, sich Zeit zu nehmen, um Ihre Berechtigungen so anzupassen, dass sie Ihren spezifischen Anforderungen entsprechen. Wenden Sie sich an Ihren Administrator oder den AWS Support, falls Sie weitere Unterstützung benötigen.

Verwenden Sie die folgenden Berechtigungen, um den Mindestzugriff zu gewähren, der für die Aktivierung von Audit Manager erforderlich ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

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

Benutzern den vollständigen Administratorzugriff auf AWS Audit Manager erlauben

Die folgenden Beispielrichtlinien gewähren vollen Administratorzugriff auf AWS Audit Manager.

- Beispiel 1 (Verwaltete Richtlinie, `AWSAuditManagerAdministratorAccess`)
- Beispiel 2 (Zielberechtigungen für den Bewertungsbericht)
- Beispiel 3 (Berechtigungen zur Aktivierung von Evidence Finder)

- Beispiel 4 (Berechtigungen zur Deaktivierung von Evidence Finder)

Beispiel 1 (Verwaltete Richtlinie, **`AWSAuditManagerAdministratorAccess`**)

Die AWSAuditManagerAdministratorAccessRichtlinie umfasst die Möglichkeit, Audit Manager zu aktivieren und zu deaktivieren, die Audit Manager Manager-Einstellungen zu ändern und alle Audit Manager Manager-Ressourcen wie Bewertungen, Frameworks, Kontrollen und Bewertungsberichte zu verwalten.

Beispiel 2 (Zielberechtigungen für den Bewertungsbericht)

Diese Richtlinie gewährt Ihnen die Erlaubnis, auf einen bestimmten S3-Bucket zuzugreifen und diesem Dateien hinzuzufügen bzw. daraus zu löschen. Auf diese Weise können Sie den angegebenen Bucket als Ziel für Bewertungsberichte in Audit Manager verwenden.

Ersetzen Sie *`placeholder text`* durch Ihre Informationen. Geben Sie den S3-Bucket an, den Sie als Ziel für Ihre Bewertungsberichte verwenden, und den KMS-Schlüssel, den Sie zur Verschlüsselung Ihrer Bewertungsberichte verwenden.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::example-s3-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }
  ]
}
```

Beispiel 3 (Berechtigungen zur Aktivierung von Evidence Finder)

Die folgende Berechtigungsrichtlinie ist erforderlich, wenn Sie die Beweissuch-Funktion aktivieren und verwenden möchten. Diese Richtlinienerklärung ermöglicht es Audit Manager, einen CloudTrail Lake-Ereignisdatenspeicher zu erstellen und Suchabfragen auszuführen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
                "cloudtrail:CreateEventDataStore"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Beispiel 4 (Berechtigungen zur Deaktivierung von Evidence Finder)

Diese Beispielrichtlinie gewährt die Erlaubnis, die Beweissuch-Funktion in Audit Manager zu deaktivieren. Dazu müssen Sie den Ereignisdatenspeicher löschen, der erstellt wurde, als Sie das Feature zum ersten Mal aktiviert haben.

Bevor Sie diese Richtlinie verwenden, ersetzen Sie sie durch Ihre eigenen Informationen. *placeholder text* Sie sollten die UUID des Ereignisdatenspeichers angeben, der erstellt wurde, als Sie die Beweissuche aktiviert haben. Sie können den ARN des Ereignisdatenspeichers über Ihre Audit Manager-Einstellungen abrufen. Weitere Informationen finden Sie unter GetSettings in der AWS Audit Manager -API-Referenz.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EventDataStoreId"
        }
    ]
}
```

Erlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager

In diesem Beispiel wird gezeigt, wie Sie Verwaltungszugriff auf AWS Audit Manager gewähren können.

Diese Richtlinie gewährt die Möglichkeit, alle Audit Manager-Ressourcen (Bewertungen, Frameworks und Kontrollen) zu verwalten, aber nicht die Möglichkeit, Audit Manager zu aktivieren oder zu deaktivieren oder Audit Manager-Einstellungen zu ändern.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:CreateAssessment",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:CreateControl",
                "auditmanager:DeleteControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:DeleteAssessmentFrameworkShare",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAccountStatus",
                "auditmanager:GetAssessment",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:GetControl",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:GetAssessmentReportUrl",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetDelegations",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:GetEvidenceFileUploadUrl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:GetInsights",
                "auditmanager:GetInsightsByAssessment",
                "auditmanager:GetOrganizationAdminAccount",
```

```
                "auditmanager:ListAssessments",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListControls",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:ListNotifications",
                "auditmanager:ListAssessmentControlInsightsByControlDomain",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:ListAssessmentFrameworkShareRequests",
                "auditmanager:ListControlDomainInsights",
                "auditmanager:ListControlDomainInsightsByAssessment",
                "auditmanager:ListControlInsightsByControlDomain",
                "auditmanager:ListTagsForResource",
                "auditmanager:StartAssessmentFrameworkShare",
                "auditmanager:TagResource",
                "auditmanager:UntagResource",
                "auditmanager:UpdateControl",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:UpdateAssessmentFrameworkShare",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:ValidateAssessmentReportIntegrity"
            ],
            "Resource": "*"
        },
        {
    "Sid": "ControlCatalogAccess",
    "Effect": "Allow",
    "Action": [
"controlcatalog:ListCommonControls",
"controlcatalog:ListDomains",
"controlcatalog:ListObjectives"
    ],
    "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
```

```
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Erlauben Sie Benutzern nur Lesezugriff auf AWS Audit Manager

Diese Richtlinie gewährt nur Lesezugriff auf AWS Audit Manager Ressourcen wie Bewertungen, Frameworks und Kontrollen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API oder. AWS CLI 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": "*"
        }
    ]
}
```

Senden AWS Audit Manager von Benachrichtigungen an Amazon SNS SNS-Themen zulassen

Die Richtlinien in diesem Beispiel gewähren Audit Manager die Berechtigung, Benachrichtigungen an ein bestehendes Amazon SNS-Thema zu senden.

- Beispiel 1 — Wenn Sie Benachrichtigungen von Audit Manager erhalten möchten, verwenden Sie dieses Beispiel, um Ihrer SNS-Themenzugriffsrichtlinie Berechtigungen hinzuzufügen.

- Beispiel 2 — Wenn Ihr SNS-Thema AWS Key Management Service (AWS KMS) für serverseitige Verschlüsselung (SSE) verwendet, verwenden Sie dieses Beispiel, um der KMS-Schlüsselzugriffsrichtlinie Berechtigungen hinzuzufügen.

In den folgenden Richtlinien ist der Prinzipal, der die Berechtigungen erhält, der Prinzipal des Audit Manager-Dienstes, der `auditmanager.amazonaws.com` ist. Wenn der Prinzipal in einer Richtlinien-Anweisung ein AWS -Service-Prinzipal ist, empfehlen wir dringend, die `aws:SourceArn`- oder globalen `aws:SourceAccount`-Bedingungsschlüssel in der Richtlinie zu verwenden. Sie können diese globalen Bedingungskontextschlüssel verwenden, um das Szenario eines verwirrten Stellvertreters zu verhindern.

Beispiel 1 (Berechtigungen für das SNS-Thema)

Diese Richtlinienanweisung erlaubt es Audit Manager, Ereignisse in dem angegebenen SNS-Thema zu veröffentlichen. Jede Anfrage zur Veröffentlichung in dem angegebenen SNS-Thema muss die Bedingungen der Richtlinie erfüllen.

Bevor Sie diese Richtlinie verwenden, ersetzen Sie sie *`placeholder text`* durch Ihre eigenen Informationen. Beachten Sie die folgenden Punkte:

- Wenn Sie den `aws:SourceArn`-Bedingungsschlüssel in dieser Richtlinie verwenden, muss der Wert dem ARN der Audit Manager-Ressource entsprechen, von der die Benachrichtigung stammt. Im folgenden Beispiel verwendet `aws:SourceArn` einen Platzhalter (`*`) für die Ressourcen-ID. Dies erlaubt alle Anfragen, die von Audit Manager kommen, für alle Audit Manager-Ressourcen. Mit dem globalen `aws:SourceArn`-Bedingungsschlüssel können Sie entweder `StringLike` oder den `ArnLike`-Bedingungsoperator verwenden. Als bewährte Methode empfehlen wir die Verwendung von `ArnLike`.
- Wenn Sie den `aws:SourceAccount`Bedingungsschlüssel verwenden, können Sie entweder den `StringEquals` oder den `StringLike`-Bedingungsoperator verwenden. Als bewährte Methode empfehlen wir Ihnen, `StringEquals` zu verwenden, um die geringste Berechtigung zu erteilen.
- Wenn Sie sowohl `aws:SourceAccount` als auch `aws:SourceArn` verwenden, müssen sie dieselbe Konto-ID haben.

JSON

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

```
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-1:111122223333:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:us-east-1:111122223333:*"
        }
      }
    }
}
```

Im folgenden alternativen Beispiel wird nur der `aws:SourceArn`-Bedingungsschlüssel zusammen mit dem `StringLike`-Bedingungsoperator verwendet:

```
    "Condition": {
      "StringLike": {
        "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
      }
    }
```

Im folgenden alternativen Beispiel wird nur der `aws:SourceAccount`-Bedingungsschlüssel zusammen mit dem `StringLike`-Bedingungsoperator verwendet:

```
  "Condition": {
    "StringLike": {
      "aws:SourceAccount": "accountID"
    }
  }
```

Beispiel 2 (Berechtigungen für den KMS-Schlüssel, der mit dem SNS-Thema verknüpft ist)

Diese Richtlinienanweisung ermöglicht es Audit Manager, den KMS-Schlüssel zum Generieren des Datenschlüssels zu verwenden, den es zum Verschlüsseln eines SNS-Themas verwendet.

Jede Anforderung, den KMS-Schlüssel für die angegebene Produktion zu verwenden, muss die Richtlinienbedingungen erfüllen.

Bevor Sie diese Richtlinie verwenden, ersetzen Sie sie durch Ihre eigenen Informationen. *placeholder text* Beachten Sie die folgenden Punkte:

- Wenn Sie den `aws:SourceArn`-Bedingungsschlüssel in dieser Richtlinie verwenden, muss der Wert dem ARN der Ressource entsprechen, die verschlüsselt wird. In diesem Fall ist es beispielsweise das SNS-Thema in Ihrem Konto. Legen Sie den Wert auf den ARN oder ein ARN-Muster mit Platzhalterzeichen (*) fest. Sie können entweder den `StringLike` oder den `ArnLike`-Bedingungsoperator mit dem `aws:SourceArn`-Bedingungsschlüssel verwenden. Als bewährte Methode empfehlen wir die Verwendung von `ArnLike`.
- Wenn Sie den `aws:SourceAccount`Bedingungsschlüssel verwenden, können Sie entweder den `StringEquals` oder den `StringLike`-Bedingungsoperator verwenden. Als bewährte Methode empfehlen wir Ihnen, `StringEquals` zu verwenden, um die geringste Berechtigung zu erteilen. Wenn Sie den ARN des SNS-Themas nicht kennen, können Sie `aws:SourceAccount` verwenden.
- Wenn Sie sowohl `aws:SourceAccount` als auch `aws:SourceArn` verwenden, müssen sie dieselbe Konto-ID haben.

JSON

```
{
     "Version":"2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:us-east-1:123456789012:key/*",
       "Condition": {
           "StringEquals": {
                "aws:SourceAccount": "123456789012"
            },
```

```
            "ArnLike": {
                "aws:SourceArn": "arn:aws:sns:us-east-1:123456789012:topicName"
            }
        }
    }
}
```

Im folgenden alternativen Beispiel wird nur der `aws:SourceArn`-Bedingungsschlüssel zusammen mit dem `StringLike`-Bedingungsoperator verwendet:

```
    "Condition": {
      "StringLike": {
        "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
      }
    }
```

Im folgenden alternativen Beispiel wird nur der `aws:SourceAccount`-Bedingungsschlüssel zusammen mit dem `StringLike`-Bedingungsoperator verwendet:

```
  "Condition": {
    "StringLike": {
      "aws:SourceAccount": "accountID"
    }
  }
```

Erlauben Sie Benutzern, Suchanfragen in der Beweissuche durchzuführen

Die folgende Richtlinie gewährt Berechtigungen zum Durchführen von Abfragen in einem CloudTrail Lake-Ereignisdatenspeicher. Diese Berechtigungsrichtlinie ist erforderlich, wenn Sie die Beweissuch-Funktion verwenden möchten.

JSON

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

```
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zu einem Problem mit dem verwirrten Stellvertreter führen. Ein serviceübergreifender Identitätswechsel kann auftreten, wenn ein Service (der Anruf-Service) einen anderen Service anruft (den aufgerufenen Service). Der aufrufende Dienst kann so manipuliert werden, dass er seine Berechtigungen verwendet, um auf die Ressourcen eines anderen Kunden zuzugreifen, obwohl er dazu nicht berechtigt ist. Um dies zu verhindern, bietet Amazon Web Services Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen zu beschränken, die einem anderen Dienst für den Zugriff auf Ihre Ressourcen AWS Audit Manager gewährt werden.

- Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Wenn Sie mehrere Ressourcen angeben möchten, können Sie auch `aws:SourceArn` mit einem Platzhalter (`*`) verwenden.

  Beispielsweise könnten Sie ein Amazon-SNS-Thema verwenden, um Aktivitätsbenachrichtigungen von Audit Manager zu erhalten. In diesem Fall ist der ARN-Wert von `aws:SourceArn` in Ihrer SNS-Zugriffsrichtlinie die Audit Manager-Ressource, von der die Benachrichtigung stammt. Da Sie wahrscheinlich über mehrere Audit Manager-Ressourcen verfügen, empfehlen wir die Verwendung von `aws:SourceArn` mit einem Platzhalter. Auf diese Weise können Sie alle Ihre Audit Manager-Ressourcen in Ihrer SNS-Themenzugriffsrichtlinie angeben.

- Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.
- Wenn der `aws:SourceArn`-Wert nicht die Konto-ID enthält, z. B. den ARN eines Amazon-S3-Buckets, müssen Sie beide globalen Bedingungskontext-Schlüssel verwenden, um Berechtigungen einzuschränken.
- Wenn Sie beide Bedingungen verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert die gleiche Konto-ID aufweisen, wenn sie in der gleichen Richtlinienanweisung verwendet werden.
- Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen Amazon-Ressourcenname (ARN) der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel `aws:SourceArn` mit Platzhalterzeichen (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Audit Manager Confused-Deputy-Support

Audit Manager bietet verwirrte stellvertretende Unterstützung in den folgenden Szenarien. Diese Richtlinienbeispiele zeigen, wie Sie die `aws:SourceArn`- und `aws:SourceAccount`-Bedingungsschlüssel verwenden können, um das Confused-Deputy-Support-Problem zu vermeiden.

- Beispiel-Richtlinie: Das SNS-Thema, das Sie für den Empfang von Audit Manager-Benachrichtigungen verwenden
- Beispielrichtlinie: Der KMS-Schlüssel, mit dem Sie Ihr SNS-Thema verschlüsseln

Audit Manager bietet keinen Confused-Deputy-Support für den kundenverwalteten Schlüssel, den Sie in Ihren Audit Manager Konfiguration Ihrer Datenverschlüsselungseinstellungen-Einstellungen angeben. Wenn Sie Ihren eigenen, vom Kunden verwalteten Schlüssel bereitgestellt haben, können Sie die `aws:SourceAccount`- oder `aws:SourceArn`-Bedingungen in dieser KMS-Schlüsselrichtlinie nicht verwenden.

Beispiele für ressourcenbasierte Richtlinien AWS Audit Manager

Amazon S3 S3-Bucket-Richtlinie

Die folgende Richtlinie ermöglicht CloudTrail die Übermittlung von Ergebnissen der Evidence Finder-Abfrage an den angegebenen S3-Bucket. Als bewährte Sicherheitsmethode `aws:SourceArn` trägt der globale IAM-Bedingungsschlüssel dazu bei, dass nur für den Ereignisdatenspeicher in den S3-Bucket CloudTrail geschrieben wird.

> **Important**
>
> Sie müssen einen S3-Bucket für die Lieferung von CloudTrail Lake-Abfrageergebnissen angeben. Weitere Informationen finden Sie unter Angeben eines vorhandenen Buckets für CloudTrail Lake-Abfrageergebnisse.

Ersetzen Sie die *`placeholder text`* wie folgt durch Ihre eigenen Informationen:

- *`amzn-s3-demo-destination-bucket`*Ersetzen Sie es durch den S3-Bucket, den Sie als Exportziel verwenden.
- *`myQueryRunningRegion`*Ersetzen Sie es durch das AWS-Region für Ihre Konfiguration passende.
- *`myAccountID`*Ersetzen Sie durch die AWS-Konto ID, die für verwendet wird CloudTrail. Dies entspricht möglicherweise nicht der AWS-Konto ID für den S3-Bucket. Wenn es sich um den Ereignisdatenspeicher einer Organisation handelt, müssen Sie die AWS-Konto für das Verwaltungskonto verwenden.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
```

```
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
    }
```

AWS Key Management Service Richtlinie

Wenn in Ihrem S3-Bucket die Standardverschlüsselung auf eingestellt ist`SSE-KMS`, gewähren Sie CloudTrail in der Ressourcenrichtlinie Ihres AWS Key Management Service Schlüssels Zugriff darauf, damit der Schlüssel verwendet werden kann. Fügen Sie in diesem Fall dem AWS KMS Schlüssel die folgende Ressourcenrichtlinie hinzu.

JSON

```
{
```

```
 "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinien für AWS Audit Manager

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das

Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

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

Themen

- AWS verwaltete Richtlinie: AWSAudit ManagerAdministratorAccess
- AWS verwaltete Richtlinie: AWSAudit ManagerServiceRolePolicy
- AWS Audit Manager Aktualisierungen der AWS verwalteten Richtlinien

AWS verwaltete Richtlinie: AWSAudit ManagerAdministratorAccess

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

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Administratorzugriff auf ermöglichen AWS Audit Manager. Dieser Zugriff umfasst die Möglichkeit AWS Audit Manager, alle Audit Manager Manager-Ressourcen wie Bewertungen AWS Audit Manager, Frameworks, Kontrollen und Bewertungsberichte zu aktivieren und zu deaktivieren, Einstellungen zu ändern und zu verwalten.

AWS Audit Manager erfordert umfassende Berechtigungen für mehrere AWS Dienste. Dies liegt daran, dass mehrere AWS Dienste AWS Audit Manager integriert werden können, um automatisch Beweise aus den AWS-Konto einzelnen Diensten im Rahmen einer Bewertung zu sammeln.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `Audit Manager` – erlaubt Prinzipalen vollständige Berechtigungen für AWS Audit Manager - Ressourcen.
- `Organizations` – ermöglicht Prinzipalen, Konten und Organisationseinheiten aufzulisten und einen delegierten Administrator zu registrieren oder abzumelden. Dies ist erforderlich, damit Sie die Unterstützung mehrerer Konten aktivieren und Bewertungen für mehrere Konten durchführen und Nachweise in einem delegierten Administratorkonto konsolidieren können. AWS Audit Manager
- `iam` – ermöglicht Prinzipalen das Abrufen und Auflisten von Benutzern in IAM sowie das Erstellen einer servicebezogenen Rolle. Dies ist erforderlich, damit Sie Prüfungs- und Bewertungsverantwortliche benennen können. Diese Richtlinie erlaubt es Prinzipalen außerdem,

die serviceverbundene Rolle zu löschen und den Löschstatus abzurufen. Dies ist erforderlich, damit AWS Audit Manager Sie Ressourcen bereinigen und die mit dem Dienst verknüpfte Rolle für Sie löschen können, wenn Sie den Dienst in der deaktivieren. AWS-Managementkonsole

- `s3` – ermöglicht Prinzipalen, verfügbare Amazon Simple Storage Service (Amazon S3) -Buckets aufzulisten. Dieses Feature ist erforderlich, damit Sie den S3-Bucket bestimmen können, in dem Sie Beweisberichte speichern oder manuelle Beweise hochladen möchten.
- `kms` – ermöglicht Prinzipalen, Schlüssel aufzulisten und zu beschreiben, Aliase aufzulisten und Freigaben zu erteilen. Dies ist erforderlich, damit Sie vom Kunden verwaltete Schlüssel für die Datenverschlüsselung auswählen können.
- `sns` – ermöglicht Prinzipalen, Abonnementthemen in Amazon SNS aufzulisten. Dies ist erforderlich, damit Sie angeben können, an welches SNS-Thema Sie Benachrichtigungen über AWS Audit Manager senden möchten.
- `events`— Ermöglicht Prinzipalen das Auflisten und Verwalten von Schecks von. AWS Security Hub CSPM Dies ist erforderlich, damit automatisch AWS Security Hub CSPM Ergebnisse für die AWS Dienste gesammelt werden AWS Audit Manager können, die von AWS Security Hub CSPMüberwacht werden. Es kann diese Daten dann in Beweise umwandeln, die in Ihre AWS Audit Manager -Bewertungen aufgenommen werden.
- `tag` – ermöglicht es Prinzipalen, markierte Ressourcen abzurufen. Dies ist erforderlich, damit Sie Tags als Suchfilter verwenden können, wenn Sie Frameworks, Kontrollen und Bewertungen in AWS Audit Manager durchsuchen.
- `controlcatalog`— Ermöglicht es Prinzipalen, die Domänen, Ziele und allgemeinen Kontrollen aufzulisten, die von AWS Control Catalog bereitgestellt werden. Dies ist erforderlich, damit Sie die Funktion für allgemeine Steuerungen in AWS Audit Manager verwenden können. Wenn Sie über diese Berechtigungen verfügen, können Sie eine Liste mit häufig verwendeten Steuerelementen in der AWS Audit Manager Steuerelementbibliothek anzeigen und die Steuerelemente nach Domäne und Ziel filtern. Sie können allgemeine Steuerelemente auch als Beweisquelle verwenden, wenn Sie ein benutzerdefiniertes Steuerelement erstellen.

JSON

AWS verwaltete Richtlinie: AWSAudit ManagerServiceRolePolicy

Sie können `AWSAuditManagerServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft`AWSServiceRoleForAuditManager`, mit der Sie Aktionen AWS Audit Manager in Ihrem Namen ausführen können. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Audit Manager.

Mit der Richtlinie für Rollenberechtigungen `AWSAuditManagerServiceRolePolicy` können Sie AWS Audit Manager automatisierte Beweise sammeln lassen, indem Sie wie folgt vorgehen:

- Sammeln Sie Daten aus den folgenden Datenquellen:
  - Verwaltungsereignisse von AWS CloudTrail
  - Konformitätsprüfungen von AWS-Config-Regeln
  - Konformitätsprüfungen von AWS Security Hub CSPM
- Verwenden Sie API-Aufrufe, um Ihre Ressourcenkonfigurationen für die folgende AWS-Services zu beschreiben.

  > **Tip**
  >
  > Weitere Informationen zu den API-Aufrufen, die Audit Manager verwendet, um Beweise aus diesen Services zu sammeln, finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen in diesem Handbuch.

  - Amazon API Gateway
  - AWS Backup
  - Amazon Bedrock
  - AWS Certificate Manager
  - Amazon CloudFront
  - AWS CloudTrail
  - Amazon CloudWatch
  - CloudWatch Amazon-Protokolle
  - Amazon-Cognito-Benutzerpools
  - AWS Config
  - Amazon Data Firehose

- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (ICH BIN)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming für Apache Kafka
- OpenSearch Amazon-Dienst
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker KI
- AWS Secrets Manager
- AWS Security Hub CSPM
- Amazon Simple Notification Service

- Amazon Simple Queue Service

- AWS WAF

Details zu Berechtigungen

`AWSAuditManagerServiceRolePolicy`ermöglicht AWS Audit Manager es, die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `apigateway:GET`
- `autoscaling:DescribeAutoScalingGroups`
- `backup:ListBackupPlans`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListGuardrails`
- `bedrock:ListModelCustomizationJobs`
- `cloudfront:GetDistribution`
- `cloudfront:GetDistributionConfig`
- `cloudfront:ListDistributions`
- `cloudtrail:DescribeTrails`
- `cloudtrail:GetTrail`
- `cloudtrail:ListTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`

- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables

- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig

- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys

- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration

- `license-manager:ListLicenseConfigurations`
- `license-manager:ListUsageForLicenseConfiguration`
- `logs:DescribeDestinations`
- `logs:DescribeExportTasks`
- `logs:DescribeLogGroups`
- `logs:DescribeMetricFilters`
- `logs:DescribeResourcePolicies`
- `logs:FilterLogEvents`
- `logs:GetDataProtectionPolicy`
- `organizations:DescribeOrganization`
- `organizations:DescribePolicy`
- `rds:DescribeCertificates`
- `rds:DescribeDBClusterEndpoints`
- `rds:DescribeDBClusterParameterGroups`
- `rds:DescribeDBClusters`
- `rds:DescribeDBInstances`
- `rds:DescribeDBInstanceAutomatedBackups`
- `rds:DescribeDBSecurityGroups`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterSnapshots`
- `redshift:DescribeLoggingStatus`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketAcl`
- `s3:GetBucketLogging`
- `s3:GetBucketOwnershipControls`
- `s3:GetBucketPolicy`
  - Diese API-Aktion erfolgt innerhalb des Bereichs, AWS-Konto in dem die verfügbar service-linked-role ist. Sie kann nicht auf kontoübergreifende Bucket-Richtlinien zugreifen.
- `s3:GetBucketPublicAccessBlock`

- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions

- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

JSON

AWS Audit Manager Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS Audit Manager seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS Audit Manager Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die mit dem Dienst verknüpfte Rolle ermöglicht es nun AWS Audit Manager , die `bedrock:ListGuardrails` Aktion auszuführen. Diese API-Aktion ist erforderlich, um die zu unterstützen. AWS Framework für bewährte Methoden für generative KI v2 Es ermöglicht Audit Manager, automatisierte Nachweise über die Leitplanken zu sammeln, die für Ihre Trainingsdatensätze mit generativen KI-Modelldaten vorhanden sind.	24.09.2024
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Wir haben die folgenden Berechtigungen hinzugefügt. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager kann jetzt die folgenden Aktionen ausführen, um automatisierte Beweise über die Ressourcen in Ihrem zu sammeln AWS-Konto. • `sagemaker:DescribeAlgorithm` • `sagemaker:DescribeDomain` • `sagemaker:DescribeEndpoint` • `sagemaker:DescribeFlowDefinition` • `sagemaker:DescribeHumanTaskUi` • `sagemaker:DescribeLabelingJob` • `sagemaker:DescribeModel`	10.06.2024

Änderungen	Beschreibung	Datum
	• sagemaker:DescribeModelBias JobDefinition • sagemaker:DescribeModelCard • sagemaker:DescribeModelQual ityJobDefinition • sagemaker:DescribeTrainingJob • sagemaker:DescribeUserProfile • sagemaker:ListAlgorithms • sagemaker:ListDomains • sagemaker:ListEndpoints • sagemaker:ListFlowDefinitions • sagemaker:ListHumanTaskUis • sagemaker:ListLabelingJobs • sagemaker:ListModels • sagemaker:ListModelBiasJobD efinitions • sagemaker:ListModelCards • sagemaker:ListModelQualityJ obDefinitions • sagemaker:ListMonitoringAlerts • sagemaker:ListMonitoringSch edules • sagemaker:ListTrainingJobs • sagemaker:ListUserProfiles	

Änderungen	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Wir haben die folgenden Berechtigungen hinzugefügt. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager kann jetzt die folgenden Aktionen ausführen, um automatisierte Beweise über die Ressourcen in Ihrem zu sammeln AWS-Konto. • `iam:ListAttachedGroupPolicies` • `iam:ListAttachedUserPolicies` • `iam:ListGroupsForUser` • `es:ListDomainNames` Wir haben dem `APIGatewayAccess` Abschnitt der Richtlinie auch eine neue Ressource hinzugefügt (`arn:aws:apigateway:*::/restapis`). Die Richtlinie gewährt nun die angegebene Berechtigung (in diesem Fall die `apigateway:GET` Aktion) nicht nur für die Stufen und Staging-Ressourcen von API Gateway REST APIs, sondern auch für den REST APIs selbst. Diese Änderung erweitert den Geltungsbereich der Richtlinie effektiv um die Möglichkeit, Informationen über den API-Gateway-REST APIs selbst abzurufen, zusätzlich zu den damit verbundenen Phasen und Phasenressourcen APIs.	17.05.2024

Änderungen	Beschreibung	Datum
AWSAuditManagerAdministratorAccess – Aktualisierung auf eine bestehende Richtlinie	Wir haben die folgenden Berechtigungen zu `AWSAuditManagerAdministratorAccess` hinzugefügt. • `controlcatalog:ListCommonControls` • `controlcatalog:ListDomains` • `controlcatalog:ListObjectives` Mit diesem Update können Sie sich die Kontrolldomänen, Kontrollziele und allgemeinen Kontrollen ansehen, die im AWS Control Catalog bereitgestellt werden. Diese Berechtigungen sind erforderlich, wenn Sie die Funktion für allgemeine Steuerelemente in verwenden möchten AWS Audit Manager.	15.05.2024

Änderungen	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Wir haben die folgenden Berechtigungen hinzugefügt. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager kann jetzt die folgenden Aktionen ausführen, um automatisierte Beweise über die Ressourcen in Ihrem zu sammeln AWS-Konto. • `apigateway:GET` • `autoscaling:DescribeAutoScalingGroups` • `backup:ListBackupPlans` • `cloudfront:GetDistribution` • `cloudfront:GetDistributionConfig` • `cloudfront:ListDistributions` • `cloudtrail:GetTrail` • `cloudtrail:ListTrails` • `dynamodb:DescribeContinuousBackups` • `dynamodb:DescribeBackup` • `dynamodb:DescribeTableReplicaAutoScaling` • `ec2:DescribeInstanceCreditSpecifications` • `ec2:DescribeInstanceAttribute` • `ec2:DescribeSecurityGroupRules` • `ec2:DescribeVpcEndpointConnections` • `ec2:DescribeVpcEndpointServiceConfigurations` • `ec2:GetLaunchTemplateData`	15.05.2024

Änderungen	Beschreibung	Datum
	• es:DescribeDomains • es:DescribeDomain • es:DescribeDomainConfig • iam:GetAccessKeyLastUsed • iam:GetGroupPolicy • iam:GetPolicy • iam:GetPolicyVersion • iam:GetRolePolicy • iam:GetUser • iam:GetUserPolicy • iam:ListAccessKeys • iam:ListAttachedRolePolicies • iam:ListMfaDeviceTags • iam:ListMfaDevices • iam:ListPolicyVersions • logs:GetDataProtectionPolicy • rds:DescribeDBInstanceAutomatedBackups • rds:DescribeDBClusterEndpoints • rds:DescribeDBClusterParameterGroups • redshift:DescribeClusterSnapshots • redshift:DescribeLoggingStatus • s3:GetBucketAcl • s3:GetBucketLogging • s3:GetBucketOwnershipControls • s3:GetBucketTagging • sagemaker:DescribeEndpointConfig	

Änderungen	Beschreibung	Datum
	• `sagemaker:ListEndpointConfigs` • `secretsmanager:DescribeSecret` • `secretsmanager:ListSecrets` • `sns:ListTagsForResource` • `waf-regional:GetRule` • `waf-regional:GetWebAcl` • `waf-regional:ListRules` • `waf:GetRule` • `waf:GetRuleGroup` • `waf:ListRuleGroups` • `waf:ListRules` • `waf:ListWebAcls` • `wafv2:ListWebAcls`	
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die mit dem Dienst verknüpfte Rolle ermöglicht nun AWS Audit Manager die Ausführung der Aktion. `s3:GetBucketPolicy` Diese API-Aktion ist erforderlich, um die zu unterstützen. AWS Framework für bewährte Methoden für generative KI v2 Es ermöglicht Audit Manager, automatisierte Nachweise über die Richtlinieneinschränkungen zu erfassen, die für Ihre Trainingsdatensätze mit generativen KI-Modelldaten gelten. Die `GetBucketPolicy` Aktion erfolgt innerhalb des Bereichs, AWS-Konto in dem die verfügbar service-linked-role ist. Sie kann nicht auf kontoübergreifende Bucket-Richtlinien zugreifen.	12.06.2023

Änderungen	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Wir haben die folgenden Berechtigungen hinzugefügt. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager kann jetzt die folgenden Aktionen ausführen, um automatisierte Beweise über die Ressourcen in Ihrem zu sammeln AWS-Konto. • `acm:GetAccountConfiguration` • `acm:ListCertificates` • `backup:ListRecoveryPointsByResource` • `bedrock:GetCustomModel` • `bedrock:GetFoundationModel` • `bedrock:GetModelCustomizationJob` • `bedrock:GetModelInvocationLoggingConfiguration` • `bedrock:ListCustomModels` • `bedrock:ListFoundationModels` • `bedrock:ListModelCustomizationJobs` • `cloudtrail:LookupEvents` • `cloudwatch:DescribeAlarmsForMetric` • `cloudwatch:GetMetricStatistics` • `cloudwatch:ListMetrics` • `directconnect:DescribeDirectConnectGateways` • `directconnect:DescribeVirtualGateways` • `dynamodb:ListBackups`	11.06.2023

Änderungen	Beschreibung	Datum
	• dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers	

Änderungen	Beschreibung	Datum
	• elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates	

Änderungen	Beschreibung	Datum
	• rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Wir haben die folgenden Berechtigungen zu AWSAuditManagerServiceRolePolicy hinzugefügt. • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07.07.2022

Änderungen	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die mit dem Dienst verknüpfte Rolle ermöglicht es nun AWS Audit Manager , die Aktion auszuführen. `organizations:DescribeOrganization` Außerdem haben wir den Umfang der `CreateEventsAccess` -Ressource von einem Platzhalter (`*`) auf einen bestimmten Ressourcentyp (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`) reduziert. Schließlich haben wir einen `Null`-Bedingungsoperator für den `events:source` -Bedingungsschlüssel hinzugefügt, um zu bestätigen, dass ein Quellwert existiert und sein Wert nicht Null ist.	20.05.2022
AWSAuditManagerAdministratorAccess – Aktualisierung auf eine bestehende Richtlinie	Wir haben die Richtlinie für `events:source` aktualisiert, um zu verdeutlichen, dass es sich um einen Schlüssel mit mehreren Werten handelt.	29.04.2022
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Wir haben die Richtlinie für `events:source` aktualisiert, um zu verdeutlichen, dass es sich um einen Schlüssel mit mehreren Werten handelt.	16.03.2022
AWS Audit Manager hat begonnen, Änderungen zu verfolgen	AWS Audit Manager hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	05/06/2021

Fehlerbehebung bei AWS Audit Manager Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit Audit Manager und IAM auftreten könnten.

Themen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Audit Manager

Der `AccessDeniedException` Fehler tritt auf, wenn ein Benutzer nicht berechtigt ist, die Audit Manager Manager-API-Operationen zu verwenden AWS Audit Manager .

In diesem Fall muss Ihr Administrator die Richtlinie aktualisieren, um Ihnen den Zugriff zu ermöglichen.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Audit Manager übergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte 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 Audit Manager 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 AWS Audit Manager Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen 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 dazu, ob Audit Manager diese Funktionen unterstützt, finden Sie unter Wie AWS Audit Manager funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen in AWS-Konten Ihrem Besitz gewähren können, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , dem Sie gehören.
- 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.

Verwenden von serviceverknüpften Rollen für AWS Audit Manager

AWS Audit Manager verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverbundene Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Audit Manager verknüpft ist. Dienstbezogene Rollen sind von Audit Manager vordefiniert und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Audit Manager erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Audit Manager definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Audit Manager die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-Linked Role (Serviceverknüpfte Rolle) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für AWS Audit Manager

Audit Manager verwendet die angegebene serviceverknüpfte Rolle**`AWSServiceRoleForAuditManager`**, die den Zugriff auf AWS-Services und -Ressourcen ermöglicht, die von AWS Audit Manager verwendet oder verwaltet werden.

Die serviceverknüpfte Rolle `AWSServiceRoleForAuditManager` vertraut dem Service `auditmanager.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Richtlinie für Rollenberechtigungen ermöglicht es Audit Manager `AWSAuditManagerServiceRolePolicy`, automatisierte Nachweise über Ihre AWS Nutzung zu sammeln. Genauer gesagt, kann er die folgenden Aktionen in Ihrem Namen ergreifen.

- Audit Manager kann AWS Security Hub CSPM damit Nachweise für Konformitätsprüfungen sammeln. In diesem Fall verwendet Audit Manager die folgende Berechtigung, um die Ergebnisse von Sicherheitsprüfungen direkt von zu melden AWS Security Hub CSPM. Anschließend fügt er die Ergebnisse als Beweise Ihren jeweiligen Bewertungskontrollen bei.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Weitere Informationen darüber, welche spezifischen Security Hub CSPM-Steuerelemente Audit Manager beschreiben kann, finden Sie unter AWS Security Hub CSPM Kontrollen, die von unterstützt werden. AWS Audit Manager

- Audit Manager kann AWS Config damit Nachweise für Konformitätsprüfungen sammeln. In diesem Fall verwendet Audit Manager die folgenden Berechtigungen, um die Ergebnisse von AWS Config

Regelauswertungen direkt von zu melden AWS Config. Anschließend fügt er die Ergebnisse als Beweise Ihren jeweiligen Bewertungskontrollen bei.

- `config:DescribeConfigRules`
- `config:DescribeDeliveryChannels`
- `config:ListDiscoveredResources`

> **Note**
>
> Weitere Informationen darüber, welche spezifischen AWS Config Regeln Audit Manager beschreiben kann, finden Sie unter AWS Config Regeln, die von unterstützt werden AWS Audit Manager.

- Audit Manager kann verwendet werden AWS CloudTrail , um Nachweise zu Benutzeraktivitäten zu sammeln. In diesem Fall verwendet Audit Manager die folgenden Berechtigungen, um Benutzeraktivitäten aus CloudTrail Protokollen zu erfassen. Anschließend fügt er die Aktivität als Beweis Ihren entsprechenden Bewertungskontrollen bei.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

> **Note**
>
> Weitere Informationen darüber, welche spezifischen CloudTrail Ereignisse Audit Manager beschreiben kann, finden Sie unter AWS CloudTrail Ereignisnamen, die von unterstützt werden AWS Audit Manager.

- Audit Manager kann AWS API-Aufrufe verwenden, um Nachweise zur Ressourcenkonfiguration zu sammeln. In diesem Fall verwendet Audit Manager die folgenden Berechtigungen zum Aufrufen von Read-Only APIs , die Ihre Ressourcenkonfigurationen für Folgendes beschreiben. AWS-Services Anschließend fügt er die API-Antworten als Beweis Ihren jeweiligen Bewertungskontrollen bei.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `apigateway:GET`
  - `autoscaling:DescribeAutoScalingGroups`
  - `backup:ListBackupPlans`

- backup:ListRecoveryPointsByResource
- bedrock:GetCustomModel
- bedrock:GetFoundationModel
- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListGuardrails
- bedrock:ListModelCustomizationJobs
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling

- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId

- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams

- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders

- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances

- `rds:DescribeDBInstanceAutomatedBackups`
- `rds:DescribeDBSecurityGroups`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterSnapshots`
- `redshift:DescribeLoggingStatus`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketAcl`
- `s3:GetBucketLogging`
- `s3:GetBucketOwnershipControls`
- `s3:GetBucketPolicy`
  - Diese API-Aktion wird innerhalb des Bereichs ausgeführt, in AWS-Konto dem die verfügbar service-linked-role ist. Sie kann nicht auf kontoübergreifende Bucket-Richtlinien zugreifen.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketTagging`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `sagemaker:DescribeAlgorithm`
- `sagemaker:DescribeDomain`
- `sagemaker:DescribeEndpoint`
- `sagemaker:DescribeEndpointConfig`
- `sagemaker:DescribeFlowDefinition`
- `sagemaker:DescribeHumanTaskUi`
- `sagemaker:DescribeLabelingJob`
- `sagemaker:DescribeModel`
- `sagemaker:DescribeModelBiasJobDefinition`
- `sagemaker:DescribeModelCard`
- `sagemaker:DescribeModelQualityJobDefinition`
- `sagemaker:DescribeTrainingJob`

- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule

- `waf:GetRuleGroup`
- `waf:ListActivatedRulesInRuleGroup`
- `waf:ListRuleGroups`
- `waf:ListRules`
- `waf:ListWebAcls`
- `wafv2:ListWebAcls`

> **Note**
>
> Weitere Informationen zu den spezifischen API-Aufrufen, die Audit Manager beschreiben kann, finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen.

Die vollständigen Informationen zu den Berechtigungen der serviceverknüpften Rolle `AWSServiceRoleForAuditManager` finden Sie AWSAuditManagerServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

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

Die AWS Audit Manager dienstverknüpfte Rolle erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie sie aktivieren AWS Audit Manager, erstellt der Dienst automatisch die dienstverknüpfte Rolle für Sie. Sie können Audit Manager auf der Onboarding-Seite von oder über die API oder AWS CLI aktivieren. AWS-Managementkonsole Weitere Informationen finden Sie unter Aktiviert AWS Audit Manager in diesem Benutzerhandbuch.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen.

Bearbeitung der mit dem Dienst verknüpften AWS Audit Manager Rolle

AWS Audit Manager erlaubt es Ihnen nicht, die mit dem `AWSServiceRoleForAuditManager` Dienst verknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet

werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Erlauben Sie einer IAM-Entität, die Beschreibung der serviceverknüpften **`AWSServiceRoleForAuditManager`**-Rolle zu bearbeiten

Fügen Sie die folgende Anweisung der Berechtigungsrichtlinie für die IAM-Entität hinzu, die die Beschreibung einer serviceverknüpften Rolle bearbeiten soll.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Löschen der mit dem Dienst verknüpften AWS Audit Manager Rolle

Wenn Sie Audit Manager nicht mehr verwenden, empfehlen wir, die serviceverknüpfte `AWSServiceRoleForAuditManager`-Rolle zu löschen. Auf diese Weise ist keine ungenutzte Entität vorhanden, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie löschen können.

Bereinigen der serviceverknüpften Rolle

Bevor Sie mit IAM eine serviceverknüpfte Audit Manager-Rolle löschen können, müssen Sie sich zunächst vergewissern, dass die Rolle über keine aktiven Sitzungen verfügt, und alle Ressourcen entfernen, die von der Rolle verwendet werden. Stellen Sie dazu sicher, dass Audit Manager insgesamt abgemeldet ist. AWS-Regionen Nach der Abmeldung verwendet Audit Manager die serviceverknüpfte Rolle nicht mehr.

Anweisungen zum Aufrufen von Audit Manager finden Sie in den folgenden Ressourcen:

- Deaktivierung AWS Audit Manager in dieser Anleitung
- DeregisterAccount in der AWS Audit Manager -API-Referenz
- deregister-account in der Referenz für AWS CLI AWS Audit Manager

Anweisungen zum manuellen Löschen von Audit Manager-Ressourcen finden Sie unter Löschen von Audit Manager-Daten in diesem Handbuch.

Löschen der serviceverknüpften -Rolle

Sie können die serviceverknüpfte Rolle unter Verwendung der IAM-Konsole, der AWS Command Line Interface (AWS CLI) oder der API-IAM löschen.

IAM console

Führen Sie diese Schritte aus, um die serviceverknüpfte Rolle über die IAM-Konsole zu löschen.

So löschen Sie eine serviceverknüpfte Rolle (Konsole)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Wählen Sie im Navigationsbereich der IAM Console Roles (Rollen) aus. Aktivieren Sie dann das Kontrollkästchen (nicht den Namen oder die Zeile) neben `AWSServiceRoleForAuditManager`.
3. Wählen Sie für Role actions (Rollenaktionen) oben auf der Seite Delete role (Rolle löschen).
4. Überprüfen Sie im Bestätigungsdialogfeld die Informationen zum letzten Zugriff; diese zeigen an, wann jede der ausgewählten Rollen zuletzt auf einen AWS-Service-Service zugegriffen hat. Auf diese Weise können Sie leichter bestätigen, ob die Rolle derzeit aktiv ist. Wenn Sie fortfahren möchten, geben Sie **`AWSServiceRoleForAuditManager`** in das Texteingabefeld ein und wählen Sie Delete (Löschen), um die serviceverknüpfte Rolle zur Löschung zu übermitteln.
5. Sehen Sie sich die Benachrichtigungen in der IAM-Konsole an, um den Fortschritt der Löschung der serviceverknüpften Rolle zu überwachen. Da die Löschung der serviceverknüpften IAM-Rolle asynchron erfolgt, kann die Löschung nach dem Übermitteln der Rolle für die Löschung erfolgreich sein oder fehlschlagen. Wenn der Vorgang erfolgreich ist, wird die Rolle aus der Liste entfernt und eine Erfolgsmeldung oben auf der Seite angezeigt.

AWS CLI

Sie können IAM-Befehle von verwenden, um eine AWS CLI dienstverknüpfte Rolle zu löschen.

So löschen Sie eine serviceverknüpfte Rolle (AWS CLI)

1. Geben Sie den folgenden Befehl ein, um die Rolle in Ihrem Konto aufzulisten:

   ```
   aws iam get-role --role-name AWSServiceRoleForAuditManager
   ```

2. Da eine serviceverknüpfte Rolle nicht gelöscht werden kann, wenn sie verwendet wird oder ihr Ressourcen zugeordnet sind, müssen Sie eine Löschungsanforderung übermitteln. Diese Anforderung kann verweigert werden, wenn diese Bedingungen nicht erfüllt sind. Sie benötigen die `deletion-task-id` aus der Antwort, um den Status der Löschaufgabe zu überprüfen.

   Geben Sie den folgenden Befehl ein, um eine Löschanforderung für eine serviceverknüpfte Rolle zu übermitteln:

   ```
   aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
   ```

3. Verwenden Sie den folgenden Befehl, um den Status der Löschaufgabe zu überprüfen:

   ```
   aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
   ```

   Der Status der Löschaufgabe kann `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` oder `FAILED` lauten. Wenn die Löschung fehlschlägt, gibt der Aufruf den Grund zurück, sodass Sie das Problem beheben können.

IAM API

Sie können die IAM-API zum Löschen einer serviceverknüpften Rolle verwenden.

So löschen Sie eine serviceverknüpfte Rolle (API)

1. Rufen Sie an GetRole, um die Rolle in Ihrem Konto aufzulisten. Geben Sie in der Anforderung `AWSServiceRoleForAuditManager` als den `RoleName` an.
2. Da eine serviceverknüpfte Rolle nicht gelöscht werden kann, wenn sie verwendet wird oder ihr Ressourcen zugeordnet sind, müssen Sie eine Löschungsanforderung übermitteln. Diese Anforderung kann verweigert werden, wenn diese Bedingungen nicht erfüllt sind. Sie benötigen die `DeletionTaskId` aus der Antwort, um den Status der Löschaufgabe zu überprüfen.

Rufen DeleteServiceLinkedRoleSie an, um einen Löschantrag für eine dienstbezogene Rolle einzureichen. Geben Sie in der Anforderung `AWSServiceRoleForAuditManager` als den `RoleName` an.

3. Um den Status der Löschung zu überprüfen, rufen Sie GetServiceLinkedRoleDeletionStatus auf. Geben Sie in der Anforderung die `DeletionTaskId` an.

   Der Status der Löschaufgabe kann `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` oder `FAILED` lauten. Wenn die Löschung fehlschlägt, gibt der Aufruf den Grund zurück, sodass Sie das Problem beheben können.

Tipps zum Löschen der serviceverknüpften Audit Manager Manager-Rolle

Der Löschvorgang für die serviceverknüpfte Audit Manager-Rolle schlägt möglicherweise fehl, wenn Audit Manager die Rolle verwendet oder über zugeordnete Ressourcen verfügt. Dies kann in den folgenden Szenarien passieren:

1. Ihr Konto ist immer noch in einem oder mehreren Fällen bei Audit Manager registriert AWS-Regionen.
2. Ihr Konto ist Teil einer AWS Organisation, und das Verwaltungskonto oder das delegierte Administratorkonto ist weiterhin in Audit Manager integriert.

Um ein Problem mit einem fehlgeschlagenen Löschen zu lösen, überprüfen Sie zunächst, ob Sie Teil einer Organisation AWS-Konto sind. Sie können dies tun, indem Sie den DescribeOrganizationAPI-Vorgang aufrufen oder zur AWS Organizations Konsole navigieren.

Wenn Sie AWS-Konto Teil einer Organisation sind

1. Verwenden Sie Ihr Verwaltungskonto, um Ihren delegierten Administrator in Audit Manager aus allen Bereichen zu entfernen, in AWS-Regionen denen Sie einen hinzugefügt haben.
2. Verwenden Sie Ihr Verwaltungskonto, um Audit Manager überall dort abzumelden, AWS-Regionen wo Sie den Service genutzt haben.
3. Versuchen Sie erneut, die mit dem Dienst verknüpfte Rolle zu löschen, indem Sie die Schritte des vorherigen Verfahrens befolgen.

Wenn Sie AWS-Konto nicht Teil einer Organisation sind

1. Stellen Sie sicher, dass Sie Audit Manager überall dort abgemeldet haben, AWS-Regionen wo Sie den Service genutzt haben.
2. Versuchen Sie erneut, die mit dem Dienst verknüpfte Rolle zu löschen, indem Sie die Schritte des vorherigen Verfahrens befolgen.

Nachdem Sie sich bei Audit Manager abgemeldet haben, verwendet der Dienst die dienstverknüpfte Rolle nicht mehr. Sie können die Rolle dann erfolgreich löschen.

Unterstützte Regionen für AWS Audit Manager serviceverknüpfte Rollen

AWS Audit Manager unterstützt die Verwendung von dienstbezogenen Rollen überall dort, AWS-Regionen wo der Dienst verfügbar ist. Weitere Informationen finden Sie unter AWS -Service-Endpunkte.

Überprüfung der Einhaltung der Vorschriften für AWS Audit Manager

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

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Verständnis von Resilienz in AWS Audit Manager

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind.

Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

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

Sicherheit der Infrastruktur in AWS Audit Manager

Als verwalteter Service ist AWS Audit Manager durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsservices 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 AWS Audit Manager 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.

Sie können diese API-Operationen von jedem Netzwerkstandort aus aufrufen, AWS Audit Manager unterstützt jedoch ressourcenbasierte Zugriffsrichtlinien, die Einschränkungen auf der Grundlage der Quell-IP-Adresse beinhalten können. Sie können Audit Manager Manager-Richtlinien auch verwenden, um den Zugriff von bestimmten Amazon Virtual Private Cloud (Amazon VPC) - Endpunkten oder bestimmten zu kontrollieren. VPCs Dadurch wird der Netzwerkzugriff auf eine bestimmte Audit Manager Manager-Ressource effektiv nur von der spezifischen VPC innerhalb des AWS Netzwerks isoliert.

AWS Audit Manager und Schnittstellen-VPC-Endpunkte ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC und AWS Audit Manager durch die Erstellung eines Schnittstellen-VPC-Endpunkts herstellen. Schnittstellenendpunkte werden mit einer

Technologie betrieben AWS PrivateLink, mit der Sie privat auf Audit Manager zugreifen können, APIs ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect-Verbindung zu benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Audit Manager APIs zu kommunizieren. Datenverkehr zwischen Ihrer VPC und AWS Audit Manager verlässt das AWS Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon-VPC-Benutzerhandbuch.

Überlegungen zu AWS Audit Manager VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für einrichten, stellen Sie sicher AWS Audit Manager, dass Sie die Eigenschaften und Einschränkungen der Schnittstellen-Endpunkte im Amazon VPC-Benutzerhandbuch lesen.

AWS Audit Manager unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus.

Erstellen eines Schnittstellen-VPC-Endpunkts für AWS Audit Manager

Sie können einen VPC-Endpunkt für den AWS Audit Manager Service entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für die AWS Audit Manager Verwendung des folgenden Dienstnamens:

- `com.amazonaws.region.auditmanager`

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an die AWS Audit Manager Verwendung des Standard-DNS-Namens für die Region stellen, `auditmanager.us-east-1.amazonaws.com` z. B.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für AWS Audit Manager

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf AWS Audit Manager steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Aktionen AWS Audit Manager

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für AWS Audit Manager. Wenn diese Richtlinie an einen Endpunkt angefügt wird, gewährt sie Zugriff auf die aufgelisteten Audit Manager-Aktionen für alle Prinzipale auf allen Ressourcen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessment",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Anmeldung und Überwachung AWS Audit Manager

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Audit Manager und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um Audit Manager zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Konto -Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail - Benutzerhandbuch.
- Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software-as-a-Service (SaaS-) Anwendungen und AWS Diensten und leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können Sie Ereignisse überwachen, die in Services auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Überwachung AWS Audit Manager mit Amazon EventBridge

Amazon EventBridge hilft Ihnen dabei, Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu automatisieren AWS-Services und automatisch darauf zu reagieren.

Sie können EventBridge Regeln verwenden, um Audit Manager Manager-Ereignisse zu erkennen und darauf zu reagieren. Ruft auf der Grundlage der von Ihnen erstellten EventBridge Regeln eine oder mehrere Zielaktionen auf, wenn ein Ereignis den Werten entspricht, die Sie in einer Regel angeben. Abhängig vom Ereignistyp können Sie Benachrichtigungen versenden, Ereignisinformationen erfassen, Korrekturmaßnahmen ausführen, Ereignisse auslösen oder andere Aktionen ausführen.

Beispielsweise können Sie feststellen, wann die folgenden Audit Manager-Ereignisse in Ihrem Konto auftreten:

- Ein Prüfungsverantwortlicher erstellt, aktualisiert oder löscht eine Bewertung
- Ein Prüfungsverantwortlicher delegiert einen Kontrollsatz zur Überprüfung
- Ein Bevollmächtigter schließt seine Prüfung ab und reicht den überprüften Kontrollsatz an den Prüfungsverantwortlichen zurück
- Ein Prüfungsverantwortlicher aktualisiert den Status einer Prüfungskontrolle

Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Verwende eine AWS Lambda Funktion, um eine Benachrichtigung an einen Slack-Channel weiterzuleiten.
- Übertragen Sie Daten von Prüfungen an einen Amazon Kinesis Data Stream, um eine umfassende Echtzeit-Statusüberwachung zu unterstützen.
- Senden Sie ein Thema von Amazon Simple Notification Service (Amazon SNS) an Ihre E-Mail.
- Lassen Sie sich mit einer CloudWatch Amazon-Alarmaktion benachrichtigen.

> **Note**
>
> Audit Manager liefert Ereignisse auf dauerhafter Basis. Das bedeutet, dass Audit Manager erfolgreich versucht, Ereignisse EventBridge mindestens einmal zuzustellen. In Fällen, in denen Ereignisse aufgrund einer EventBridge Serviceunterbrechung nicht zugestellt werden können, werden sie später von Audit Manager für bis zu 24 Stunden erneut versucht.

EventBridge Beispielformat für Audit Manager

Der folgende JSON-Code zeigt ein Beispiel für ein Ereignis zur Erstellung einer Bewertung in Audit Manager. Informationen zu den Feldern in diesem Ereignis finden Sie unter Referenz zur Ereignisstruktur.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
```

```
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Voraussetzungen für die Erstellung einer EventBridge Regel

Bevor Sie Regeln für Audit Manager-Ereignisse erstellen, empfehlen wir Ihnen Folgendes:

- Machen Sie sich mit Ereignissen, Regeln und Zielen in vertraut EventBridge. Weitere Informationen finden Sie unter Was ist Amazon EventBridge? im EventBridge Amazon-Benutzerhandbuch.
- Erstellen Sie ein zu nutzendes Ziel für die Ereignisregeln. Sie können zum Beispiel ein Amazon-SNS-Thema erstellen, damit Sie bei der Prüfung des Kontrollsatzes eine SMS oder E-Mail erhalten. Weitere Informationen finden Sie unter EventBridge Targets (Ziele).

Eine EventBridge Regel für Audit Manager erstellen

Gehen Sie wie folgt vor, um eine EventBridge Regel zu erstellen, die bei einem von Audit Manager ausgegebenen Ereignis ausgelöst wird. Ereignisse werden auf bestmögliche Weise ausgegeben.

Um eine EventBridge Regel für Audit Manager zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie auf der Seite Define rule detail (Regeldetail festlegen) einen Namen und eine Beschreibung für die Regel ein.
5. Behalten Sie die Standardwerte für Event Bus und Regeltyp bei und wählen Sie dann Weiter aus.
6. Wählen Sie auf der Seite „Ereignismuster erstellen“ unter Ereignisquelle die Option AWS Ereignisse oder EventBridge Partnerereignisse aus.
7. Wählen Sie als Creation method (Erstellungsmethode) die Option Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

8. Schreiben Sie unter Event pattern (Ereignismuster) ein Ereignismuster in JSON und geben Sie die Felder an, die Sie für den Abgleich verwenden möchten.

   Um ein Audit Manager-Ereignis zuzuordnen, können Sie das folgende einfache Muster verwenden:

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   *Event*Ersetzen Sie es durch einen der folgenden unterstützten Werte:

   a. Geben Sie `Assessment Created` ein, um Benachrichtigungen zu erhalten, wenn eine Bewertung erstellt wird.

   b. Geben Sie `Assessment Updated` ein, um Benachrichtigungen zu erhalten, wenn eine Bewertung aktualisiert wird.

   c. Geben Sie `Assessment Deleted` ein, um Benachrichtigungen zu erhalten, wenn eine Bewertung gelöscht wird.

   d. Geben Sie `Assessment ControlSet Delegation Created` ein, um Benachrichtigungen zu erhalten, wenn ein Kontrollsatz zur Überprüfung delegiert wird.

   e. Geben Sie `Assessment ControlSet Reviewed` ein, um Benachrichtigungen zu erhalten, wenn ein Prüfungskontrollsatz überprüft wird.

   f. Geben Sie `Assessment Control Reviewed` ein, um Benachrichtigungen zu erhalten, wenn eine Bewertungskontrolle überprüft wird.

   > **Tip**
   >
   > Fügen Sie Ihrem Ereignismuster nach Bedarf weitere Felder hinzu. Weitere Informationen zu verfügbaren Feldern finden Sie unter EventBridge Amazon-Ereignismuster.

9. Wählen Sie Weiter aus.

10. Wählen Sie im Abschnitt Select target(s) (Ziel(e) auswählen) das Ziel aus, das Sie für diese Regel erstellt haben, und konfigurieren Sie dann weitere für diesen Typ erforderliche Optionen. Wenn Sie zum Beispiel Amazon SNS wählen, stellen Sie sicher, dass Ihr SNS-Thema korrekt konfiguriert ist, damit Sie per E-Mail oder SMS benachrichtigt werden.

> **Tip**
>
> Die angezeigten Felder variieren je nach ausgewähltem Dienst. Weitere Informationen zu verfügbaren Zielen finden Sie unter In der EventBridge Konsole verfügbare Ziele.

11. Für viele Zieltypen sind EventBridge Berechtigungen erforderlich, um Ereignisse an das Ziel zu senden. In diesen Fällen EventBridge kann die IAM-Rolle erstellt werden, die für die Ausführung Ihrer Regel erforderlich ist.

    a. Um automatisch eine IAM-Rolle zu erstellen, wählen Sie Eine neue Rolle für diese spezifische Ressource erstellen.

    b. Wenn Sie eine zuvor erstellte IAM-Rolle verwenden möchten, wählen Sie Use existing role (Vorhandene Rolle verwenden)

12. (Optional) Wählen Sie Add another target (Weiteres Ziel hinzufügen) aus, um ein weiteres Ziel für diese Regel hinzuzufügen.
13. Wählen Sie Weiter aus.
14. (Optional) Fügen Sie auf der Seite Configure tags (Tags konfigurieren) beliebige Tags hinzu und wählen Sie Next (Weiter).
15. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die eingerichteten Regeln, um sicherzustellen, dass sie den Anforderungen Ihrer Ereignisüberwachung entsprechen.
16. Wählen Sie Regel erstellen aus. Ihre Regel wird nun auf Audit Manager-Ereignisse überwachen und diese an das von Ihnen angegebene Ziel senden.

AWS Audit Manager API-Aufrufe protokollieren mit CloudTrail

Audit Manager ist in einen Dienst integriert CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service in Audit Manager ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für Audit Manager als Ereignisse. Die Aufrufe, die erfasst werden, umfassen Aufrufe von der Audit Manager-Konsole und Codeaufrufe der Audit Manager-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 Audit Manager.

Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen.

Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Audit Manager gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zum Audit Manager in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in Audit Manager auftritt, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet.

Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -API-Ereignisverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Audit Manager, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket.

Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie 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

Alle Audit Manager Manager-Aktionen werden von der AWS Audit Manager API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe der `UpdateAssessmentFramework` API-Operationen `CreateControl`,`DeleteControl`, und Einträge in den CloudTrail Protokolldateien.

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 Anforderung mit Root-Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Grundlegendes zu Einträgen in der Protokolldatei von Audit Manager

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. 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 die `CreateAssessment`Aktion demonstriert.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
```

```
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

Grundlegendes zur Konfiguration und Schwachstellenanalyse in AWS Audit Manager

Konfiguration und IT-Kontrollen liegen in der gemeinsamen Verantwortung AWS von Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Deaktivierung AWS Audit Manager

Sie können Audit Manager deaktivieren, wenn Sie den Service nicht mehr verwenden möchten. Wenn Sie Audit Manager deaktivieren, haben Sie auch die Möglichkeit, alle Ihre Daten zu löschen.

Standardmäßig werden Ihre Daten nicht gelöscht, wenn Sie Audit Manager deaktivieren. Nachweisdaten werden ab dem Zeitpunkt der Erstellung zwei Jahre lang aufbewahrt. Ihre anderen Audit Manager-Ressourcen (einschließlich Bewertungen, benutzerdefinierte Kontrollen und benutzerdefinierte Frameworks) werden auf unbestimmte Zeit aufbewahrt und sind verfügbar, wenn Sie Audit Manager in Zukunft erneut aktivieren. Weitere Informationen zur Datenaufbewahrung finden Sie unter Datenschutz in diesem Handbuch.

Wenn Sie Ihre Daten löschen möchten, löscht Audit Manager alle Nachweisdaten zusammen mit allen Audit Manager-Ressourcen, die Sie erstellt haben (einschließlich Bewertungen, benutzerdefinierter Kontrollen und benutzerdefinierter Frameworks). Alle Ihre Daten werden innerhalb von sieben Tagen nach Deaktivierung von Audit Manager gelöscht.

Themen

Verfahren

Sie können Audit Manager über die Audit Manager Manager-Konsole, die AWS Command Line Interface (AWS CLI) oder die Audit Manager Manager-API deaktivieren.

⚠ Warning

- Wenn Sie Audit Manager deaktivieren, wird Ihr Zugriff gesperrt und der Service sammelt keine Nachweise mehr für bestehende Bewertungen. Sie können auf nichts im Service zugreifen, es sei denn, Sie aktivieren Audit Manager erneut.
- Das Löschen aller Daten ist eine permanente Aktion. Wenn Sie sich entscheiden, Audit Manager in Zukunft wieder zu aktivieren, können Ihre Daten nicht wiederhergestellt werden.

Audit Manager console

Um Audit Manager auf der Audit Manager-Konsole zu deaktivieren

1. Gehen Sie auf der Registerkarte Allgemeine Einstellungen zum Abschnitt Deaktivieren AWS Audit Manager.
2. Wählen Sie Disable (deaktivieren) aus.
3. Überprüfen Sie im Popup-Fenster Ihre aktuellen Datenaufbewahrungseinstellungen.
    a. Um mit Ihrer aktuellen Auswahl fortzufahren, wählen Sie Audit Manager deaktivieren.
    b. Um Ihre aktuelle Auswahl zu ändern, führen Sie die folgenden Schritte aus:
        i. Wählen Sie Abbrechen, um zur Einstellungsseite zurückzukehren.
        ii. Um die Standardeinstellung für die Datenspeicherung zu verwenden, deaktivieren Sie Alle Daten löschen. Bei dieser Auswahl werden Nachweisdaten ab dem Zeitpunkt ihrer Erstellung zwei Jahre lang aufbewahrt, und andere Ressourcen des Audit Manager werden auf unbestimmte Zeit aufbewahrt.
        iii. Um Ihre Daten zu löschen, aktivieren Sie Alle Daten löschen.
        iv. Wählen Sie Deaktivieren und anschließend Audit Manager deaktivieren, um Ihre Auswahl zu bestätigen.

AWS CLI

Bevor Sie beginnen

Bevor Sie Audit Manager deaktivieren, können Sie den Befehl update-settings ausführen, um Ihre bevorzugte Datenaufbewahrungsrichtlinie festzulegen. Standardmäßig speichert Audit Manager Ihre Daten. Wenn Sie die Löschung Ihrer Daten beantragen möchten, verwenden Sie den Parameter `--deregistration-policy` mit dem `deleteResources`-Wert auf `ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Um Audit Manager zu deaktivieren in AWS CLI

Wenn Sie bereit sind, Audit Manager zu deaktivieren, führen Sie den Befehl deregister-account aus.

```
aws auditmanager deregister-account
```

Audit Manager API

Bevor Sie beginnen

Bevor Sie Audit Manager deaktivieren, können Sie den UpdateSettingsAPI-Vorgang verwenden, um Ihre bevorzugte Datenaufbewahrungsrichtlinie festzulegen. Standardmäßig speichert Audit Manager Ihre Daten. Wenn Sie Ihre Daten löschen möchten, können Sie das DeregistrationPolicyAttribut verwenden, um die Löschung Ihrer Daten anzufordern.

Um Audit Manager mithilfe der API zu deaktivieren

Wenn Sie bereit sind, Audit Manager zu deaktivieren, rufen Sie den DeregisterAccountVorgang auf.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Operationen und Parameter in einer der sprachspezifischen Sprachen AWS SDKs.

Nächste Schritte

Wenn Sie Audit Manager erneut aktivieren müssen, nachdem Sie ihn deaktiviert haben, gehen Sie wie folgt vor, um den Dienst wieder zum Laufen zu bringen.

Um Audit Manager erneut zu aktivieren, nachdem Sie ihn deaktiviert haben

Gehen Sie zur Homepage des Audit Manager-Service und befolgen Sie die Schritte, um Audit Manager als neuen Benutzer einzurichten. Weitere Informationen finden Sie unter Einrichtung AWS Audit Manager mit den empfohlenen Einstellungen.

Tip

- Wenn Sie sich entschieden haben, Ihre Daten zu löschen, als Sie Audit Manager deaktiviert haben, müssen Sie warten, bis Ihre Daten gelöscht sind, bevor Sie den Service wieder aktivieren können. Je nachdem, wie viele Daten Sie haben, kann dies bis zu sieben Tage dauern. Sie können jedoch gerne versuchen, Audit Manager vorher erneut zu aktivieren. In vielen Fällen werden Daten in nur einer Stunde gelöscht.
- Wenn Sie sich dafür entschieden haben, Ihre Daten nicht zu löschen, gehen Ihre vorhandenen Bewertungen in einen Ruhezustand über und es werden keine Nachweise mehr gesammelt. Um erneut mit der Erfassung von Nachweisen für eine bereits

bestehende Bewertung zu beginnen, bearbeiten Sie die Bewertung und wählen Sie Speichern, ohne Änderungen vorzunehmen.

Weitere Ressourcen

- Weitere Informationen zur Datenspeicherung in Audit Manager finden Sie unter Datenschutz in diesem Handbuch.

Dokumentenverlauf für AWS Audit Manager das Benutzerhandbuch

In der folgenden Tabelle werden die wichtigen Änderungen in den einzelnen Versionen des AWS Audit Manager Benutzerhandbuchs ab dem 8. Dezember 2020 beschrieben.

Änderung	Beschreibung	Datum
Updates für fünf unterstützte Frameworks	Die folgenden Frameworks wurden aktualisiert: • CCCS Medium Cloud Control • ISO/IEC 27001:2013 Anhang A • PCI DSS V3.2.1 • PCI DSS V4.0 • SSAE-18 SOC 2	17. Juli 2025
Updates für fünf unterstützte Frameworks	Die folgenden Frameworks wurden aktualisiert: • Amazon Web Services (AWS) Well Architected Framework (WAF) v10 • FedRAMP Security Baseline Controls r4 • NIST SP 800-171 Rev. 2 • NIST-CSF-V1.1 • NIST-SP-800-53-R5	19. Juni 2025
Updates für drei unterstützte Frameworks	Die folgenden Frameworks wurden aktualisiert: • ACSC Essential Eight	4. Juni 2025

	• ACSC ISM • CIS Critical Security Controls Version 8.0, IG1	
Aktualisiertes unterstütztes Framework: CIS Controls v7.1, IG1	Das CIS Controls v7.1 IG1 Framework wurde aktualisiert. Weitere Informationen finden Sie unter CIS Controls v7.1,. IG1	14. Mai 2025
Die ListBuckets s3_-Richtlinie wurde aktualisiert	AWS Audit Manager hat die `s3_ListBuckets` Richtlinie und die Dokumentation aktualisiert, sodass sie der Richtlinie `s3_GetBucketEncryption` entsprechen. Weitere Informationen finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen.	24. März 2025
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditManagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	24. September 2024
Neues unterstütztes Framework: Best Practices für AWS generative KI v2	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter AWS Generative AI Best Practices Framework v2.	11. Juni 2024

Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditManagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	10. Juni 2024
Verwenden Sie allgemeine Kontrollen, um die Durchführung von Bewertungen anhand Ihrer Unternehmenskontrollen zu vereinfachen	Wenn Sie ein benutzerdefiniertes Steuerelement erstellen, können Sie jetzt allgemeine Kontrollen als Beweisquelle verwenden. Jedes gemeinsame Steuerelement ist einer verwalteten Gruppierung relevanter AWS Datenquellen zugeordnet. Diese vordefinierten Gruppierungen vereinfachen die Erfassung von Nachweisen, da nicht mehr festgelegt werden muss, welche AWS Ressourcen für eine bestimmte Kontrolle bewertet werden müssen. Informationen darüber, wie Sie gängige Kontrollen finden und sie als Beweisquellen verwenden können, finden Sie in der Kontrollbibliothek.	6. Juni 2024

Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditManagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	17. Mai 2024
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat die AWSAuditManagerAdministratorAccessRichtlinie aktualisiert. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	15. Mai 2024
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditManagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	15. Mai 2024
Support für zusätzliche AWS API-Aufrufe	Sie können jetzt zusätzliche AWS API-Aufrufe als Datenquellen für Ihre benutzerdefinierten Steuerelemente in Audit Manager verwenden. Weitere Informationen finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen.	15. Mai 2024

Neues unterstütztes Framework: PCI DSS V4.0	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter PCI DSS V4.0.	19. Dezember 2023
Support für zusätzliche AWS API-Aufrufe	Sie können jetzt zusätzlic he AWS API-Aufrufe als Datenquellen für Ihre benutzerdefinierten Steuerele mente in Audit Manager verwenden. Weitere Informati onen finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolld atenquellen.	07. Dezember 2023
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditM anagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	6. Dezember 2023
Support AWS Security Hub CSPM konsolidierter Kontrolle rgebnisse	Audit Manager unterstützt jetzt konsolidierte Kontrollen in AWS Security Hub CSPM. Weitere Informationen finden Sie unter AWS Security Hub CSPM Kontrollen, die von unterstützt werden AWS Audit Manager.	16. November 2023

Integration mit MetricStream	Sie können jetzt Beweise aus Audit Manager in MetricStr eam aufnehmen. Weitere Informationen finden Sie unter Integrationen mit externen GRC-Lösungsanbietern.	14. November 2023
Neues unterstütztes Framework: Best Practices für AWS generative KI	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter AWS -Best Practices -Framework für generative KI v1 .	8. November 2023
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditM anagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	6. November 2023
Integration mit Amazon EventBridge	Sie können jetzt Ereigniss e überwachen, die in Ihrer ereignisgesteuerten Architektur auftreten, AWS Audit Manager und diese Ereignisse als Teil Ihrer ereignisgesteuerten Architekt ur verwenden. Weitere Informationen finden Sie unter Überwachung AWS Audit Manager mit Amazon EventBridge.	18. August 2023

Support bei Risikobewertungen und neuen manuellen Nachweisoptionen	Sie können jetzt den Workflow zur Erstellung benutzerdefinierter Kontrollen verwenden, um Risikobewertungen zu unterstützen. Eine Kontrolle kann jetzt eine Frage zur Risikobewertung darstellen, und Sie können eine Antwort geben, indem Sie eine Datei hochladen oder Text als manuellen Nachweis eingeben. Weitere Informationen finden Sie unter Benutzerdefiniertes Steuerelement erstellen und Manuellen Nachweis hinzufügen.	12. Juni 2023
Support für CSV-Exporte	Sie können jetzt Ihre Beweissuche-Suchergebnisse im CSV-Format exportieren. Weitere Informationen finden Sie unter Exportieren Ihrer Suchergebnisse.	9. Juni 2023
Neues unterstütztes Framework: Handbuch zur Informationssicherheit des Australian Cyber Security Centre (ACSC)	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie im Informationssicherheitshandbuch des Australian Cyber Security Centre (ACSC).	24. März 2023

Verbesserte Bewertungsberichte	Wir haben das Format und den Inhalt der Bewertungsberichte von Audit Manager verbessert. Weitere Informationen zur Navigation und zum Verständnis von Bewertungsberichten finden Sie unter Bewertungsberichte.	23. März 2023
Support für paginierte API-Aufrufe	AWS Audit Manager unterstützt jetzt paginierte API-Aufrufe als Datenquelle für die Beweiserhebung. Weitere Informationen finden Sie unter Paginierte API-Aufrufe.	08. März 2023
Neues unterstütztes Framework: HIPAA Final Omnibus Security Rule 2013	Ein neues vorgefertigtes Framework ist jetzt in verfügbar. AWS Audit Manager Weitere Informationen finden Sie unter HIPAA Final Omnibus Security Rule 2013. Zur Differenzierung wird das zuvor bestehende HIPAA-Framework (in der Framework-Bibliothek früher HIPAA genannt) jetzt HIPAA Security Rule 2003 genannt.	08. März 2023

Support für zusätzliche AWS API-Aufrufe	Sie können jetzt weitere neun AWS API-Aufrufe als Datenquelle für Ihre benutzerdefinierten Steuerelemente in Audit Manager verwenden. Weitere Informationen finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen.	03. März 2023
Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden	Aktualisierung des Leitfadens zur Ausrichtung an bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in IAM.	06. Januar 2023
Neue Datenaufbewahrungseinstellung	Wenn Sie Audit Manager deaktivieren, können Sie entscheiden, ob Sie alle Ihre Daten löschen möchten. Weitere Informationen finden Sie unter Deaktivieren AWS Audit Manager und Löschen von Audit Manager-Daten.	06. Januar 2023
Support für die Beweissuche	Sie können jetzt die Beweissuche verwenden, um Suchanfragen zu Ihren Beweisdaten durchzuführen. Weitere Informationen finden Sie unter Beweissuche.	18. November 2022

Neues unterstütztes Framework: Essential Eight des Australian Cyber Security Centre (ACSC)	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie in Essential Eight des Australian Cyber Security Centre (ACSC).	24. August 2022
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditManagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	7. Juli 2022
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditManagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	20. Mai 2022
Neues unterstütztes Framework: Medium Cloud Control Profile des kanadischen Zentrums für Cybersicherheit	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter Medium Cloud Control Profile des Canadian Centre for Cyber Security.	6. Mai 2022

Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat die AWSAuditManagerAdministratorAccessRichtlinie aktualisiert. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Audit Manager.	29. April 2022
Support für zusätzliche AWS Config verwaltete Regeln	Sie können jetzt weitere 91 AWS Config verwaltete Regeln als Datenquelle für Ihre benutzerdefinierten Kontrollen in Audit Manager verwenden. Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln verwenden mit AWS Audit Manager.	27. April 2022
Support für AWS Config benutzerdefinierte Regeln	Sie können jetzt AWS Config benutzerdefinierte Regeln als Datenquelle für Ihre benutzerdefinierten Steuerelemente in Audit Manager verwenden. Weitere Informationen finden Sie unter Verwenden von AWS Config benutzerdefinierten Regeln mit AWS Audit Manager.	27. April 2022
Neues unterstütztes Framework: ISO/IEC 27001:2013 Anhang A	Ein neues vorgefertigtes Framework ist jetzt in verfügbar. AWS Audit Manager Weitere Informationen finden Sie in Anhang A zu ISO/IEC 27001:2013.	7. April 2022

Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Audit Manager hat das aktualisiert AWSAuditManagerServiceRolePolicy. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Audit Manager.	16. März 2022
Neues unterstütztes Framework: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4	Zwei neue vorgefertigte Frameworks sind jetzt verfügbar in AWS Audit Manager: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 und CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 und 2. Weitere Informationen finden Sie unter CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.4.0.	2. März 2022
Neues unterstütztes Framework: CIS Controls v8 IG1	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter CIS Controls v8 IG1.	2. März 2022

AWS Audit Manager Dashboard	Sie können jetzt das Audit Manager-Dashboard verwenden, um Ihre aktiven Bewertungen zu überwachen und fehlerhafte Beweise schnell zu identifizieren. Weitere Informationen finden Sie unter Verwendung des Audit Manager Dashboards.	18. November 2021
Freigeben eines benutzerdefinierten Frameworks	Sie können jetzt Ihre benutzerdefinierten Audit Manager Manager-Frameworks mit anderen AWS-Konto teilen oder sie AWS-Region unter Ihrem eigenen Konto in ein anderes replizieren. Weitere Informationen finden Sie unter Freigeben eines benutzerdefinierten Frameworks.	22. Oktober 2021
Neue Beispiele für Kontrollen AWS Audit Manager	Sie können sich nun Beispiele für Kontrollen ansehen und erfahren, wie Audit Manager Ihnen hilft, Ihre AWS Umgebung an die jeweiligen Anforderungen anzupassen. Weitere Informationen finden Sie unter Beispiele für AWS Audit Manager Kontrollen.	21. September 2021

Neues unterstütztes Framework: Gramm-Leach-Bliley Act (GLBA)	Ein neues vorgefertigtes Framework ist jetzt in verfügbar. AWS Audit Manager Weitere Informationen finden Sie unter Gramm-Leach-Bliley Act (GLBA).	2. September 2021
Neues Kapitel zur Fehlerbehebung	Ein neues Kapitel zur Fehlerbehebung ist nun verfügbar. Weitere Informationen finden Sie unter Problembehandlung unter AWS Audit Manager.	23. August 2021
Neues Kapitel und Tutorial zur Delegierung	Wir haben unsere Delegationsdokumentation um ein neues Kapitel erweitert. Weitere Informationen finden Sie unter Delegationen in AWS Audit Manager. Wir haben auch ein neues Tutorial hinzugefügt, das sich an Delegierte richtet, die zum ersten Mal einen Kontrollsatz überprüfen. AWS Audit Manager Weitere Informationen finden Sie unter Tutorial für Delegierte: Überprüfung eines Kontrollsatzes.	25. Juni 2021
Neues unterstütztes Framework: NIST SP 800-171 Rev. 2	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter NIST SP 800-171 Rev. 2.	17. Juni 2021

Verbesserte Bewertungsberichte	Wir haben das Format und den Inhalt der AWS Audit Manager Bewertungsberichte verbessert. Weitere Informationen zur Navigation und zum Verständnis der neuen Bewertungsberichte finden Sie unter Bewertungsberichte.	8. Juni 2021
Neue Seite mit AWS verwalteten Richtlinien	AWS Audit Manager hat damit begonnen, Änderungen an seinen verwalteten Richtlinien zu verfolgen. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien für AWS Audit Manager.	6. Mai 2021
Neues unterstütztes Framework: NIST Cybersecurity Framework Version 1.1	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter NIST Cybersecurity Framework Version 1.1.	5. Mai 2021
Neues unterstütztes Framework: AWS Well-Architected	Ein neues vorgefertigtes Framework ist jetzt in verfügbar. AWS Audit Manager Weitere Informationen finden Sie unter AWS Well-Architected.	5. Mai 2021

Neues unterstütztes Framework: Bewährte AWS Methoden zur Grundlage nsicherheit	Ein neues vorgefertigtes Framework ist jetzt in verfügbar. AWS Audit Manager Weitere Informati onen finden Sie unter AWS Bewährte Methoden der grundlegenden Sicherheit.	5. Mai 2021
Neues unterstütztes Framework: GxP EU Annex 11	Ein neues vorgefertigtes Framework ist jetzt in verfügbar. AWS Audit Manager Weitere Informati onen finden Sie in GxP EU Annex 11.	28. April 2021
Neues unterstütztes Framework: NIST 800-53 (Rev. 5) Low-Moderate-High	Ein neues vorgefertigtes Framework ist jetzt in verfügbar. AWS Audit Manager Weitere Informati onen finden Sie unter NIST 800-53 (Rev. 5). Low-Moder ate-High	25. März 2021

Neue unterstützte Frameworks: CIS Benchmark for AWS Audit Manager CIS Foundations Benchmark v1.3	Zwei neue vorgefertigte Frameworks sind jetzt verfügbar in AWS Audit Manager: CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1, und CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1 und 2. Weitere Informationen finden Sie unter CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22. März 2021
Erstversion	Erste Version des AWS Audit Manager Benutzerhandbuchs und der API-Referenz.	08. Dezember 2020

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.