aws

Benutzerhandbuch

AWS Audit-Manager

AWS Audit-Manager: Benutzerhandbuch

Table of Contents

Was ist AWS Audit Manager?

Willkommen beim AWS Audit Manager-Benutzerhandbuch.

AWS Audit Manager hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Konformität mit Branchenstandards 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 Featureieren. 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 sowohl für die AWS-Konto als auch für die Services erfasst, 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.

Featureen von Audit Manager

Mit AWS Audit Manager können Sie folgende Aktionen 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 Beweisen, 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 ManagerStandard-Frameworks. Diese Frameworks bieten vorgefertigte Kontrollzuordnungen für gängige Compliance-Standards und -Vorschriften. Dazu gehören der CIS Foundation Benchmark, PCI DSS, DS-GVO, HIPAA, SOC2, GxP und bewährte Verfahren für den Betrieb. AWS
- 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.
- Erheben von Beweisen – Verwenden Sie die Feature zur Beweissuche, 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 Kontrollen – Erstellen Sie Ihre eigene Kontrolle von Grund auf neu oder passen Sie eine vorhandene Kontrolle an Ihre Bedürfnisse an. Sie können auch die Feature für benutzerdefinierte Kontrollen verwenden, um Fragen zur Risikobewertung zu erstellen und die Antworten auf diese Fragen als manuelle Beweise zu speichern.
- Anpassen von Frameworks – Erstellen Sie Ihre eigenen Frameworks mit Standard- oder benutzerdefinierten Kontrollen, die auf Ihren konkreten Anforderungen für interne Audits basieren.
- Teilen Sie benutzerdefinierte Frameworks – Teilen Sie Ihre benutzerdefinierten Audit Manager-Frameworks mit einem anderen AWS-Konto oder replizieren Sie sie in eine andere 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 bei der Sammlung von Beweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Standards und -Vorschriften relevant sind. Ihre Einhaltung wird jedoch nicht bewertet. Die auf diese Weise gesammelten Beweise AWS Audit Manager enthalten 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 ManagerKonzepte und Terminologie – Erfahren Sie mehr über die wichtigsten Konzepte und Begriffe, die in Audit Manager verwendet werden, wie z. B. Bewertungen, Frameworks und Kontrollen.
2. Wie AWS Audit Manager Beweise erhebt – Erfahren Sie, wie Audit Manager Beweise für eine Ressourcenbewertung erhebt.
3. Einrichtung – Erfahren Sie mehr über die Einrichtungsanforderungen für Audit Manager.
4. Erste Schritte – Folgen Sie einem Tutorial, um Ihre erste Audit Manager-Bewertung zu erstellen.
5. AWS Audit ManagerAPI-Referenz – Machen Sie sich mit den API-Aktionen und Datentypen von Audit Manager vertraut.

Weitere Ressourcen für den Audit Manager

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

- Erheben Sie Beweise und verwalten Sie Auditdaten mit AWS Audit Manager
- Manuelles Konfigurieren einer benutzerdefinierten Audit Manager-Bewertung in AWS-Workshops

- Integrieren Sie das Drei-Linien-Modell (Teil 2): Verwandeln Sie AWS Config-Konformitätspakete in AWS Audit Manager-Bewertungen aus dem AWSManagement & Governance-Blog

Konzepte und Terminologie zu AWS Audit Manager

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

A

A| B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | 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. Je nach Ihren Geschäftsanforderungen können Sie 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 Kontrollen, die Sie entsprechend Ihren internen Auditanforderungen anpassen und gruppieren können. Wenn Sie ein Framework als Ausgangspunkt verwenden, können Sie eine Bewertung erstellen, in der die AWS-Konten und Leistungen spezifiziert werden, die Sie in den Umfang Ihres Audits einbeziehen möchten.

Wenn Sie eine Bewertung erstellen, beginnt Audit Manager automatisch mit der Bewertung der Ressourcen in Ihren AWS-Konten und Leistungen auf der 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 Featureieren.

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 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 Generieren eines Bewertungsberichts.

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 Ziel des Bewertungsberichts (optional).

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 Featureieren 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
- Security Operations Center/Incident Response
- 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 verwalten, indem Sie die Rolle des Audit-Verantwortlichen/Delegierten verwenden und jedem Benutzer spezielle IAM-Richtlinien zuweisen. 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.

C

A| B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Änderungsprotokoll

Für jede Kontrolle in einer Bewertung erfasst Audit Manager Änderungsprotokolle, um die Benutzeraktivitäten für diese Kontrolle nachzuverfolgen. Anschließend können Sie einen Audit Trail mit Aktivitäten überprüfen, die sich auf eine bestimmte Kontrolle beziehen. Weitere Informationen darüber, welche Benutzeraktivitäten in Änderungsprotokollen erfasst werden, finden Sie unter Registerkarte „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.

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. Kontrollen dienen dazu, die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Informationen zu schützen und eine Reihe definierter Sicherheitsanforderungen zu erfüllen. Sie bieten die Gewissheit, dass Ihre Ressourcen wie vorgesehen Featureieren, 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. Jeder Beweise wird zu einem Datensatz, anhand dessen Sie die Einhaltung der Kontrollanforderungen nachweisen können.

In Audit Manager gibt es zwei Arten:

- Standardkontrollen – Dies sind vorgefertigte Kontrollen, die einem bestimmten Framework in Audit Manager zugeordnet sind. Verwenden Sie Standardkontrollen, um Sie bei der Prüfungsvorbereitung für verschiedene Compliance-Standards und -Vorschriften zu unterstützen.
- Benutzerdefinierte Kontrollen – Dies sind benutzerdefinierte Kontrollen, die Sie als Audit Manager-Benutzer definieren. Verwenden Sie benutzerdefinierte Kontrollen, um bestimmte Compliance-Anforderungen für interne Audits oder Risikobewertungen von Lieferanten zu erfüllen.

Weitere Informationen finden Sie unter Beispiele für AWS Audit Manager-Kontrollen. Anweisungen zum Erstellen und Konfigurieren von Kontrollen finden Sie unter Kontrollbibliothek.

Kontrolldomänen

Sie können sich eine Kontrolldomäne als eine allgemeine Kategorie von Kontrollen vorstellen, die nicht spezifisch für ein bestimmtes Framework ist. Kontrolldomänengruppierungen sind eine der leistungsstärksten Featureen 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.

> **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.

Audit Manager unterteilt Kontrollen in die folgenden Kontrolldomänen.

Kontrolld omänenname	Beschreibung dessen, wofür diese Kontrollen gelten
Geschäftskontinuität und Notfallplanung	Wie Sie Prozesse einrichten, die kritische Geschäftsabläufe vor den Auswirkungen größerer System- und Netzwerkstörungen schützen.
Änderungsmanagement	Wie Sie Änderungen an Ihrer Cloud-Infrastruktur testen, genehmigen, implementieren und dokumentieren.
Datensicherheit und Datenschutz	Wie Sie den Datenschutz, die Verfügbarkeit und die Integrität Ihrer Daten sichern.
Entwicklungs- und Konfigurationsmanagement	Wie Sie Ihre Cloud-Infrastruktur in einem gewünschten und konsistenten Zustand halten.
Governance und Aufsicht	Wie Sie Ihre Nutzung von Cloud-Computing mit Ihren rechtlichen, regulatorischen und ethischen Verpflichtungen in Einklang bringen.
Identity and Access Management	Wie Sie sicherstellen, dass die richtigen Benutzer den entsprechenden Zugriff auf Ihre Technologieressourcen haben.
Vorfallmanagement	Wie Sie Verantwortlichkeiten und Verfahren festlegen, die eine schnelle und effektive Reaktion auf Sicherheitsvorfälle gewährleisten.
Protokollierung und Überwachung	So überprüfen Sie Benutzeraktivitäten auf Hinweise darauf, dass eine unbefugte Aktivität versucht oder ausgeführt wurde.
Netzwerkmanagement	Wie Sie Ihr Datennetzwerk mithilfe eines Netzwerkmanagementsystems verwalten und betreiben.
Personalmanagement	Wie Sie Personalsicherheitsrisiken auf organisatorischer Ebene bewerten und verwalten.
Physische Sicherheit	Wie Sie physische Sicherheitsprobleme in Ihren Einrichtungen erkennen und verhindern.

Kontrolld omänenname	Beschreibung dessen, wofür diese Kontrollen gelten
Risikomanagement	Wie Sie potenzielle Risiken und Verluste bewerten und wie Sie solche Bedrohungen reduzieren oder beseitigen.
Lieferketten-Manag ement	Wie Sie die mit IT-Produkten, Anbietern und Lieferketten verbundenen Risiken identifizieren, bewerten und mindern.
Verwaltung von Benutzergeräten	So reduzieren Sie das Risiko, dass die IT-Hardware Ihrer Mitarbeiter verloren geht, beschädigt oder kompromittiert wird.
Schwachst ellenmanagement	Wie Sie alle bekannten Schwachstellen für Ressourcen in Ihrer Cloud-Infrastruktur definieren, bewerten und beheben.

D

A| B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Datenquelle

Audit Manager verwendet eine Datenquelle, um Beweise für eine Kontrolle zu erheben. Die folgende Terminologie beschreibt, was eine Datenquelle ist und wie sie Featureiert.

- Ein Datenquellentyp definiert, woher Audit Manager Beweise für eine Kontrolle erhebt. Wenn Sie Ihre eigenen Beweise hochladen, ist der Datenquellentyp Manuell. Wenn Audit Manager die Beweise in Ihrem Namen erhebt, ist der Datenquellentyp einer der folgenden: AWS Security Hub, AWS Config, AWS CloudTrail oder AWS- API-Aufrufe. Die Audit Manager-API bezeichnet einen Datenquellentyp als sourceType (Singular) oder ControlSources (Plural).
- Ein Mapping ist ein bestimmtes Schlüsselwort, das sich auf einen Datenquellentyp bezieht. Dies kann beispielsweise ein CloudTrail-Ereignisname oder ein AWS Config-Name sein. Die Audit Manager-API bezeichnet dies als SourceKeyword (Singular) oder ControlMappingSources (Plural).
- Ein Datenquellenname ist ein Name, der einer Datenquelle gegeben wird. Mit anderen Worten, ein Datenquellenname bezeichnet die Kombination aus Datenquellentyp und Zuordnung. Für Standardkontrollen stellt Audit Manager einen Standarddatenquellennamen bereit (z. B. Datenquelle 1 und Datenquelle 2). Für benutzerdefinierte Kontrollen können Sie Ihren eigenen Datenquellennamen angeben. Dies kann Ihnen helfen, zwischen mehreren Zuordnungen zu

unterscheiden, die unter denselben Datenquellentyp fallen. Die Audit Manager-API bezeichnet einen Datenquellennamen als SourceName.

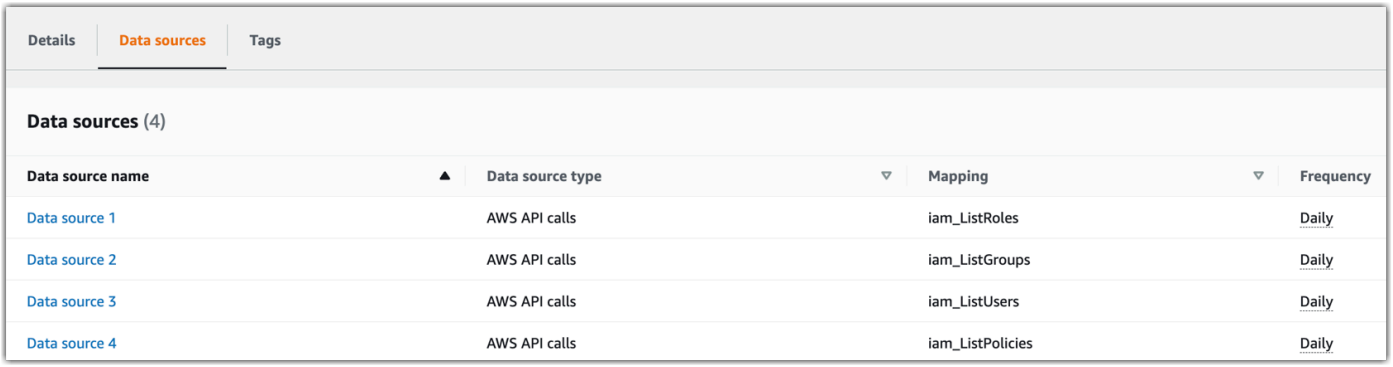
Eine einzelne Kontrolle kann mehrere Datenquellentypen und mehrere Zuordnungen haben. Beispielsweise kann eine Kontrolle Beweise aus einer Mischung von Datenquellentypen (wie AWS Config und Security Hub) erheben. Eine andere Kontrolle hat möglicherweise AWS Config als einzigen Datenquellentyp mit mehrere AWS Config-Regeln als Zuordnungen.

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

Datenquellentyp	Beschreibung	Beispiel für Zuweisungen
AWS Security Hub	Verwenden Sie diesen Datenquellentyp, um eine Momentaufnahme Ihrer Ressourcensicherheit zu erstellen. Audit Manager verwendet den Namen einer Security Hub-Kontrolle als Zuordnungsschlüsselwort und meldet das Ergebnis dieser Sicherheitsprüfung direkt von Security Hub.	`1.1 – Avoid the use of the "root" account`
AWS Config	Verwenden Sie diesen Datenquellentyp, um einen Snapshot Ihrer Ressourcensicherheit zu erstellen. Audit Manager verwendet den Namen einer AWS Config-Regel als Zuordnungsschlüsselwort und meldet das Ergebnis dieser Regelprüfung direkt von AWS Config.	`EC2_INSTANCE_MANAGED_BY_SSM`

Datenquellentyp	Beschreibung	Beispiel für Zuweisungen
AWS CloudTrail	Verwenden Sie diesen Datenquellentyp, um eine bestimmte Benutzera ktivität nachzuverfolgen, die für Ihr Audit erforderl ich ist. Audit Manager verwendet den Namen eines CloudTrail-Ereignisses als Zuordnungsschlüsselwort und erfasst die entsprech enden Benutzeraktivitäten aus Ihren CloudTrail-Protoko llen.	`CreateAccessKey`
AWS-API-Aufrufe	Verwenden Sie diesen Datenquellentyp, um über einen API-Aufruf an einen bestimmten AWS-Servi ce einen Snapshot Ihrer Ressourcenkonfiguration zu erstellen. Audit Manager verwendet den Namen des API-Aufrufs als Zuordnung sschlüsselwort und sammelt die API-Antwort.	`ec2_DescribeSecuri tyGroups`

Die folgende Abbildung zeigt Beispiele für verschiedene Datenquellen, wie sie in der Audit Manager-Konsole zu sehen sind.



> **Note**
>
> Einige Datenquellentypen sind zwar AWS-Services, aber ein Datenquellentyp unterscheidet sich von einer Leistung im Umfang. Weitere Informationen finden Sie unter Was ist der Unterschied zwischen einer Leistung im Umfang und einem Datenquellentyp? im Abschnitt Problembehebung dieses Handbuchs.

Delegierter

Ein Delegierter ist ein AWS Audit Manager-Benutzer mit eingeschränkten Rechten. 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 Delegierungen in AWS Audit Manager.

E

A| B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | 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.

- Automatisierte Beweise – Dies sind die Beweise, die Audit Manager automatisch sammelt. Dies umfasst die folgenden drei Kategorien automatisierter Beweise:
  - Compliance-Überprüfung – Das Ergebnis einer Compliance-Überprüfung wird von AWS Security Hub, AWS Config, oder beiden erfasst. Beispiele für Compliance-Überprüfungen sind ein Sicherheitsprüfungsergebnis von Security Hub für eine PCI-DSS-Kontrolle und eine AWS Config-Regelauswertung für eine HIPAA-Kontrolle. Weitere Informationen finden Sie unter AWS Config-Regeln, die von AWS Audit Manager unterstützt werden und AWS Security Hub-Kontrollen, die von AWS Audit Manager unterstützt werden.
  - Benutzeraktivität – Benutzeraktivitäten, die eine Ressourcenkonfiguration ändern, werden in den 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-Ereignisnamen, die von AWS Audit Manager unterstützt werden.
  - Konfigurationsdaten – Ein Snapshot der Ressourcenkonfiguration wird direkt von einem AWS-Service auf täglicher, wöchentlicher oder monatlicher Basis erfasst. 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 von AWS Audit Manager unterstützte API-Aufrufen.
- Manuelle Beweise – Dies sind die Beweise, die Sie selbst zu Audit Manager hinzufügen. Es gibt drei Möglichkeiten, eigene Beweise hinzuzufügen:
  - Importieren einer Datei aus Amazon S3
  - Laden Sie eine Datei von Ihrem Browser hoch
  - Geben Sie eine Textantwort auf eine Frage zur Risikobeurteilung ein

  Weitere Informationen finden Sie unter Manuelle Beweise in AWS Audit Manager hinzufügen .

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 über die Beweissammlung finden Sie unter Wie AWS Audit Manager Beweise sammelt. Anweisungen zum Überprüfen von Beweisen in einer Bewertung finden Sie unter Überprüfung der Beweise in einer Bewertung.

Methode zur Beweissuche

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

- Automatisierte Kontrollen erfassen automatisch Beweise aus AWS-Datenquellen. Diese automatisierten Beweise können Ihnen helfen, die vollständige oder teilweise Einhaltung der Kontrolle nachzuweisen.
- Bei manuellen Kontrollen müssen Sie Ihre eigenen Beweise hochladen, um die Einhaltung der Kontrolle 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.
> Beispiele:
>
> - Das Framework AWS Generative KI Best Practices enthält eine Kontrolle 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 Beweise, aus denen hervorgeht, ob CloudWatch-Alarme für das AWS-Konto 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 hierzu finden Sie unter Exportziel (optional).

F

A| B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Framework

Ein Audit Manager-Framework ist eine Datei, die verwendet wird, um Bewertungen für einen bestimmten Standard oder ein bestimmtes Prinzip der Risikosteuerung zu strukturieren und zu automatisieren. Diese Frameworks helfen Ihnen dabei, Ihre AWS-Ressourcen den Anforderungen einer Kontrolle zuzuordnen. Sie enthalten eine Sammlung von vorgefertigten oder vom Kunden definierten Kontrollen. Die Sammlung enthält Beschreibungen und Testverfahren für jede Kontrolle. Diese Kontrollen sind auf der Grundlage der Anforderungen eines bestimmten Compliance-Standards oder einer bestimmten Compliance-Verordnung organisiert und gruppiert. Beispiele hierfür sind PCI DSS und die DSGVO.

In Audit Manager gibt es zwei Arten von Frameworks:

- Standard-Frameworks – Vorgefertigte Frameworks, die auf AWS bewährten Methoden für verschiedene Compliance-Standards und Vorschriften basieren. Sie können diese Frameworks verwenden, um Sie bei der Vorbereitung von Audits zu unterstützen.
- Benutzerdefinierte Frameworks – Maßgeschneiderte Frameworks, die Sie als Audit Manager-Benutzer selbst definieren. Sie können diese Frameworks verwenden, um Sie bei der

Prüfungsvorbereitung gemäß Ihren konkreten Compliance- oder Risk-Governance-Anforderungen zu unterstützen.

Anweisungen zum Erstellen und Verwalten von Frameworks finden Sie unter Framework-Bibliothek.

> **Note**
>
> AWS Audit Manager hilft bei der Sammlung von Beweisen, die für die Überprüfung der Einhaltung bestimmter Compliance-Standards und -Vorschriften relevant sind. Ihre Einhaltung wird jedoch nicht bewertet. Die auf diese Weise gesammelten Beweise AWS Audit Manager enthalten 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 Feature zur gemeinsamen Nutzung benutzerdefinierter Frameworks von Audit Manager verwenden, um Ihre benutzerdefinierten Frameworks schnell über AWS-Konten und Regionen hinweg zu teilen. Um ein benutzerdefiniertes Framework gemeinsam zu nutzen, erstellen Sie eine Anfrage zur gemeinsamen Nutzung. Der Empfänger der Teilungsanfrage 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.

R

A| B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Ressource

Eine Ressource ist ein Sachwert oder ein Informationsgut, das im Rahmen eines Audits bewertet wird. Beispiele für AWS sind Amazon EC2-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 Beweise zur Compliance-Überprüfung für Kontrollen, die AWS Config und Security Hub als Datenquellentyp verwenden. 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:

- Nicht konform – Dies bezieht sich auf Ressourcen, bei denen Probleme mit der Compliance-Überprüfung aufgetreten sind. Dies passiert, wenn Security Hub ein Fehlerergebnis für die Ressource meldet oder wenn AWS Config ein nicht konformes Ergebnis gemeldet wird.
- Konform – Dies bezieht sich auf Ressourcen, bei denen keine Probleme mit der Compliance-Überprüfung aufgetreten sind. Dies passiert, wenn Security Hub ein Bestanden-Ergebnis für die Ressource meldet oder wenn AWS Config ein konformes Ergebnis gemeldet wird.
- Nicht eindeutig – Dies bezieht sich auf Ressourcen, für die keine Compliance-Überprüfung verfügbar oder anwendbar ist. Dies passiert, wenn AWS Config oder Security Hub der zugrunde liegende Datenquellentyp ist, diese Services jedoch nicht aktiviert sind. Dies ist auch der Fall, wenn der zugrunde liegende Datenquellentyp keine Compliance-Überprüfungen unterstützt (z. B. manuelle Beweise, AWS-API-Aufrufe oder CloudTrail).

S

A| B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Leistung im Umfang

Dies ist ein AWS-Service, der im Umfang Ihrer Bewertung enthalten ist. Wenn Sie angeben, dass eine Leistung im Umfang Ihrer Bewertung enthalten ist, bewertet Audit Manager die Ressourcen dieses Services. Der Audit Manager kann eine Vielzahl von Ressourcen aus einer Leistung im Umfang beurteilen. Zu den Beispielressourcen gehören:

- Eine Amazon-EC2-Instance.
- Ein S3-Bucket
- Ein Benutzer oder eine Rolle
- Eine DynamoDB-Tabelle
- Eine Netzwerkkomponente wie eine Amazon Virtual Private Cloud (VPC)-Sicherheitsgruppe oder eine Netzwerk-Zugriffskontrollliste (Access Control List, ACL)

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung aus einem Standard-Framework zu erstellen oder zu aktualisieren, ist die Liste der im Umfang enthaltenen AWS-Services standardmäßig vorausgewählt. Diese Liste kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Standard-Frameworks. Wenn ein Standard-Framework nur manuelle Kontrollen enthält, fallen keine AWS-Services in Ihre Bewertung, und Sie können Ihrer Bewertung keine Services hinzufügen.

Wenn Sie die Liste der Services bearbeiten müssen, die für ein Standard-Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

> **Note**
>
> Beachten Sie, dass sich eine Leistung im Umfang von einem Datenquellentyp unterscheidet, bei dem es sich auch um einen AWS-Service oder etwas anderes handeln kann. Weitere Informationen finden Sie unter Was ist der Unterschied zwischen einer Leistung im Umfang und einem Datenquellentyp? im Abschnitt Problembehebung dieses Handbuchs.

Wie AWS Audit Manager Beweise sammelt

Bei jeder aktiven Bewertung in AWS Audit Manager werden automatisch Beweise aus einer Reihe von Datenquellen gesammelt. Jede Bewertung hat einen definierten Umfang, der die AWS-Services und die Konten festlegt, aus welchen Audit Manager Daten sammelt. Alle dieser definierten Leistungen und Konten umfassen mehrere Ressourcen, und jede Ressource ist ein Systeminventar, das Ihnen gehört. 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 Compliance-Überprüfung und alle Benutzeraktivitäten erfasst. 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 Beweisen finden Sie unter Beweise 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 mit dieser Ressource erfasst wurden, als auch die Metadaten, die angeben, welche Kontrolle die Daten unterstützen. AWS 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 Erfassung von Beweisen ist ein fortlaufender Prozess, der mit der Erstellung Ihrer Bewertung beginnt. AWS Audit Manager sammelt Beweise aus mehreren Datenquellen mit unterschiedlichen Frequenzen. Daher gibt es keine allgemeingültige Antwort darauf, wie oft Beweise gesammelt werden. Die Häufigkeit der Beweissuche hängt von der Art der Beweise und ihrer Datenquelle ab, wie unten beschrieben.

- Compliance-Überprüfungen – Audit Manager sammelt diese Art von Beweisen von AWS Security Hub und AWS Config.
  - Für AWS Security Hub richtet sich die Häufigkeit der Beweissuche nach dem Zeitplan Ihrer Security Hub-Prüfungen. Weitere Informationen zum Zeitplan der Security Hub-Prüfungen finden Sie unter Zeitplan für die Ausführung von Sicherheitsprüfungen im AWS Security HubBenutzerhandbuch. Weitere Informationen zu den von Audit Manager unterstützten Security Hub-Prüfungen finden Sie unter AWS Security Hub -Steuerelemente, die von unterstützt werden AWS Audit Manager.
  - Für AWS Config richtet sich die Häufigkeit der Beweissuche nach 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 ConfigBenutzerhandbuch. Weitere Informationen zu den von Audit Manager unterstützten AWS-Config-Regeln finden Sie unter AWS-Config-Regeln unterstützt von AWS Audit Manager.
- Benutzeraktivität – Audit Manager sammelt diese Art von AWS CloudTrail Beweisen kontinuierlich. Diese Häufigkeit ist kontinuierlich, da Benutzeraktivitäten zu jeder Tageszeit auftreten können. Weitere Informationen finden Sie unter AWS CloudTrail -Ereignisnamen, die von unterstützt werden AWS Audit Manager.

- Konfigurationsdaten – Audit Manager erfasst diesen Beweistyp 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 Kontrollbibliothek. Weitere Informationen darüber, wie Audit Manager API-Aufrufe zur Erstellung von Beweisen verwendet, finden Sie unter Von unterstützte API-Aufrufe 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-Kontrollen

Sie können sich die Beispiele auf dieser Seite ansehen, um mehr darüber zu erfahren, wie Kontrollen in AWS Audit Manager Featureieren. In diesen Beispielen wird beschrieben, wie eine Kontrolle aussieht, wie Audit Manager Beweise für diese Kontrolle generiert und welche nächsten Schritte Sie ergreifen können, um die Einhaltung der Vorschriften nachzuweisen.

> **Tip**
>
> Wir empfehlen Ihnen, im Audit Manager für eine optimale Benutzererfahrung AWS Config und AWS Security Hub zu aktivieren. Wenn Sie diese Services aktivieren, können sie als Datenquellentyp für die Kontrollen in Ihren Audit Manager-Bewertungen verwendet werden. Mit anderen Worten, Audit Manager kann die Ergebnisse von Security Hub und AWS-Config-Regeln verwenden, um automatisierte Beweise zu generieren.
>
> - Stellen Sie nach der Aktivierung von AWS Security Hub 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 von AWS Config sicher, dass Sie auch das entsprechende Konformitätspaket aktivieren AWS-Config-Regeln oder ein Konformitätspaket für den Compliance-Standard bereitstellen, 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

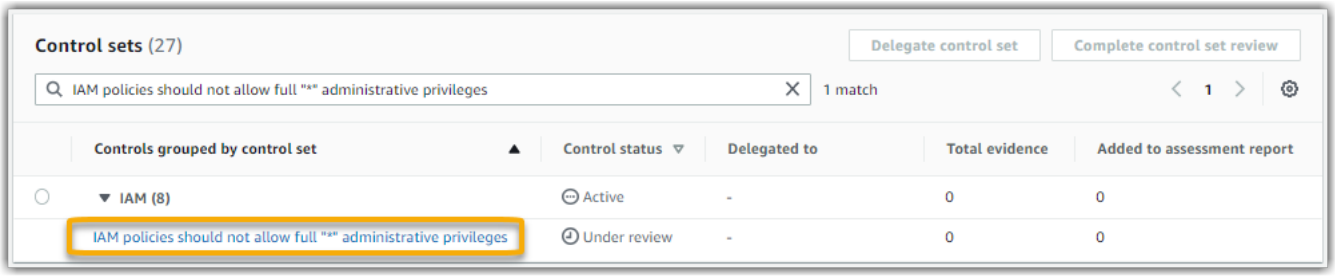
Automatisierte Kontrollen, die AWS Security Hub als Datenquellentyp verwenden

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

Beispiel für Kontrolldetails

- Name der Kontrolle – `IAM policies should not allow full "*" administrative privileges`
- Kontrollsatz – Diese Kontrolle gehört zum Kontrollsatz `IAM`. Dies ist eine Gruppierung von Kontrollen, die sich auf die Identitäts- und Zugriffsverwaltung beziehen.
- Datenquellentyp – AWS Security Hub.
- Art des Beweises – Compliance-Überprüfung

Im folgenden Beispiel befindet sich diese Kontrolle in einer Audit Manager-Bewertung, die auf der Grundlage des FSBP-Frameworks erstellt wurde.



Die Bewertung zeigt den Kontrollstatus. Sie zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden und wie viele dieser Beweise in Ihrem Bewertungsbericht enthalten sind. 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 Ihre IAM-Richtlinien zu weit gefasst sind, um die FSBP-Anforderungen zu erfüllen. Insbesondere kann er überprüfen, ob Ihre vom Kunden verwalteten IAM-Richtlinien Administratorrechte haben, die den folgenden Platzhalterhinweis enthalten: `"Effect": "Allow"` mit `"Action": "*"` über `"Resource": "*"`.

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 IAM-Richtlinien die Ressource und Security Hub und AWS Config sind der Datenquellentyp. Audit Manager sucht nach dem Ergebnis einer bestimmten Security Hub-Prüfung ([IAM.1]), die wiederum eine AWS Config-Regel verwendet, um Ihre IAM-Richtlinien (iam-policy-no-statements-with-admin-access) auszuwerten.
2. Das Ergebnis der Ressourcenbewertung wird gespeichert und in prüferfreundliche Beweise umgewandelt. Audit Manager generiert Compliance-Überprüfungs-Nachweise für Kontrollen, die Security Hub als Datenquellentyp verwenden. Dieser Beweis enthält das Ergebnis der Compliance-Überprüfung, die direkt von Security Hub gemeldet wurde.
3. Audit Manager fügt die gespeicherten Beweise der Kontrolle mit dem Namen `IAM policies should not allow full "*" administrative privileges` 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 Nicht bestanden-Regel von Security Hub an. Dies kann passieren, wenn Ihre IAM-Richtlinien Platzhalter (*) enthalten und zu weit gefasst sind, um die Kontrolle zu erfüllen. In diesem Fall können Sie Ihre IAM-Richtlinien so aktualisieren, dass sie keine vollen Administratorrechte gewähren. Bestimmen Sie, was Benutzer tun müssen, und gestalten Sie dann entsprechende Richtlinien, mit denen die Benutzer nur diese Aufgaben ausführen können. Diese Abhilfemaßnahme trägt dazu bei, Ihre AWS-Umgebung mit den FSBP-Anforderungen in Einklang zu bringen.

Wenn Ihre IAM-Richtlinien 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 Featureiert.

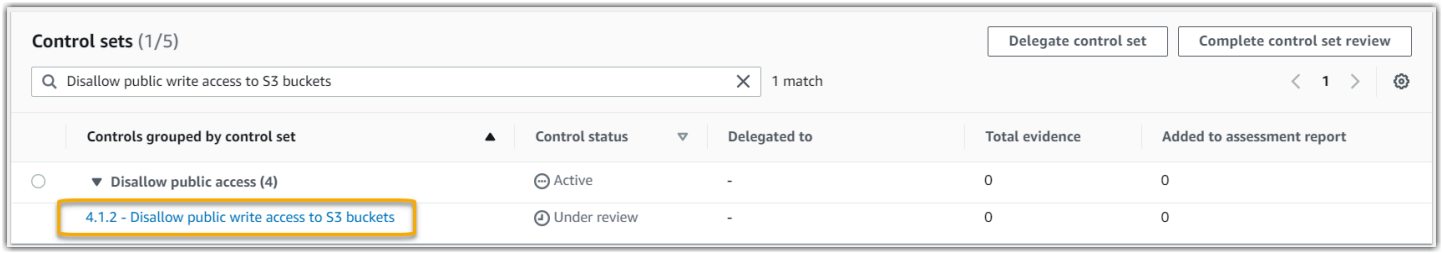
Automatisierte Kontrollen, die AWS Config als Datenquellentyp verwenden

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

Beispiel für Kontrolldetails

- Name der Kontrolle – `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.
- Datenquellentyp – AWS Config.
- Art des Beweises – Compliance-Überprüfung

Im folgenden Beispiel befindet sich diese Kontrolle in einer Audit Manager-Bewertung, die mit dem AWS Control Tower-Guardrails-Framework erstellt wurde.



Die Bewertung zeigt den Kontrollstatus, wie viele Beweise bisher für diese Kontrolle gesammelt wurden und wie viele dieser Beweise in Ihrem Bewertungsbericht enthalten sind. 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 AWS Control Tower-Anforderungen zu erfüllen. 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 Umfang Ihrer Bewertung fallen.
2. Das Ergebnis der Ressourcenbewertung wird gespeichert und in prüferfreundliche Beweise umgewandelt. Audit Manager generiert Beweise zur Compliance-Überprüfung für Kontrollen, die AWS Config als Datenquellentyp verwendet werden. Diese Beweise enthalten das Ergebnis der Compliance-Überprüfung, über die direkt aus AWS Config berichtet wurde.
3. Audit Manager fügt die gespeicherten Beweise der Kontrolle mit dem Namen `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 aus AWS Config an, die 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 Abhilfemaßnahme trägt dazu bei, Ihre AWS-Umgebung an die AWS Control Tower-Anforderungen anzupassen.

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 Featureiert.

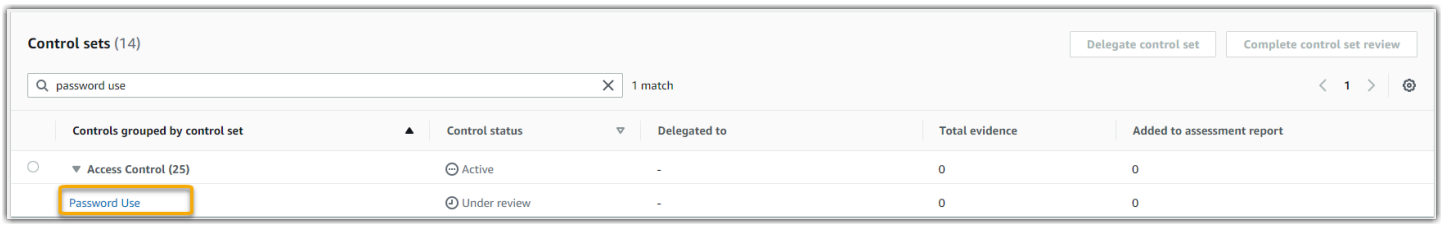
Automatisierte Kontrollen, die AWS-API-Aufrufe als Datenquellentyp verwenden

Dieses Beispiel zeigt eine benutzerdefinierte Kontrolle, die AWS-API-Aufrufe als Datenquellentyp verwendet. Audit Manager verwendet diese Kontrolle, um Beweise zu generieren, die dazu beitragen können, Ihre AWS-Umgebung an Ihre konkreten 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.
- Datenquellentyp – AWS-API-Aufrufe
- Art des Beweises – Konfigurationsdaten

Im folgenden Beispiel befindet sich diese Kontrolle in einer Audit Manager-Bewertung, die anhand eines benutzerdefinierten Frameworks erstellt wurde.



Die Bewertung zeigt den Kontrollstatus. Sie zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden und wie viele dieser Beweise in Ihrem Bewertungsbericht enthalten sind. 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 sind der Datenquellentyp. Audit Manager sucht nach dem Ergebnis eines bestimmten IAM-API-Aufrufs (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 Antworten auf den API-Aufruf einzusehen. Die Antwort auf GetAccountPasswordPolicy beschreibt die Komplexitätsanforderungen und die obligatorischen Rotationsperioden für die Benutzerkennwörter in Ihrem Konto. Sie können

diese API-Antwort als Beweis verwenden, um nachzuweisen, dass Sie über ausreichende Richtlinien zur Passwortzugriffskontrolle für diejenigen AWS-Konten verfügen, die in Ihren Bewertungsbereich 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 Featureiert.

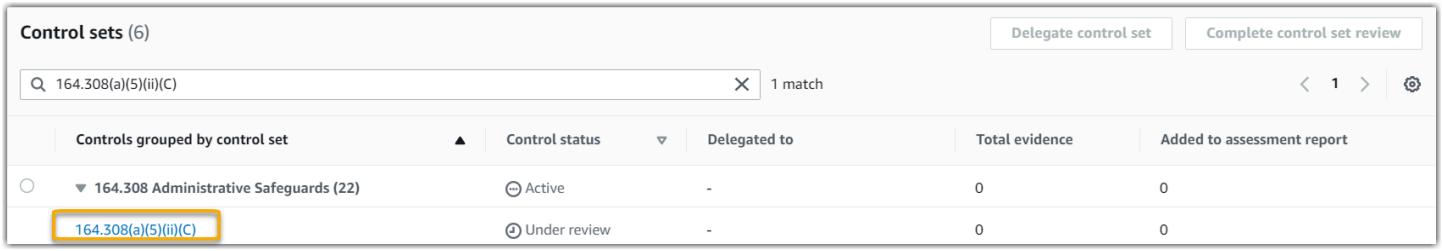
Automatisierte Kontrollen, die AWS CloudTrail als Datenquellentyp verwendet werden

Dieses Beispiel zeigt eine Kontrolle, die AWS CloudTrail als Datenquellentyp verwendet. Dies ist eine Standardkontrolle, die dem HIPAA-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)`
- Kontrollsatz – Diese Kontrolle gehört zu dem Kontrollsatz, der aufgerufen wird`164.308 Administrative Safeguards`.
- 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. Sie zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden und wie viele dieser Beweise in Ihrem Bewertungsbericht enthalten sind. 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 erfordert ein Überwachungsverfahren zur Erkennung unangemessener Anmeldungen. Ein Beispiel für eine unangemessene Anmeldung ist, wenn jemand mehrere Kombinationen von Benutzernamen oder Passwörtern eingibt, um auf ein Informationssystem zuzugreifen. Audit Manager hilft Ihnen bei der Validierung dieser Kontrolle, indem er eine Liste aller erkannten Anmeldeversuche für die Ressourcen bereitstellt, die in den Umfang Ihrer Bewertung fallen.

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 Benutzer die Ressource und CloudTrail der Datenquellentyp. Audit Manager sucht nach dem Ergebnis aller Anmeldeereignisse für die AWS-Managementkonsole, die von CloudTrail protokolliert wurden. 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 Beweise für Benutzeraktivitäten für Kontrollen, die CloudTrail als Datenquellentyp verwenden. Diese Beweise enthalten die Originaldaten, die von Ihren Benutzern erfasst wurden, sowie zusätzliche Metadaten, die angeben, welche Kontrolle die Daten unterstützen.
3. Audit Manager fügt die gespeicherten Beweise der Kontrolle mit dem Namen `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 die Beweise überprüfen, um die Anmeldeereignisse zu sehen, die von CloudTrail protokolliert wurden. Dieses Protokoll beschreibt die Anmeldeaktivitäten Ihrer Benutzer auf der Konsole und umfasst die folgenden Informationen:

- Jede erfolgreiche Anmeldung
- Jeder erfolglose Anmeldeversuch
- Überprüfung, wann die Multi-Faktor-Authentifizierung (MFA) durchgesetzt wurde
- Die IP-Adresse jedes Anmeldeereignisses

Sie können dieses Protokoll als Beweis verwenden, um nachzuweisen, dass Sie über ausreichende Überwachungsverfahren für diejenigen AWS-Konten verfügen, die im Rahmen Ihrer Bewertung behandelt werden. Wenn Sie möchten, können Sie auch zusätzliche Kommentare abgeben, indem Sie der Kontrolle einen Kommentar hinzufügen. Wenn das Protokoll beispielsweise Unstimmigkeiten aufweist, z. B. mehrere erfolglose Anmeldeversuche, können Sie einen Kommentar hinzufügen, in dem beschrieben wird, 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 Featureiert.

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.

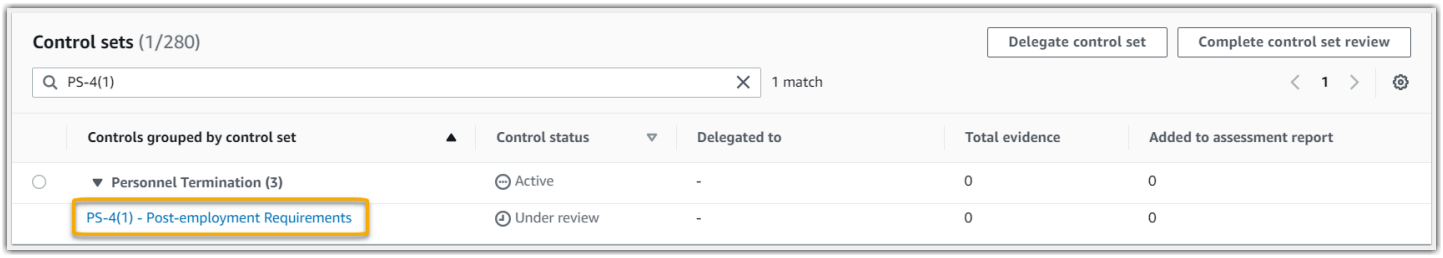
Dieses Beispiel zeigt eine manuelle Steuerung, für die Audit Manager keine automatisierten Beweise sammelt. Dies ist eine Standardkontrolle, die dem Framework NIST 800-53 (Rev. 5) entnommen wurde. Sie können Audit Manager verwenden, um Beweise hochzuladen und zu speichern, welche die Einhaltung dieser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

Beispiel für Kontrolldetails

- Name der Kontrolle – `PS-4(1) - Post-employment Requirements`

- Kontrollsatz – Diese Kontrolle gehört zum Kontrollsatz `Personnel Termination`. Dabei handelt es sich um eine Gruppe von Kontrollen, die sich auf die Informationssicherheit im Zusammenhang mit Kündigungsverfahren beziehen.
- Datenquellentyp – Manuell
- Art des Beweises – Manuell

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



Die Bewertung zeigt den Kontrollstatus. Sie zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden und wie viele dieser Beweise in Ihrem Bewertungsbericht enthalten sind. 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 zu bestätigen, dass Sie Unternehmensinformationen schützen, falls ein Mitarbeiter entlassen wird. Insbesondere können Sie nachweisen, dass Sie Personen, die gekündigt haben, regelmäßig über geltende, rechtsverbindliche Anforderungen zum Schutz von Unternehmensinformationen nach Beendigung des Arbeitsverhältnisses informieren. Darüber hinaus können Sie nachweisen, dass alle gekündigten Personen im Rahmen des Kündigungsprozesses in Ihrem Unternehmen eine Bestätigung der Anforderungen für die Beendigung des Arbeitsverhältnisses unterzeichnen.

Wie können Sie Beweise für diese Kontrolle manuell hochladen

Sie können die folgenden Schritte ausführen, um manuelle Beweise hochzuladen, die diese Kontrolle unterstützen:

1. Platzieren Sie die manuellen Beweise, die Sie hochladen möchten, in einen Amazon Simple Storage Service (S3) -Bucket und notieren Sie sich die S3-URI.

2. Öffnen Sie in Ihrer Audit Manager-Bewertung die Kontrolle, wechseln Sie zur Registerkarte „Beweisordner“ und laden Sie Beweise hoch, indem Sie die S3-URI eingeben. Anweisungen finden Sie unter Manuelles Hochladen von Beweisen in AWS Audit Manager.
3. Audit Manager erstellt einen Beweisordner, der nach dem Datum benannt ist, an dem Sie die Beweise hochladen. Anschließend fügt er die hochgeladenen Beweise der Kontrolle in Ihrer Bewertung hinzu, die `PS-4(1) - Post-employment Requirements` benannt ist.

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 rechtsverbindlichen Anforderungen nach Beendigung des Arbeitsverhältnisses hochladen, die Ihre Personalabteilung an entlassene Mitarbeiter ausstellt. Wenn Personen während des Prüfungszeitraums gekündigt wurden, können Sie auch datierte Kopien hochladen, die an diese entlassenen Personen adressiert sind.

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 kein Bestätigungsschreiben haben, das von einer Person unterzeichnet wurde, die gekündigt hat. Sie könnten die Kontrolle an einen Mitarbeiter aus der Personalabteilung delegieren, der dann eine Kopie des unterschriebenen Schreibens hochladen kann. Oder, falls während des Prüfungszeitraums keinem Mitarbeiter gekündigt wurde, können Sie einen Kommentar hinterlassen, aus dem hervorgeht, warum der Kontrolle keine unterschriebenen Schreiben beigefügt wurden.

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 Featureiert.

Kontrollen mit gemischten Datenquellentypen (automatisiert und manuell)

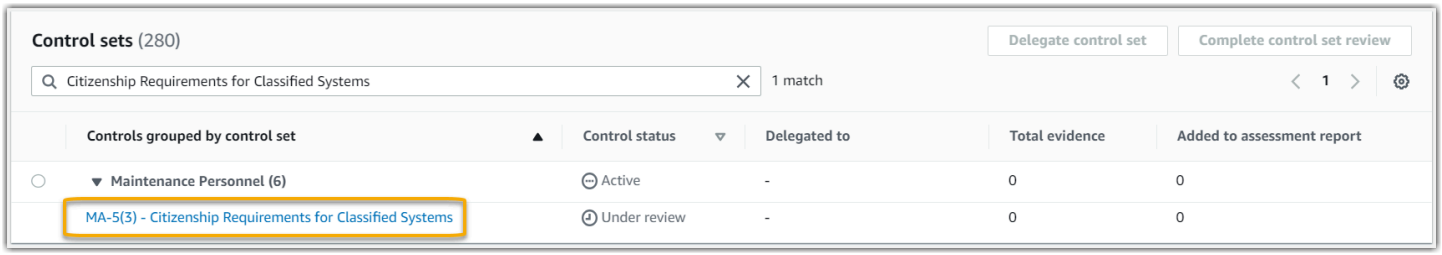
In vielen Fällen ist eine Kombination aus automatisierten und manuellen Beweisen erforderlich, um einer Kontrolle gerecht zu werden. Obwohl Audit Manager automatisierte Beweise bereitstellen kann, die für die Kontrolle relevant sind, müssen Sie diese Daten möglicherweise durch manuelle Beweise ergänzen,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

Dieses Beispiel zeigt eine Kontrolle, das eine Kombination aus manuellen Beweisen und automatisierten Beweisen verwendet, die aus AWS-API-Aufrufen stammen. 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 – `MA-5(3) - Citizenship Requirements for Classified Systems`
- Kontrollsatz – Diese Kontrolle gehört zum Kontrollsatz `Maintenance Personnel`. Dabei handelt es sich um eine Gruppe von Kontrollen, die sich auf Personen beziehen, die Hardware- oder Softwarewartungen an Organisationssystemen durchführen.
- Datenquellentyp – AWS-API-Aufrufe sowie ergänzende manuelle Beweise
- Art des Beweises – Konfigurationsdaten

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. Sie zeigt auch, wie viele Beweise bisher für diese Kontrolle gesammelt wurden und wie viele dieser Beweise in Ihrem Bewertungsbericht enthalten sind. 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 sicherzustellen, dass das Personal, das Ihre Wartungs- und Diagnosetätigkeiten durchführt, den erforderlichen Staatsbürgerschaftsstatus besitzt. Wenn Ihr System vertrauliche Informationen verarbeitet, speichert oder überträgt, müssen Sie nachweisen, dass Ihr Wartungspersonal US-Bürger ist. Audit Manager hilft Ihnen dabei, dies zu überprüfen. Zu diesem Zweck wird eine vollständige Liste aller IAM-Richtlinien und -Prinzipale zurückgegeben, die in den Rahmen Ihrer Bewertung fallen. Anschließend können Sie überprüfen

und nachweisen, dass die Benutzer der Liste die erforderlichen Staatsbürgerschaftsanforderungen erfüllen. Sie können dies tun, indem Sie zusätzliche Beweise für ihren Staatsbürgerschaftsstatus manuell hochladen.

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 IAM-Richtlinien und -Prinzipale die Ressourcen und AWS-API-Aufrufe sind die Datenquelle. Audit Manager sucht nach dem Ergebnis von vier konkreten IAM-API-Aufrufen (ListUsers/ListRoles/ListGroups/ListPolicies) und gibt eine Liste der IAM-Richtlinien und -Prinzipalen zurück, 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 Datenquellentyp 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 Kontrolle mit dem Namen `MA-5(3) - Citizenship Requirements for Classified Systems` in Ihrer Bewertung hinzu.

Wie können Sie Beweise für diese Kontrolle manuell hochladen

Sie können die folgenden Schritte ausführen, um manuelle Beweise hochzuladen, welche die automatisierten Beweise ergänzen:

1. Platzieren Sie den Staatsbürgerschaftsnachweis in einem Amazon-Simple-Storage-Service (Amazon S3)-Bucket und notieren Sie sich die S3-URI.
2. Öffnen Sie in Ihrer Audi Manager-Bewertung die Kontrolle, wechseln Sie zur Registerkarte „Beweisordner“ und laden Sie Beweise hoch. Sie tun dies, indem Sie den S3-URI eingeben. Anweisungen finden Sie unter Manuelle Beweise hinzufügen in AWS Audit Manager.
3. Audit Manager fügt die hochgeladenen Beweise der Kontrolle mit dem Namen `MA-5(3) - Citizenship Requirements for Classified Systems` 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 könnten Sie die Beweise überprüfen und eine Liste mit 20 Benutzern sehen. Wenn Sie sich nicht sicher sind, wie Sie feststellen können, welche Benutzer Wartungspersonal sind oder welche Staatsbürgerschaft diese Benutzer haben, können Sie die Kontrolle zur Überprüfung an einen Fachexperten delegieren. Der Delegierte kann die Liste des Wartungspersonals bestätigen und zusätzliche Beweise manuell hochladen, um den entsprechenden Staatsbürgerschaftsstatus nachzuweisen. Die Bestätigung der Staatsbürgerschaft aller relevanten aufgelisteten Benutzer hilft dabei, Ihre AWS-Umgebung mit den NIST-Anforderungen in Einklang zu bringen. Wenn Ihr System keine vertraulichen Informationen verarbeitet, speichert oder überträgt, können Sie alternativ einen Kommentar hinterlassen, in dem angegeben wird, warum diese Kontrolle nicht anwendbar ist.

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 Featureiert.

Integrationen mit verwandten AWS-Services

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

AWS Security Hub

AWS Security Hub überwacht Ihre Umgebung mithilfe automatisierter Sicherheitsprüfungen, die auf bewährten AWS-Verfahren und Industriestandards basieren. Wenn Security Hub aktiviert ist, kann Audit Manager Snapshots Ihrer Ressourcensicherheit erfassen, indem die Ergebnisse der Sicherheitsprüfungen direkt von Security Hub gemeldet werden. Weitere Informationen zum Security Hub finden Sie unter Was ist AWS Security Hub? im AWS Security Hub-Benutzerhandbuch.

AWS CloudTrail

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

AWS Config

AWS Config ermöglicht eine detaillierte Ansicht der Konfiguration von 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 Snapshots Ihrer Ressourcensicherheit, indem die Ergebnisse direkt von AWS Config gemeldet werden. Weitere Informationen zu AWS Config, finden Sie unter Was ist AWS Config? im AWS Config-Benutzerhandbuch.

AWS License Manager

AWS License Manager optimiert die Migration von Softwarelizenzen zur Cloud. Während der Entwicklung der Cloud-Infrastruktur auf AWS können Sie Kosten durch die Wiederverwendung vorhandener Lizenzen zur Verwendung mit Cloud-Ressourcen sparen. 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 zum License Manager finden Sie unter Was ist AWS License Manager? im AWS License Manager-Benutzerhandbuch.

AWS Control Tower

AWS Control Tower setzt präventive und erkennende Schutzmaßnahmen für die Cloud-Infrastruktur durch. Audit Manager bietet ein AWS Control Tower-Leitlinien-Framework, das Sie bei der Vorbereitung Ihrer Audits unterstützt. Dieses Framework enthält alle AWS Config-Regeln, die auf Leitlinien von AWS Control Tower basieren. Weitere Informationen zu AWS Control Tower, finden Sie 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 AWS-Infrastruktur bietet. AWS Artifact bietet Beweise dafür, dass die AWS-Cloud-Infrastruktur die Compliance-Anforderungen erfüllt. Im Gegensatz dazu hilft Ihnen AWS Audit Manager dabei, Beweise zu sammeln, zu überprüfen und zu verwalten, um nachzuweisen, dass Ihre Nutzung von AWS-Services gesetzeskonform 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 AWS Management Console herunterladen.

Eine Liste der AWS-Services, die in den Umfang bestimmter Compliance-Programme fallen, finden Sie unter AWS-Services im Umfang gemäß Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

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 Beweise 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 Featureieren

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

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 Beweisen über Ihre AWS-Nutzung. Sie können diese AWS-Beweise dann zusammen mit den anderen Beweisen, 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-Kontingente (aber nicht alle) sind unter dem AWS Audit Manager-Namespace in der Service Quotas-Konsole für Dienstkontingente aufgeführt. Informationen zum Anfordern einer Quotas-Erhöhung 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 sich an MetricStream, um Zugriff auf die MetricStream-GRC-Software zu erhalten und diese zu erwerben.

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 Beweisen aus Audit Manager in MetricStream können Sie proaktiv nicht konforme Beweise aus Ihrer AWS-Umgebung identifizieren und diese zusammen mit Beweisen aus Ihren lokalen Datenquellen oder anderen Cloud-Partnern überprüfen. 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 Integration von MetricStream und Audit Manager können Sie die folgenden API-Operationen ausführen.

Aufgabe	API-Vorgang
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
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

Verwandte MetricStream-Links

- AWS Marketplace-link
- Link zum Produkt
- Preisgestaltung

Audit Manager mit einem AWS-SDK verwenden

AWS-Software Development Kits (SDKs) sind für viele gängige Programmiersprachen erhältlich. 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 for C++	AWS SDK for C++API-Referenz für Audit Manager	Codebeispiele AWS SDK for C++	
AWS SDK for Go	AWS SDK for Go-API-Referenz für Audit Manager	Codebeispiele AWS SDK for Go	
AWS SDK for Java	AWS SDK for Java 2.x-API-Referenz für Audit Manager	Codebeispiele AWS SDK for Java	
AWS SDK for JavaScript	AWS SDK for JavaScript-API-Referenz für Audit Manager	Codebeispiele AWS SDK for JavaScript	
AWS SDK for .NET	AWS SDK for .NET-API-Referenz für Audit Manager	Codebeispiele AWS SDK for .NET	
AWS SDK for PHP	AWS SDK for PHP-API-Referenz für Audit Manager	Codebeispiele AWS SDK for PHP	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto)-API-Referenz für Audit Manager	Codebeispiele AWS SDK for Python (Boto3)	
AWS SDK for Ruby	AWS SDK for Ruby-API-Referenz für Audit Manager	Codebeispiele AWS SDK for Ruby	

Beispiele, die speziell für Audit Manager gedacht sind, finden Sie unter Codebeispiele für AWS Audit Manager.

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

Einrichten von AWS Audit Manager

Bevor Sie Audit Manager verwenden, stellen Sie sicher, dass Sie die folgenden Einrichtungsschritte abgeschlossen haben.

Themen

- Voraussetzungen: Erstellen von AWS-Konto und Berechtigungen einrichten
- Audit Manager aktivieren: Verwenden Sie die Konsole, AWS CLI, oder die API, um Audit Manager zu aktivieren
- Empfehlungen: Richten Sie empfohlene Integrationen mit anderen AWS-Services ein

Voraussetzungen

Gehen Sie wie folgt vor, um einen AWS-Konto Benutzer und einen Administrator mit Berechtigungen für das Audit Manager-Setup zu erstellen.

Schritte

- So melden Sie sich für ein AWS-Konto an
- Einen Administratorbenutzer erstellen
- Fügen Sie die Berechtigungen hinzu, die für Zugriff und Aktivierung des Audit Manager erforderlich sind

> **Important**
>
> Wenn Sie bereits über AWS und IAM verfügen, können Sie die Schritte 1 und 2 überspringen. Sie müssen jedoch Schritt 3 abschließen, damit Sie über die erforderlichen Berechtigungen zum Einrichten von Audit Manager verfügen.

So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein AWS-Konto

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

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

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

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Einen Administratorbenutzer erstellen

Wenn Sie sich für ein AWS-Konto registriert haben, sichern Sie Ihr Root-Benutzer des AWS-Kontos, aktivieren Sie AWS IAM Identity Center und erstellen Sie einen Administratorbenutzer, damit Sie nicht den Root-Benutzer für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei AWS Management Console als Kontobesitzer an, indem Sie Stammbenutzer 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-AnmeldungBenutzerhandbuch zu .
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

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

Erstellen eines Administratorbenutzers

1. Aktivieren Sie IAM Identity Center.

   Eine genaue Anleitung finden Sie unter Aktivieren von AWS IAM Identity Center im AWS IAM Identity Center-Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center administrativen Zugriff.

   Eine Anleitung zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Konfigurieren des Benutzerzugriffs mit standardmäßigem IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center-Benutzerhandbuch.

Als Administratorbenutzer anmelden

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

  Hilfe bei der Anmeldung mit einem IAM-Identity-Center-Benutzer finden Sie unter Anmelden beim AWS-Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

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 verwaltete Richtlinie AWSAuditManagerAdministratorAccess. Dies ist eine per AWS verwaltete Richtlinie, die in AWS-Konto verfügbar ist. Es ist die empfohlene Richtlinie für Audit Manager-Administratoren.

> **Tip**
>
> Aus Sicherheitsgründen empfehlen wir, dass Sie zunächst mit AWS verwalteten Richtlinien beginnen und dann zur geringsten Berechtigung übergehen. Diese AWS verwalteten Richtlinien erteilen Berechtigungen für viele häufige Anwendungsfälle. Beachten Sie, dass AWS-verwaltete Richtlinien für alle AWS-Kunden verfügbar sind. Sie bieten möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle. 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 Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer 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.

Aktivieren von AWS Audit Manager

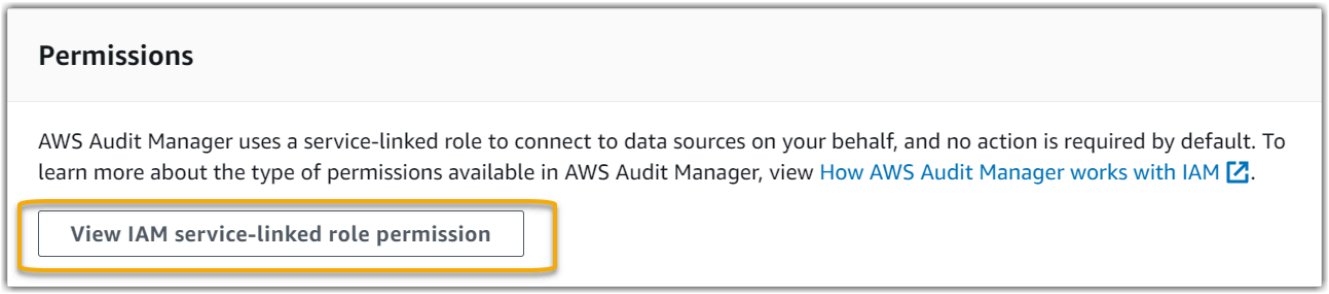
Die Aktivierung von Audit Manager erfolgt über AWS Management Console, die Audit Manager-API oder über AWS Command Line Interface (AWS CLI).

Audit Manager console

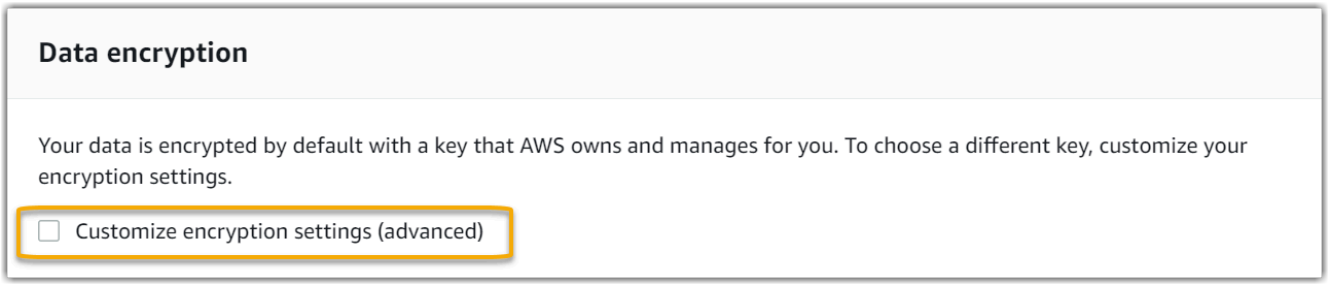
Audit Manager über die Konsole aktivieren

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Verwenden Sie zur Anmeldung die Daten Ihrer IAM-Identität.
3. Wählen Sie Set up (Festlegen)AWS Audit Manager.

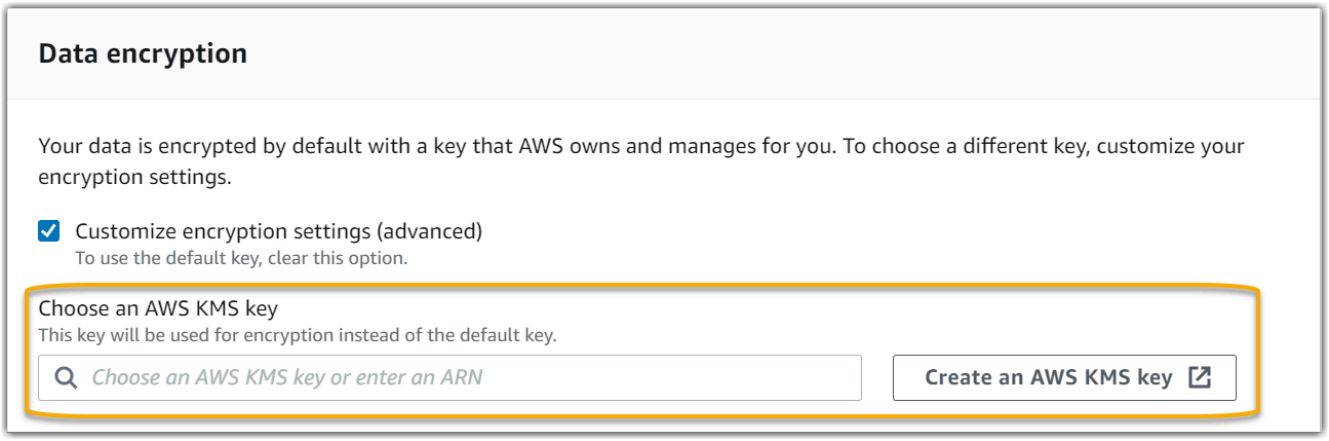
4. Unter Berechtigungen ist keine Aktion erforderlich. Grund dafür ist, dass Audit Manager eine serviceverknüpfte Rolle verwendet, um in Ihrem Namen eine Verbindung zu Datenquellen herzustellen. Sie können die serviceverknüpfte Rolle überprüfen, indem Sie die Berechtigung Serviceverknüpfte IAM-Rolle anzeigen wählen.



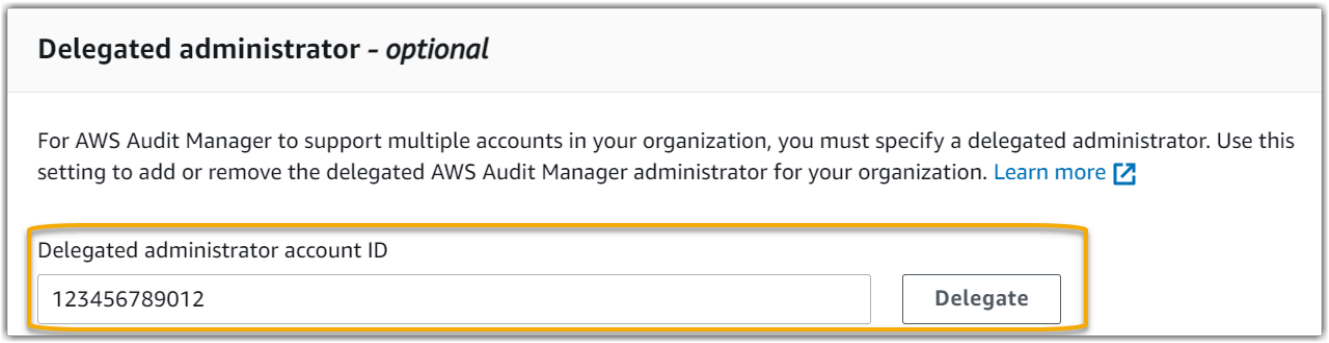
5. Unter Datenverschlüsselung ist die Standardoption, dass Audit Manager Ihre Daten erstellt, verwaltet und sicher speichert. AWS KMS key



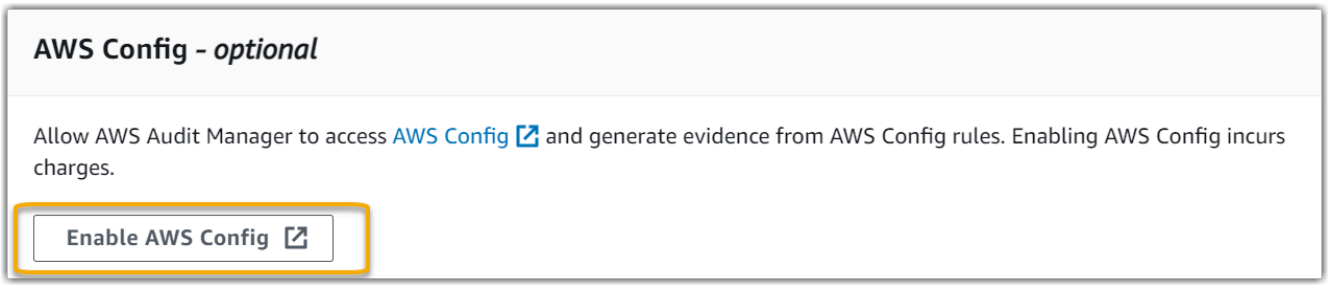
Wenn Sie Ihren eigenen, vom Kunden verwalteten Schlüssel verwenden möchten, um Daten in Audit Manager zu verschlüsseln, aktivieren Sie das Kontrollkästchen neben Verschlüsselung anpassen (erweitert). Sie können dann einen vorhandenen KMS-Schlüssel wählen oder einen neuen Schlüssel erstellen.



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 Setup von AWS Organizations für die Verwendung mit Audit Manager.

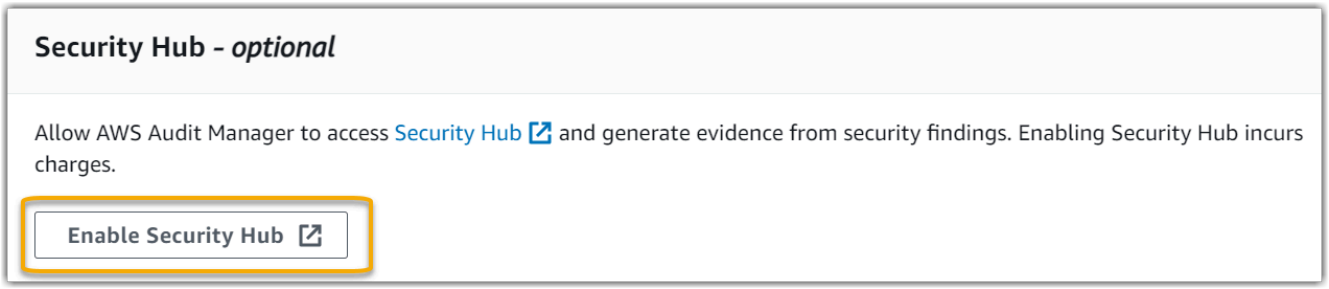


7. (Optional) Wir empfehlen Ihnen, die Option AWS Config unter AWS Config – optional zu aktivieren, um eine optimale Benutzererfahrung zu erzielen. Auf diese Weise kann Audit Manager mithilfe von AWS Config-Regeln Beweise generieren. Weitere Anweisungen und Setup-Empfehlungen finden Sie unter Aktivieren und Setup von AWS Config für die Verwendung mit Audit Manager.



8. (Optional) Unter Security Hub – optional empfehlen wir Ihnen, Security Hub zu aktivieren, um eine optimale Benutzererfahrung zu erzielen. Auf diese Weise kann Audit Manager mithilfe von Security Hub-Checks Beweise generieren. Weitere Anweisungen und Setup-

Empfehlungen finden Sie unter Aktivieren und Setup von AWS Security Hub für die Verwendung mit Audit Manager.



9. Wählen Sie Setup abschließen, um den Einrichtungsvorgang abzuschließen.

AWS CLI

Audit Manager über AWS CLI aktivieren

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 den *`Platzhaltertext`* 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 über AWS CLI und Anweisungen zur Installation der AWS CLI-Tools finden Sie in den folgenden Themen im AWS Command Line Interface Benutzerhandbuch.

- Benutzerhandbuch für AWS Command Line
- Einrichtung der AWS Command Line Interface

Audit Manager API

Zur Aktivierung von Audit Manager über Audit Manager-API

Verwenden Sie den Vorgang RegisterAccount 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 Ihres Unternehmens für Audit Manager festzulegen. Wenn Sie hier nichts angeben, wird kein delegierter Administrator registriert.

Eingabebeispiel (ersetzen Sie den *Platzhaltertext* durch Ihre eigenen Informationen):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Ausgabebeispiel

```
{
  "status": "ACTIVE"
}
```

Empfehlungen

Für eine optimale Erfahrung mit Audit Manager empfehlen wir, dass Sie die folgenden AWS-Services-Featureen berücksichtigen und aktivieren.

Themen

Empfohlene Audit Manager-Setup-Einstellungen

Nachdem Sie Audit Manager aktiviert haben, empfehlen wir, das Beweissuche-Feature 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.

Um die Beweissuche zu verwenden, müssen Sie diese Feature in Ihren Audit Manager-Einstellungen aktivieren. Detaillierte Anweisungen finden Sie unter Einstellungen für die Nachweissuche.

Empfohlene Integrationen mit anderen AWS-Services einrichten

Wir empfehlen die Aktivierung folgender AWS-Services für eine optimale Benutzererfahrung in Audit Manager:

- 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 und AWS Config – Wenn Sie diese AWS-Services aktivieren, können sie als Datenquellentyp für die Kontrollen in Ihren Audit Manager-Bewertungen verwendet werden. Audit Manager kann dann die Ergebnisse der Konformitätsprüfungen direkt von diesen Services aus melden.

Themen

Aktivieren und einrichten von AWS Config (optional)

Viele Kontrollelemente in Audit Manager nutzen AWS Config als Datenquellentyp. Um diese Kontrollen zu unterstützen, müssen Sie AWS Config für alle Konten in allen AWS-Region aktivieren, in denen Audit Manager aktiviert ist. Wenn Audit Manager versucht, Beweise für Kontrollen zu sammeln, die AWS Config als Datenquellentyp nutzen, und die entsprechenden AWS Config-Regeln nicht aktiviert sind, werden keine Beweise für diese Kontrollen gesammelt.

Audit Manager verwaltet AWS Config nicht für Sie. Sie können die folgenden Schritte ausführen, um AWS Config zu aktivieren und die Einstellungen zu konfigurieren.

Aufgaben zur Integration von AWS Config mit Audit Manager

Schritt 1: Aktivieren von AWS Config

Sie können AWS Config mithilfe der AWS Config-Konsole oder API aktivieren. 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

> **Important**
>
> Die Aktivierung von AWS Config ist eine optionale Empfehlung. Wenn Sie es jedoch AWS Config aktivieren, sind die folgenden Einstellungen erforderlich.

Stellen Sie nach der Aktivierung von AWS Config sicher, dass Sie auch AWS Config-Regeln aktivieren oder ein Konformitätspaket für den Compliance-Standard für Ihr Audit bereitstellen. 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, dass Sie die Parameter dieser Regel 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. In AWS Config hat die Regel zur Zugriffsschlüssel-Rotation 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 Aktivierung oder Konfiguration einer Regel finden Sie unter Arbeiten mit von AWS Config verwalteten Regeln.

Aktivieren und einrichten von AWS Security Hub (optional)

Viele Kontrollelemente in Audit Manager nutzen Security Hub als Datenquellentyp. Um diese Kontrollen zu unterstützen, müssen Sie Security Hub für alle Konten in allen Regionen aktivieren, in denen Audit Manager aktiviert ist. Wenn Audit Manager versucht, Beweise für Kontrollen zu sammeln, die Security Hub als Datenquellentyp nutzt, und die entsprechenden Security Hub-Standards nicht aktiviert sind, werden keine Beweise für diese Kontrollen gesammelt.

Audit Manager verwaltet Security Hub nicht für Sie. Sie können die folgenden Schritte ausführen, um Security Hub zu aktivieren und die Einstellungen zu konfigurieren.

Aufgaben zur Integration von AWS Security Hub mit Audit Manager

- Schritt 1: Aktivieren von AWS Security Hub
- Schritt 2: Konfigurieren Sie Ihre Security Hub-Einstellungen für die Verwendung mit Audit Manager

Schritt 1: Aktivieren von AWS Security Hub

Sie können Security Hub entweder über die Konsole oder die API aktivieren. Eine genaue Anleitung finden Sie unter Setup von AWS Security Hub im AWS Security Hub-Benutzerhandbuch.

Schritt 2: Konfigurieren Sie Ihre Security Hub-Einstellungen für die Verwendung mit Audit Manager

> **Important**
>
> Die Aktivierung von Securit Hub ist eine optionale Empfehlung. Wenn Sie es jedoch Security Hub aktivieren, sind die folgenden Einstellungen erforderlich.

Nachdem Sie Security Hub aktiviert haben, müssen Sie unbedingt wie folgt vorgehen:

- AWS Config aktivieren und die Ressourcenaufzeichnung konfigurieren – Security Hub verwendet servicebezogene AWS Config-Regeln, um die meisten Sicherheitsprüfungen für Kontrollelemente durchzuführen. Um diese Kontrollen zu unterstützen, muss AWS Config aktiviert und so konfiguriert sein, dass Ressourcen aufgezeichnet werden, die für die Kontrollelemente 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 – Diese Einstellung ist standardmäßig aktiviert, wenn Sie Security Hub am oder nach dem 23. Februar 2023 aktivieren.

  > **Note**
  >
  > Wenn die Option „Konsolidierte Ergebnisse“ aktiviert ist, generiert Security Hub für jede Sicherheitsprüfung ein einziges Ergebnis (auch wenn dieselbe Prüfung für mehrere Standards gilt). Jede Erkenntnis aus Security Hub 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 von Security Hub 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 als Datenquellentyp finden Sie unter AWS Security Hub -

Steuerelemente, die von unterstützt werden AWS Audit Manager. Weitere Informationen zu Preisen für Audit Manager finden Sie unter AWS Audit ManagerPreise.

Wenn Sie AWS Organizations verwenden und Security Hub soll Beweise von Ihren Mitgliedskonten sammeln, müssen Sie auch die folgenden Schritte in Security Hub ausführen.

So richten Sie die Security Hub-Einstellungen Ihres Unternehmens ein

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Security Hub-Konsole unter https://console.aws.amazon.com/securityhub/.
2. Benennen Sie mit Ihrem AWS Organizations-Management-Konto ein Konto als delegierten Administrator für Security Hub. Weitere Informationen finden Sie unter Festlegen eines Security-Hub-Administratorkontos im AWS Security Hub-Benutzerhandbuch.

   > **Note**
   >
   > Vergewissern Sie sich, dass das delegierte Administratorkonto, das Sie in Security Hub zugewiesen haben, 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-Benutzerhandbuch.
4. Aktivieren Sie AWS Config für jedes Mitgliedskonto des Unternehmens. Weitere Informationen finden Sie unter Aktivieren von Mitgliedskonten Ihres Unternehmens im AWS Security Hub-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-Benutzerhandbuch unter Aktivieren eines Sicherheitsstandards.

Aktivieren von AWS Organizations (optional)

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.

Aufgaben zur Integration von 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 Ihr AWS-Konto nicht Teil eines Unternehmens ist, können Sie ein Unternehmen gründen oder einem Unternehmen 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.

> **Warning**
>
> Nachdem Sie einen delegierten Administrator mithilfe eines Organizations-Verwaltungskontos angegeben haben, kann Ihr Verwaltungskonto keine zusätzlichen Bewertungen mehr in Audit Manager erstellen. Darüber hinaus wird die Erfassung von Beweisen für alle vorhandenen Bewertungen, die über das Verwaltungskonto erstellt wurden, beendet. Stattdessen sammelt Audit Manager Beweise und fügt sie dem delegierten Administratorkonto hinzu. Dabei handelt es sich um das Hauptkonto für die Verwaltung der Bewertungen Ihres Unternehmens.

Zum Hinzufügen oder Ändern des delegierten Administrators nach der Aktivierung von Audit Manager beachten Sie AWS Audit ManagerEinstellungen, Delegierter Administrator.

Zu berücksichtigende Punkte:

- Sie können Ihr -Verwaltungskonto nicht als delegierter Administrator in Audit Manager verwenden.
- Wenn Sie Audit Manager in mehreren AWS-Region aktivieren möchten, müssen Sie in jeder Region separat ein delegiertes Administratorkonto einrichten. Sie sollten in Ihren Audit Manager-Einstellungen für alle Regionen dasselbe delegierte Administratorkonto zuweisen.
- Wenn Sie bei der Aktivierung von Audit Manager einen vom Kunden verwalteten Schlüssel bereitgestellt haben, stellen Sie sicher, dass das delegierte Administratorkonto Zugriff auf diesen KMS-Schlüssel hat. Zur Überprüfung und Änderung Ihrer Audit Manager-Verschlüsselung beachten Sie Datenverschlüsselung.
- Lösungen für häufig auftretende Probleme mit Organizations und delegierten Administratoren in Audit Manager finden Sie unter Behebung von Problemen mit delegierten AWS Organizations-Administratoren.

Was soll ich als Nächstes tun?

Nachdem Sie Audit Manager eingerichtet haben, können Sie mit der Nutzung des Services beginnen. Sie können auch die Einstellungsseite der Konsole aufrufen, um alle Einstellungen zu aktualisieren, die Sie bei der Einrichtung von Audit Manager ausgewählt haben.

Erste Schritte mit Audit Manager

Sie können mit Audit Manager beginnen, indem Sie einem Tutorial folgen, das Sie Schritt für Schritt durch die Erstellung Ihrer ersten Bewertung führt. Weitere Informationen finden Sie unter Tutorial für Audit-Verantwortliche: Bewertung erstellen.

Aktualisieren Sie Ihre Audit Manager-Einstellungen

Sie können Ihre Einstellungen jederzeit aktualisieren. Weitere Informationen finden Sie unter AWS Audit Manager-Einstellungen.

Erste Schritte mit AWS Audit Manager

Verwenden Sie die Schritt-für-Schritt-Tutorials in diesem Abschnitt, um zu erfahren, wie Sie Aufgaben mit AWS Audit Manager durchführen.

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- oder DevOps-Teams jedoch auch die Persona eines Audit-Verantwortlichen 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 Nutzertypen und anderen Konzepten von Audit Manager finden Sie unter Audit-Verantwortliche und Delegierte im Konzepte und Terminologie zu AWS Audit Manager-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 schrittweisen Anweisungen, um Ihre erste Bewertung zu erstellen und schnell loszulegen. In diesem Tutorial erfahren Sie, wie Sie ein Standard-Framework verwenden können, um eine Bewertung zu erstellen und mit der automatisierten Nachweiserhebung zu beginnen.

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 Kontrollsätze und die zugehörigen Nachweise zu überprüfen sind, wie Sie Kommentare hinzufügen, zusätzliche Nachweise hochladen und den Status einer Kontrolle aktualisieren.

Tutorial für Audit-Verantwortliche: Eine Bewertung erstellen

Dieses Tutorial bietet eine praktische Einführung in AWS Audit Manager. In diesem Tutorial erstellen Sie eine Bewertung mit dem AWS Audit Manager Beispiel-Framework. Durch die Erstellung einer Bewertung starten Sie den laufenden Prozess der automatisierten Erfassung von Nachweisen für die Kontrollen in diesem Framework.

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

- Ein Standard-Framework auswählen, auf dessen Grundlage eine Bewertung erstellt werden soll
- Die AWS-Konten angeben, die in Ihre Bewertung aufgenommen werden sollen
- Die AWS-Services spezifizieren, die in Ihre Bewertung aufgenommen werden sollen
- Die Audit-Verantwortlichen für Ihre Bewertung spezifizieren
- Überprüfen und erstellen Ihrer Bewertung

Stellen Sie vor Beginn dieses Tutorial sicher, dass folgenden Bedingungen erfüllt sind:

- Sie haben alle Voraussetzungen erfüllt, die unter Einrichten von AWS Audit Manager beschrieben sind. Sie müssen Ihr 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 Beispiel 2: Vollständigen Administratorzugriff zulassen und Beispiel 3: Verwaltungszugriff zulassen.
- Sie sind mit der Terminologie und Featurealität von Audit Manager vertraut. Eine allgemeine Übersicht finden Sie unter Was ist AWS Audit Manager? und Konzepte und Terminologie zu AWS Audit Manager.

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

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 Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie LaunchAWS Audit Manager (Starten) aus.
3. Wählen Sie im Navigationsbereich Erste Schritte und dann Mit einem Framework beginnen.
4. Wählen Sie das gewünschte Framework aus, und wählen Sie dann Bewertung aus Framework erstellen. Hier wird das AWS Audit Manager Beispiel-Framework verwendet.

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 vorhandenen Amazon-S3-Bucket aus, in dem Sie Ihre Bewertungsberichte speichern möchten.
8. Vergewissern Sie sich unter Frameworks, dass AWS Audit ManagerBeispiel-Framework (oder das Framework Ihrer Wahl) ausgewählt ist.
9. Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um Ihrer Bewertung ein Tag zuzuordnen. Sie können für jeden Tag einen Schlüssel und einen Wert angeben. Der Tag-Schlüssel ist obligatorisch und kann als Suchkriterium verwendet werden, wenn Sie nach dieser Bewertung suchen. Weitere Informationen zu Tags in AWS Audit Manager finden Sie unter Markieren von AWS Audit Manager-Ressourcen.
10. Wählen Sie Next (Weiter).

Schritt 2: Geben Sie AWS-Konten im Geltungsbereich an

Geben Sie als Nächstes die AWS-Konten an, die Sie in den Umfang Ihrer Bewertung aufnehmen möchten.

AWS Audit Manager integriert sich mit AWS Organizations, sodass Sie eine Audit 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 von AWS Organizations (optional) auf der Seite Einrichtung dieses Handbuchs.

> **Note**
>
> Audit Manager kann im Rahmen einer Bewertung bis zu etwa 150 Konten unterstützen. Wenn Sie versuchen, mehr als 150 Konten einzubeziehen, schlägt die Erstellung der Bewertung möglicherweise fehl.

Um die Konten im Geltungsbereich anzugeben

1. Wählen Sie unter AWS-Konten die AWS-Konten aus, die Sie in den Umfang Ihrer Bewertung einbeziehen möchten.

- Wenn Sie Organizations in AWS 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 Next (Weiter).

Schritt 3: Geben Sie den AWS-Leistungsumfang an

Das Framework, das Sie zuvor ausgewählt haben, definiert die AWS-Services, die Audit Manager überwacht und für die er Nachweise sammelt.

Wenn Sie die Audit-Manager-Konsole verwenden, um eine Bewertung anhand dieses Standard-Frameworks zu erstellen, ist die Liste der Services im Geltungsbereich standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Standard-Frameworks. Wenn ein gelisteter AWS-Service nicht ausgewählt wurde, sammelt Audit Manager keine Nachweise von Ressourcen, die sich auf diesen Dienst beziehen. Dies ist auch der Fall, wenn er ausgewählt ist, Sie ihn aber in Ihrer Umgebung nicht aktiviert haben.

In diesem Schritt des Tutorials können Sie anhand der Framework-Definition überprüfen, welche AWS-Services in den Umfang der Bewertung fallen. Weitere Informationen zu Frameworks und dazu, wie Sie auf sie zugreifen und sie überprüfen können, finden Sie im Framework-Bibliothek-Abschnitt dieses Handbuchs.

Angabe des AWS Leistungsumfangs

1. Sehen Sie sich unter AWSServices die Liste der Services an, die in den Geltungsbereich dieser Bewertung fallen.
2. Wählen Sie Next (Weiter).

> **Tip**
>
> Wenn Sie die Liste der in den Geltungsbereich fallenden Services bearbeiten müssen, können Sie dazu die CreateAssessment-API verwenden, die von Audit Manager bereitgestellt wird.

Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Schritt 4: Geben Sie die Audit-Verantwortlichen an

In diesem Schritt geben Sie die Audit-Verantwortlichen für Ihre Bewertung an. Audit-Verantwortliche sind die Personen an Ihrem Arbeitsplatz – in der Regel aus GRC-, SecOps- oder DevOps-Teams –, die für die Verwaltung der Audit-Manager-Bewertung verantwortlich sind. Wir empfehlen ihnen, die AWSAuditManagerAdministratorAccess-Richtlinie zu verwenden.

Um die Audit-Verantwortlichen anzugeben

1. Wählen Sie unter Audit-Verantwortliche die Audit-Verantwortlichen für Ihre Bewertung aus. Sie können weitere Audit-Verantwortliche finden, indem Sie die Suchleiste verwenden, um nach Namen oder AWS-Konto zu suchen.
2. Wählen Sie Next (Weiter).

Schritt 5: 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 Ihre erste Bewertung und die fortlaufende Erfassung von Nachweisen zu starten.

Nachdem Sie eine Bewertung erstellt haben, wird die Nachweiserhebung 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 dem Erstellen der Bewertung verfügbar. AWS Audit Manager sammelt automatisch Nachweise aus mehreren Datenquellen, und die Häufigkeit dieser Nachweiserhebung hängt von der Art der Nachweise ab. Weitere Informationen finden Sie unter Häufigkeit der Beweissuche in diesem Handbuch.

Wie geht es weiter?

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 einer Bewertung– Führt Sie in die Bewertungsseite ein, auf der Sie sich mit den verschiedenen Komponenten Ihrer Bewertung vertraut machen können.
- 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 Dokument 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
- Framework-Bibliothek– Stellt die Framework-Bibliothek vor und erklärt, wie Sie ein benutzerdefiniertes Framework für Ihre eigenen spezifischen Compliance-Anforderungen erstellen können.
- Kontrollbibliothek– Stellt die Kontrollbibliothek vor und erklärt, wie Sie ein benutzerdefiniertes Steuerelement für die Verwendung in Ihrem benutzerdefinierten Framework erstellen.
- Konzepte und Terminologie zu AWS Audit Manager– Enthält Definitionen für die in Audit Manager verwendeten Konzepte und Terminologie.
- [Video] Erfassung von Nachweisen und Verwaltung von Prüfungsdaten mithilfe von 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.

Audit-Verantwortliche nutzen Audit Manager zur Erstellung von Bewertungen und sammeln Nachweise für die Kontrollen, die in dieser Bewertung aufgeführt sind. 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.

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

- Greifen Sie auf Benachrichtigungen zu, die Ihnen von einem Audit-Verantwortlichen gesendet wurden
- Überprüfen Sie einen Kontrollsatz und die zugehörigen Nachweise
- Laden Sie manuelle Nachweise zur Unterstützung einer Kontrolle hoch
- Fügen Sie einen Kommentar zu einer Kontrolle hinzu, die Sie überprüfen
- Aktualisieren Sie den Status einer Kontrolle
- Senden Sie den überprüften Kontrollsatz an den für die Prüfung Verantwortlichen, wenn Ihre Prüfung abgeschlossen ist

Stellen Sie vor Beginn dieses Tutorial sicher, dass folgenden Bedingungen erfüllt sind:

- Ihr AWS-Konto ist eingerichtet. Sie müssen Ihr AWS-Konto und die AWS Audit Manager-Konsole verwenden, um dieses Tutorial abzuschließen. Weitere Informationen finden Sie unter Einrichten von AWS Audit Manager.
- Sie sind mit der Terminologie und Featurealität von Audit Manager vertraut. Einen allgemeinen Überblick über Audit Manager finden Sie unter Was ist AWS Audit Manager? und Konzepte und Terminologie zu AWS Audit Manager.

Schritt 1: Greifen Sie auf Ihre Benachrichtigungen zu

Melden Sie sich zunächst bei AWS Audit Manager an, von wo Sie auf Ihre Benachrichtigungen zugreifen können, um die Kontrollsätze zu sehen, die Ihnen zur Überprüfung delegiert wurden.

So greifen Sie auf Ihre Benachrichtigungen zu

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.

2. Wählen Sie im linken Navigationsbereich Benachrichtigungen. Oder wählen Sie in der blauen Flash-Leiste oben auf der Seite Benachrichtigungen anzeigen, um die Benachrichtigungsseite zu öffnen.
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:

   - 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 Prüfungs-Anweisungen, die vom Audit-Verantwortlichen bereitgestellt werden.

> **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 in Prüfung markieren.
5. Informationen zum Kontrollelement finden Sie in den Ordnern Nachweise, Datenquellen, Kommentare und Changelog. Weitere Informationen zu den einzelnen Registerkarten und zur Interpretation der Informationen finden Sie unter Überprüfen der Kontrollen in einer Bewertung.

So überprüfen Sie die Nachweise für eine Kontrolle

1. Wählen Sie auf der Kontrollseite die Registerkarte Nachweisordner aus.
2. Navigieren Sie zur Tabelle Nachweisordner, 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 Nachweisordners, um ihn zu öffnen. Hier sehen Sie dann eine Zusammenfassung aller an diesem Datum gesammelten Nachweise. Diese Zusammenfassung enthält auch die Gesamtzahl der Konformitätswarnungen, die über AWS Security Hub, AWS Config oder beides gemeldet wurden. Anweisungen zur Interpretation der Daten auf dieser Seite finden Sie unter Nachweisordner überprüfen.
4. Navigieren Sie auf der Übersichtsseite der Nachweisordner 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. Anweisungen zur Interpretation der Daten auf der Seite finden Sie unter Nachweisordner überprüfen.

Schritt 3. Laden Sie manuelle Nachweise hoch (optional)

Auch wenn AWS Audit Manager für viele Kontrollen automatisch Nachweise erfasst, müssen Sie in manchen Fällen weitere Nachweise erbringen. In diesen Fällen können Sie manuell Nachweise hochladen, anhand derer Sie die Einhaltung dieser Kontrollen nachweisen können.

Bevor Sie manuelle Nachweise zu Ihrer Bewertung hochladen können, müssen Sie die Nachweise zunächst in einem S3-Bucket ablegen. Anweisungen finden Sie unter Erstellen eines Buckets und Hochladen eines Objekts im Amazon Simple Storage Service Benutzerhandbuch.

> **Important**
>
> Jedes AWS-Konto kann täglich nur bis zu 100 Nachweisdateien an einem Tag 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 Nachweise auf eine einzelne Kontrolle hochladen müssen, laden Sie Ihre Nachweise stapelweise über mehrere Tage hinweg hoch.

Um manuelle Nachweise zur Unterstützung einer Kontrolle hochzuladen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Sie können auf der Seite Benachrichtigungen die Liste der Kontrollsätze einsehen, die Ihnen zur Prüfung delegiert wurden. Legen Sie fest, für welchen Kontrollsatz Sie Nachweise hinzufügen möchten, und wählen Sie den Namen der zugehörigen Bewertung, um die Seite mit den Bewertungsdetails zu öffnen.
3. Wählen Sie die Registerkarte Kontrolle, scrollen Sie nach unten zu Kontrollsätze, und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.
4. Wählen Sie auf der Registerkarte Nachweisordner die Option Manuelle Nachweise hochladen.
5. Geben Sie auf der nächsten Seite die S3-URI der Nachweise ein. Sie finden den S3-URI, indem Sie in der Amazon-S3-Konsole zu dem Objekt navigieren und S3-URI kopieren auswählen.
6. Wählen Sie Hochladen, um die manuellen Nachweise hochzuladen.

> **Note**
>
> Wenn eine Kontrolle inaktiv ist, können Sie dieser Kontrolle keine manuellen Nachweise hinzufügen. Um manuelle Nachweise hinzuzufügen, müssen Sie zunächst den Status der Kontrolle entweder auf Wird geprüft oder geprüft ändern. Anweisungen zum Ändern eines Kontrollstatus finden Sie unterSchritt 5: Markieren Sie eine Kontrolle als überprüft (optional).

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 Kommentar abgeben aus, 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.

Wie geht es weiter?

Sie können sich weiter mit dem Wissen über die Konzepte und Tools vertraut machen, die in diesem Tutorial vorgestellt werden. Im Folgenden finden Sie einige empfohlene Ressourcen:

- Überprüfung einer Bewertung–AWS Audit Manager Führt Sie in die Bewertungsseite ein, auf der Sie sich mit den verschiedenen Komponenten einer Bewertung vertraut machen können.
- Überprüfung der Kontrollen in einer Bewertung und Überprüfung der Nachweise in einer Bewertung - Enthält Datendefinitionen, die Ihnen bei der Interpretation der Kontrollen und Nachweise für jede Bewertung helfen.
- Konzepte und Terminologie zu AWS Audit Manager – 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 Leistungskennzahlen (Key Performance Indicators, KPIs) anzeigen, die für Sie am relevantesten sind. Mithilfe eines Bewertungsfilters können Sie die Daten verfeinern, um sich auf die KPIs einer bestimmten Bewertung zu konzentrieren. 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:

Themen

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 Personen die Metriken und Aggregationen für alle aktiven Bewertungen in Ihrem AWS-Konto sehen können. Durch den Zugriff auf dieselben Informationen kann sich Ihr gesamtes Team auf dieselben KPIs und 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. Die Beweise für Compliance-Überprüfungen beziehen sich auf Kontrollelemente, die AWS Config oder AWS Security Hub als Datenquellentyp verwenden. Für diese Art von Beweisen meldet Audit Manager das Ergebnis einer Compliance-Überprüfung direkt über diese Services. Meldet Security Hub ein Fehlerergebnis oder AWS Config ein nicht konformes Ergebnis 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 Kontrollelement AWS Config oder AWS Security Hub als Datenquellentyp verwendet, Sie diese Services jedoch nicht aktiviert haben. Dies ist auch der Fall, wenn das Kontrollelement einen Datenquelltyp verwendet, der keine Compliance-Überprüfungen unterstützt, z. B. manuelle Beweise, AWS API-Aufrufe oderAWS CloudTrail.

Wenn ein Beweis in der Konsole den Status Nicht zutreffend für die Compliance-Überprüfung hat, wird er im Dashboard als nicht eindeutig eingestuft.

Konforme Beweise

Der Beweis gilt als konform, wenn bei einer Compliance-Überprüfung keine Probleme festgestellt wurden. Dies ist der Fall, wenn Security Hub als Ergebnis Pass 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 Featureen 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.

Audit Manager unterteilt Kontrollen in die folgenden Kontrolldomänen.

Kontrolldomänenname	Beschreibung dessen, wofür diese Kontrollen gelten
Geschäftskontinuität und Notfallplanung	Wie Sie Prozesse einrichten, die kritische Geschäftsabläufe vor den Auswirkungen größerer System- und Netzwerkstörungen schützen.
Änderungsmanagement	Wie Sie Änderungen an Ihrer Cloud-Infrastruktur testen, genehmigen, implementieren und dokumentieren.
Datensicherheit und Datenschutz	Wie Sie den Datenschutz, die Verfügbarkeit und die Integrität Ihrer Daten sichern.

Kontrolld omänenname	Beschreibung dessen, wofür diese Kontrollen gelten
Entwicklungs- und Konfigura tionsmanagement	Wie Sie Ihre Cloud-Infrastruktur im gewünschten und konsistenten Zustand halten.
Governance und Aufsicht	Wie Sie Ihre Nutzung von Cloud-Computing mit Ihren rechtlichen, regulatorischen und ethischen Verpflichtungen in Einklang bringen.
Identity and Access Management	Wie Sie sicherstellen, dass die richtigen Benutzer den entsprechenden Zugriff auf Ihre Technologieressourcen haben.
Vorfallmanagement	Wie Sie Verantwortlichkeiten und Verfahren festlegen, die eine schnelle und effektive Reaktion auf Sicherheitsvorfälle gewährleisten.
Protokollierung und Überwachung	So überprüfen Sie Benutzeraktivitäten auf Hinweise darauf, dass eine unbefugte Aktivität versucht oder ausgeführt wurde.
Netzwerkm anagement	Wie Sie Ihr Datennetzwerk mithilfe eines Netzwerkmanagementsystems verwalten und betreiben.
Personalm anagement	Wie Sie Personalsicherheitsrisiken auf organisatorischer Ebene bewerten und verwalten.
Physische Sicherheit	Wie Sie physische Sicherheitsprobleme in Ihren Einrichtungen erkennen und verhindern.
Risikomanagement	Wie Sie potenzielle Risiken und Verluste bewerten und wie Sie solche Bedrohungen reduzieren oder beseitigen.
Lieferketten-Manag ement	Wie Sie die mit IT-Produkten, Anbietern und Lieferketten verbundenen Risiken identifizieren, bewerten und mindern.
Verwaltung von Benutzergeräten	So reduzieren Sie das Risiko, dass die IT-Hardware Ihrer Mitarbeiter verloren geht, beschädigt oder kompromittiert wird.
Schwachst ellenmanagement	Wie Sie alle bekannten Schwachstellen für Ressourcen in Ihrer Cloud-Infrastruktur definieren, bewerten und beheben.

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.

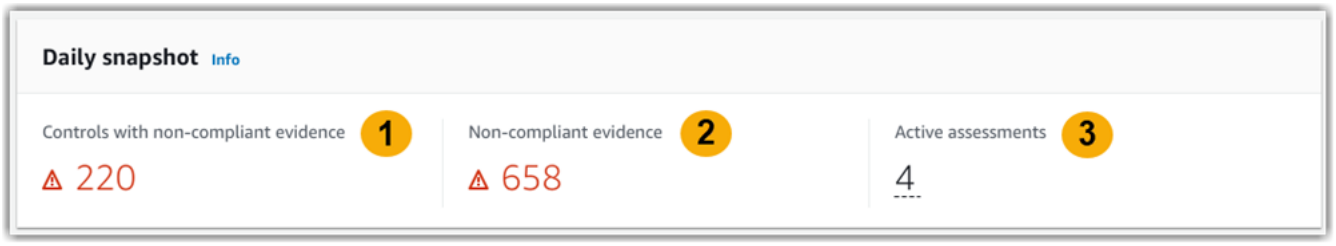
Tägliche Snapshots

Dieses Widget zeigt eine Momentaufnahme des aktuellen Compliance-Status Ihrer aktiven Bewertungen.

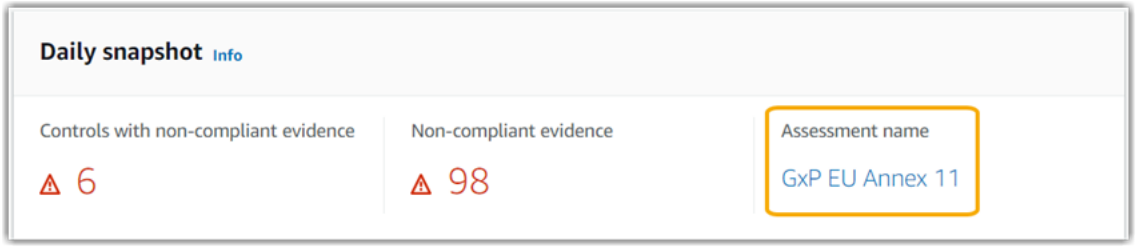
Der tägliche Snapshot spiegelt die neuesten Daten wider, die am oben im Dashboard angezeigten Datum erfasst wurden. Datum und Uhrzeit im Dashboard entsprechen der Koordinierten Weltzeit (UTC) Beachten Sie, dass es sich bei diesen Zahlen um tägliche Zählungen handelt, die auf diesem Zeitstempel basieren. 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. Nicht konforme Beweise – Die Gesamtzahl der Beweise der Compliance-Überprüfungen mit nicht konformen Ergebnissen.
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.

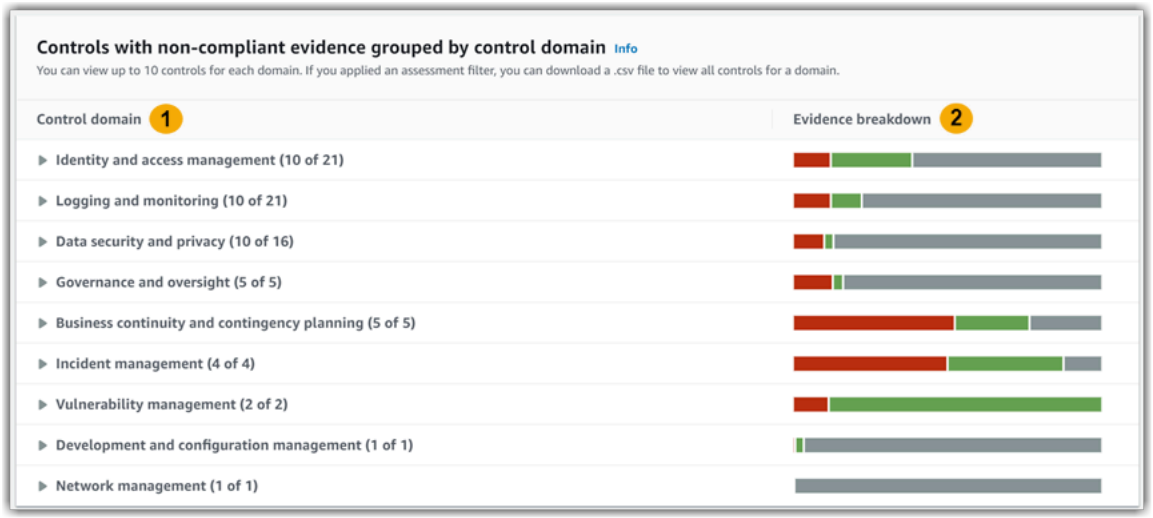


Kontrollelemente mit nicht konformen Beweisen, gruppiert nach Kontrolldomänen

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:

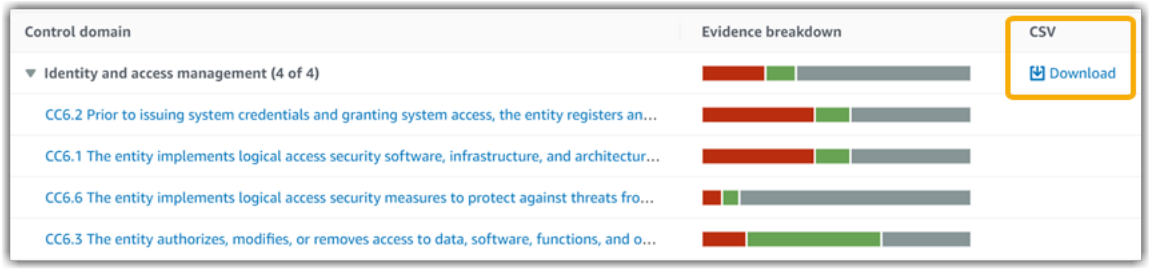
1. Kontrolldomäne – Eine Liste von control domains, die mit Ihren aktiven Bewertungen verknüpft sind.
2. Aufschlüsselung der Beweise – Ein Balkendiagramm, das eine Aufschlüsselung des Compliance-Status der Beweise zeigt.



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

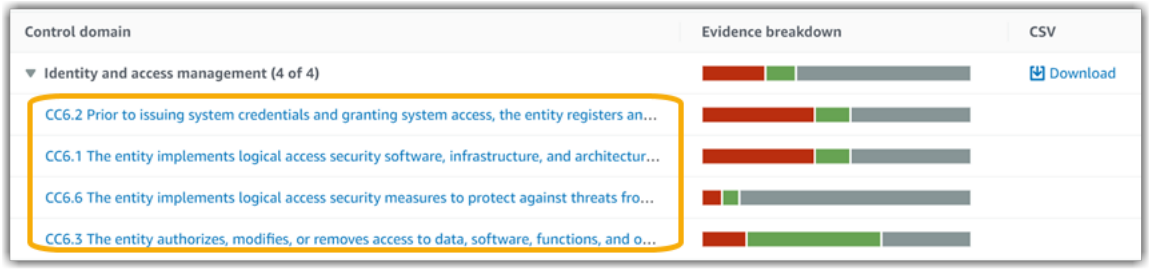
angezeigt. Darüber hinaus können Sie auch eine CSV-Datei für jede verfügbare Kontrolldomäne in der Bewertung herunterladen.



Die CSV-Datei enthält die vollständige Liste der Kontrollelemente in der Domäne, die mit nicht konformen Beweisen verknüpft sind. Im folgenden Beispiel finden Sie die .csv-Datenspalten mit fiktivenWerten.

	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 werden auf der Registerkarte Beweisordner tägliche Ordner mit Beweisen aufgeführt, die Audit Manager für dieses Kontrollelement gesammelt hat. Wählen Sie für weitere Informationen einen Ordner.
2. Beweisordner – Als Nächstes können Sie eine Ordnerübersicht und eine Liste der Beweise in diesem Ordner überprüfen. Für weitere Einzelheiten wählen Sie ein einzelnes Beweiselement aus.
3. Einzelbeweise – Schließlich können Sie die Einzelheiten zu einzelnen Beweisen untersuchen. Dazu gehören alle Anwendungs-Attribute und Ressourcendaten für die Beweise. Dies ist die detaillierteste Ebene der Beweisdaten.

Was soll ich als Nächstes tun?

Hier sind einige der nächsten Schritte, die Sie nach der Überprüfung des Dashboards ergreifen können.

- Download einer CSV-Datei – Suchen Sie nach der Bewertungs- und Kontrolldomäne, auf die Sie sich konzentrieren möchten, und laden Sie die vollständige Liste der zugehörigen Kontrollelemente herunter, deren Beweis nicht konform ist.
- 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 des Status Ihrer Bewertung – Wenn Sie die Erfassung von Beweisen für eine Bewertung beenden möchten, können Sie die Bewertung zu inaktiv ändern.

Fehlerbehebung

Antworten zu häufig gestellten Fragen und Probleme finden Sie unter Behebung von Dashboard-Problemen im Abschnitt Fehlerbehebung dieses Handbuchs.

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 die Angabe der AWS-Konten und Services, für die Sie Beweise sammeln möchten.

Sie können eine Bewertung anhand eines beliebigen Frameworks erstellen. Entweder können Sie 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 Kontrollen, die Sie entsprechend Ihren internen Auditanforderungen anpassen und gruppieren können. Weitere Informationen zu den Unterschieden zwischen standardmäßigen und benutzerdefinierten Frameworks finden Sie unter Frameworks im Abschnitt Konzepte und Terminologie dieses Handbuchs.

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 Beweise 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 Beweise AWS Audit Manager enthalten möglicherweise nicht alle Informationen über Ihre AWS-Nutzung, die für Audits erforderlich sind. AWS Audit Manager ist kein Ersatz für Rechtsbeistand oder Compliance-Experten.

Themen

- Überprüfung einer Bewertung
- Überprüfung der Kontrollen in einer Bewertung
- Überprüfung der Beweise in einer Bewertung
- Manuelle Beweise in AWS Audit Manager hinzufügen
- Generieren eines Bewertungsberichts
- Den Status einer Bewertung auf inaktiv ändern
- Löschen einer Bewertung

Erstellen einer Bewertung

Dieses Thema baut auf dem Tutorial Erste Schritte: Bewertung erstellen auf. Es enthält detaillierte Anweisungen zum Erstellen einer Bewertung anhand eines Frameworks. Gehen Sie wie folgt vor, um eine Bewertung zu erstellen und mit der laufenden Beweiserhebung zu beginnen.

Aufgaben

- Schritt 1: Bewertungsdetails festlegen
- Schritt 2: Geben Sie AWS-Konten den Umfang an
- Schritt 3: Geben Sie den Umfang der AWS-Services an
- Schritt 4: Geben Sie die Audit-Verantwortlichen an
- Schritt 5: Überprüfen und Erstellen
- Was soll ich als Nächstes tun?

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 Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Bewertungen und danach Bewertung erstellen.
   - Sie können auch im Navigationsbereich Erste Schritte und dann Bewertung erstellen auswählen.

3. Geben Sie unter Bewertungsname einen Namen für Ihre Bewertung ein.
4. (Optional) Geben Sie unter Beschreibung der Bewertung eine Beschreibung für Ihre Bewertung ein.
5. Wählen Sie unter Ziel für Bewertungsberichte einen vorhandenen Amazon-S3-Bucket aus, in dem Sie Ihre Bewertungsberichte speichern möchten.

> **Tip**
>
> Das Standardziel für Bewertungsberichte basiert auf Ihren Audit Manager-Einstellungen. Weitere Informationen finden Sie unter AWS Audit ManagerEinstellungen, Ziel des Bewertungsberichts. Wenn Sie möchten, können Sie mehrere S3-Buckets erstellen und verwenden, um Ihre Bewertungsberichte zu organisieren.

6. Wählen Sie unter Frameworks 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. Dadurch wird die Übersichtsseite des Frameworks geöffnet. Auf dieser Seite können Sie den Inhalt dieses Frameworks überprüfen. Dies beinhaltet die Kontrollen und Datenquellen des Frameworks.

7. 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. Weitere Informationen zur Verwendung von Tags in Audit Manager finden Sie unter Markieren von AWS Audit Manager-Ressourcen.
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, sollten Sie die Anforderungen für das von Ihnen gewählte Framework 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 Regel iam-password-policy 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 AWS-Konten den Umfang an

Sie können mehrere AWS-Konten angeben, die im Rahmen einer Bewertung berücksichtigt werden sollen. Audit Manager unterstützt mehrere Konten durch Integration mitAWS Organizations. Das bedeutet, dass Bewertungen von Audit Manager für mehrere Konten ausgeführt werden können, wobei die gesammelten Beweise in einem delegierten Administratorkonto zusammengefasst werden. Informationen zum Aktivieren von Organizations in Audit Manager finden Sie unter Aktivieren von AWS Organizations (optional).

> **Note**
>
> Audit Manager kann im Rahmen einer Bewertung bis zu etwa 150 Konten unterstützen. Wenn Sie versuchen, mehr als 150 Konten einzubeziehen, schlägt die Erstellung der Bewertung möglicherweise fehl.

Um den Umfang zu AWS-Konten spezifizieren

1. Wählen Sie unter AWS-Konten denjenigen AWS-Konten aus, 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, wird nur Ihr aktuelles AWS-Konto 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, können Sie 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 den Umfang der AWS-Services an

Das Framework, das Sie zuvor ausgewählt haben, definiert die AWS-Services, für die Audit Manager überwacht und Beweise sammelt. Wenn eine aufgeführter AWS-Service nicht ausgewählt ist oder ausgewählt ist, Sie ihn aber in Ihrer Umgebung nicht aktiviert haben, sammelt Audit Manager keine Beweise von Ressourcen, die sich auf diesen Service beziehen.

Sie können den Umfang der AWS-Services wie folgt angeben.

Für Bewertungen, die auf Basis von Standard-Frameworks erstellt wurden

Wenn Sie die Audit-Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt. Diese Liste kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Standard-Frameworks. Wenn das von Ihnen gewählte Standard-Framework nur manuelle Kontrollen enthält, fallen keine AWS-Services in den Umfang Ihrer Bewertung, und Sie können Ihrer Bewertung keine Services hinzufügen.

Um fortzufahren, überprüfen Sie die Liste und wählen Sie Weiter.

> **Tip**
>
> Wenn Sie die Liste der in den Umfang fallenden Services bearbeiten müssen, können Sie dazu die CreateAssessment-API verwenden, die von Audit Manager bereitgestellt wird. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Für Bewertungen, die mit benutzerdefinierten Frameworks erstellt wurden

Wenn Sie in Schritt 1 ein benutzerdefiniertes Framework ausgewählt haben, können Sie die Liste der Frameworks, die für Ihre Bewertung in Frage kommenAWS-Services, überprüfen und ändern. Wenn das von Ihnen ausgewählte benutzerdefinierte Framework nur manuelle Kontrollen enthält, werden alle AWS-Services angezeigt, aber keine ausgewählt. Sie können null oder mehr Services für den Umfang Ihrer Bewertung auswählen.

Um den Umfang zu spezifizieren AWS-Services (nur für Bewertungen, die mit benutzerdefinierten Frameworks erstellt wurden)

1. Wählen Sie unter AWS-Servicesdie Services aus, die Sie in Ihre Bewertung aufnehmen möchten. Sie können zusätzliche Services finden, indem Sie die Suchleiste verwenden, um nach Service, Kategorie oder Beschreibung zu suchen. Um einen Service hinzuzufügen, müssen Sie das Kontrollkästchen neben dem Namen des Services aktivieren. Um einen Service zu entfernen, deaktivieren Sie das Kontrollkästchen.
2. Wenn Sie mit der Auswahl fertig sind, AWS-Serviceswählen Sie Weiter.

Schritt 4: Geben Sie die Audit-Verantwortlichen an

In diesem Schritt geben Sie die Audit-Verantwortlichen für Ihre Bewertung an. Audit-Verantwortliche sind die Personen an Ihrem Arbeitsplatz – in der Regel aus GRC-, SecOps- oder DevOps-Teams –, die für die Verwaltung der Audit-Manager-Bewertung verantwortlich sind. Wir empfehlen ihnen, die AWSAuditManagerAdministratorAccess-Richtlinie zu verwenden.

Um die Audit-Verantwortlichen anzugeben

1. Sehen Sie sich unter Audit-Verantwortliche die aktuelle Liste der Audit-Verantwortlichen an. In der Spalte Audit-Verantwortliche werden die Benutzer-IDs und Rollen angezeigt. In der AWS-

KontoSpalte werden die Personen angezeigt, AWS-Konto die diesem Audit-Verantwortlichen zugeordnet sind.

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.

Schritt 5: 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 Beweisen für eine bestimmte Kontrolle beenden, indem Sie den Kontrollstatus auf inaktiv ändern.

> **Note**
>
> Automatisierte Beweise 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.

Was soll ich als Nächstes tun?

Nachdem Sie Ihre Bewertung erstellt haben, erfahren Sie mehr über Folgendes:

- Auf eine Bewertung zugreifen
- Überprüfung einer Bewertung
- Bearbeiten einer Bewertung
- Überprüfung der Kontrollen in einer Bewertung
- Überprüfung der Beweise in einer Bewertung
- Manuelle Beweise für eine Bewertung hochladen

- Delegierungen in AWS Audit Manager
- Generieren eines Bewertungsberichts
- Den Status einer Bewertung ändern
- Löschen einer Bewertung
- Fehlersuche bei der Bewertung und Beweiserhebung

Auf Ihre Bewertungen zugreifen in AWS Audit Manager

Sie können alle Ihre Bewertungen auf der Seite Bewertungen in der Audit Manager-Konsole einsehen. Von hier aus können Sie auch eine Bewertung bearbeiten, eine Bewertung löschen oder eine Bewertung erstellen.

Sie können Ihre Bewertungen auch mit der Audit Manager-API oder der AWS Command Line Interface (AWS CLI) anzeigen.

Audit Manager console

Um Ihre Bewertungen einzusehen (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich Bewertungen aus, um eine Liste Ihrer aktiven und vergangenen Bewertungen anzuzeigen. Sie können auch die Suchleiste verwenden, um nach einer Bewertung zu suchen.
3. Wählen Sie einen beliebigen Bewertungsnamen, um eine Übersichtsseite zu öffnen, auf der Sie die Details zu dieser Bewertung einsehen können.

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 einzusehen (API)

Verwenden Sie den Vorgang ListAssessments, 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 ManagerAPI-Referenz zu erfahren. Dies beinhaltet Informationen zur Verwendung des `ListAssessments` Vorgangs und der Parameter in einem der sprachspezifischen AWS-SDKs.

Bearbeiten einer Bewertung

Sie können Ihre aktiven Bewertungen in Audit Manager bearbeiten, um Informationen wie Beschreibung, Umfang, Audit-Verantwortliche und das Ziel des Bewertungsberichts zu ändern.

Aufgaben

- Schritt 1: Bewertungsdetails bearbeiten
- Schritt 2: Den Umfang der AWS-Konten bearbeiten
- Schritt 3: Den Umfang der AWS-Services bearbeiten
- Schritt 4: Bearbeiten der Audit-Verantwortlichen
- Schritt 5: 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 Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Klicken Sie im Navigationsbereich auf Bewertungen, um Ihre aktuelle Liste der Bewertungen anzuzeigen.
3. Wählen Sie eine Bewertung aus und klicken Sie auf Bearbeiten.

- Alternativ können Sie die Bewertung öffnen und dann oben rechts Bearbeiten wählen.

4. Bearbeiten Sie unter Bewertungsdetails bearbeiten den Namen, die Beschreibung und das Ziel des Bewertungsberichts.
5. Wählen Sie Weiter.

> **Tip**
>
> Um die Tags für eine Bewertung zu bearbeiten, öffnen Sie die Bewertung und wählen Sie Registerkarte „Tags“. Dort können Sie die mit der Bewertung verknüpften Tags anzeigen und bearbeiten.

Schritt 2: Den Umfang der AWS-Konten bearbeiten

In diesem Schritt können Sie die Liste der Konten ändern, die im Umfang Ihrer Bewertung enthalten sind.

Audit Manager unterstützt mehrere Konten durch Integration mitAWS Organizations. Das bedeutet, dass Audit Manager-Bewertungen für mehrere Konten ausgeführt werden können, wobei die gesammelten Beweise in einem delegierten Administratorkonto konsolidiert werden. Informationen zum Hinzufügen oder Ändern des delegierten Administrators für Audit Manager finden Sie unter AWS Audit ManagerEinstellungen, Delegierter Administrator.

> **Note**
>
> Audit Manager kann im Rahmen einer Bewertung bis zu etwa 150 Konten unterstützen. Wenn Sie versuchen, mehr als 150 Konten einzubeziehen, schlägt die Erstellung der Bewertung möglicherweise fehl.

Um den Umfang AWS-Konten zu bearbeiten

1. Wählen Sie weitere AWS-Konten unter im Umfang befindliche AWS-Konten bearbeiten aus. Sie können auch Konten entfernen, indem Sie sie aus der Liste löschen.
2. Wählen Sie Weiter aus.

Schritt 3: Den Umfang der AWS-Services bearbeiten

In diesem Schritt wird festgelegt, für welche AWS-Services Audit Manager Beweise überwacht und sammelt. Wenn eine aufgeführter AWS-Service nicht ausgewählt ist oder ausgewählt ist, Sie ihn aber in Ihrer Umgebung nicht aktiviert haben, sammelt Audit Manager keine Beweise von Ressourcen, die sich auf diesen Service beziehen.

Sie können die im Umfang befindlichen AWS-Services wie folgt überprüfen und bearbeiten.

Für Bewertungen, die auf Basis von Standard-Frameworks erstellt wurden

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung zu bearbeiten, die aus einem Standard-Framework erstellt wurde, können Sie die Liste der im Umfang enthaltenen AWS-Services überprüfen, diese Liste jedoch nicht bearbeiten. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie gemäß dem Design des Standard-Frameworks zuordnet und auswählt. Wenn die Bewertung mithilfe eines Frameworks erstellt wurde, das nur manuelle Kontrollen enthält, ist kein AWS-Services für Ihre Bewertung im Umfang enthalten, und Sie können keine Services hinzufügen.

Um fortzufahren, überprüfen Sie die Liste und wählen Sie Weiter.

> **Tip**
>
> Wenn Sie die Liste der Services, die in den Umfang einer bestehenden Bewertung fallen, können Sie dies mithilfe der UpdateAssessment-API tun, die von Audit Manager bereitgestellt wird.

Für Bewertungen, die mit benutzerdefinierten Frameworks erstellt wurden

Wenn Sie die Bewertung anhand eines benutzerdefinierten Frameworks erstellt haben, können Sie die AWS-Services bearbeiten, die im Umfang enthalten sind. Sie können null oder mehr Services für den Umfang Ihrer Bewertung auswählen.

Um den Umfang zu bearbeiten AWS-Services (nur für Bewertungen, die mit benutzerdefinierten Frameworks erstellt wurden)

1. Wählen Sie AWS-Services unter Umfang bearbeiten ggf. zusätzliche AWS-Services aus. Sie können auch Services entfernen, indem Sie sie aus der Liste löschen.
2. Wählen Sie Weiter aus.

Schritt 4: Bearbeiten der Audit-Verantwortlichen

Sie können auch die Audit-Verantwortlichen für Ihre Bewertung ändern. Audit-Verantwortliche sind die Personen an Ihrem Arbeitsplatz – in der Regel aus GRC-, SecOps- oder DevOps-Teams –, die für die Verwaltung der Audit-Manager-Bewertung verantwortlich sind. Zu ihren Aufgaben gehören die Delegierung von Kontrollsätzen für die Prüfung und die Erstellung von Bewertungsberichten. Wir empfehlen Ihnen, die Richtlinie AWSAuditManagerAdministratorAccess zu verwenden.

Um die Audit-Verantwortlichen zu bearbeiten

1. Wählen Sie neue Audit-Verantwortliche aus, die Sie der Bewertung hinzufügen möchten. Um Audit-Verantwortliche zu entfernen, löschen Sie sie aus der Liste.
2. Wählen Sie Weiter aus.

Schritt 5: 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.

> **Note**
>
> Nachdem Sie Ihre Änderungen abgeschlossen haben, werden die Änderungen an der Bewertung am darauffolgenden Tag um 00:00 Uhr UTC wirksam.

Überprüfung einer Bewertung

Nachdem Sie Bewertungen in Audit Manager erstellt haben, können Sie Ihre Bewertungen jederzeit öffnen und überprüfen.

Um eine Bewertung zu öffnen und zu überprüfen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.

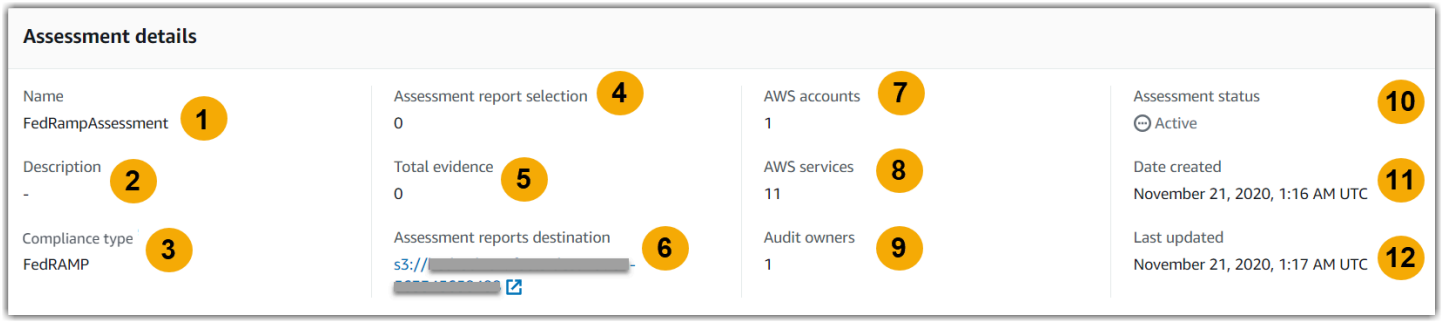
Wenn Sie eine Bewertung öffnen, wird eine Übersichtsseite mit mehreren Abschnitten angezeigt. Die Abschnitte dieser Seite und ihr Inhalt werden wie folgt beschrieben.

Abschnitte der Bewertungsseite

- Einzelheiten der Bewertung
- Registerkarte „Kontrollen“
- Registerkarte „Auswahl für den Bewertungsbericht“
- AWS-Konten-Registerkarte
- AWS-Services-Registerkarte
- Registerkarte Audit-Verantwortliche
- Registerkarte „Tags“
- Registerkarte „Änderungsprotokoll“

Einzelheiten der Bewertung

Der Abschnitt mit den Bewertungsdetails bietet einen Überblick über die Bewertung.



Dazu gehören folgende Informationen:

1. Name – Der Name, den Sie für die Bewertung angegeben haben.
2. Beschreibung – Die optionale Beschreibung, die Sie für die Bewertung angegeben haben.
3. Konformitätstyp – Der Konformitätsstandard oder die Konformitätsvorschrift, die durch die Bewertung unterstützt wird.
4. Auswahl des Bewertungsberichts – Die Anzahl der Beweise, die Sie in den Bewertungsbericht aufnehmen möchten.
5. Gesamtzahl der Beweise – Die Gesamtzahl der Beweise, die für diese Bewertung gesammelt wurden.

6. Ziel der Bewertungsberichte – Der Amazon S3-Bucket, in dem Audit Manager den Bewertungsbericht speichert.
7. AWS-Konten– Die Anzahl von AWS-Konten, die Umfang dieser Bewertung sind.
8. AWS-Services– Die Anzahl AWS-Services von, die Umfang dieser Bewertung sind.
9. Audit-Verantwortliche – Die Anzahl der Audit-Verantwortlichen für diese Bewertung.
10. Bewertungsstatus – Der Status der Bewertung.
    - Aktiv – Zeigt an, dass bei der Bewertung derzeit Beweise gesammelt werden. Neu erstellte Bewertungen haben diesen Status.
    - Inaktiv – Zeigt an, dass bei der Bewertung keine Beweise mehr gesammelt werden. Weitere Informationen zu inaktiven Bewertungen finden Sie unter Den Status einer Bewertung auf inaktiv ändern.
11. Erstellungsdatum – Das Datum, an dem die Bewertung erstellt wurde.
12. Letzte Aktualisierung – Das Datum, an dem diese Bewertung zuletzt bearbeitet wurde.

Registerkarte „Kontrollen“

Auf der Registerkarte Kontrollen wird eine Zusammenfassung der Kontrollen in der Bewertung zusammen mit einer vollständigen Liste dieser Kontrollen angezeigt. Jede Bewertung kann mehrere Kontrollsätze enthalten, und jeder Kontrollsatz enthält mehrere Kontrollen. Kontrollen und Kontrollsätze sind so angeordnet, dass sie dem Layout entsprechen, das in der zugehörigen Konformitätsnorm oder -verordnung definiert ist.

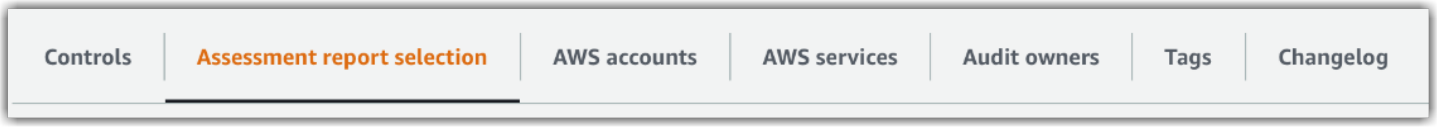
Unter Übersicht über den Kontrollstatus finden Sie eine Zusammenfassung der Kontrollen für diese Bewertung. Die Übersichtstabelle enthält die folgenden Informationen:

- Kontrollen insgesamt – Die Gesamtzahl der Kontrollen in dieser Bewertung.
- Überprüft – Die Anzahl der Kontrollen, die von einem Audit-Verantwortlichen oder Delegierten überprüft wurden.
- Wird überprüft – Die Anzahl der Kontrollen, die derzeit überprüft werden.
- Inaktiv – Die Anzahl der Kontrollen, die nicht mehr aktiv Beweise sammeln.

In der Tabelle Kontrollsätze wird eine Liste von Kontrollen angezeigt, die nach Kontrollsätzen gruppiert ist. Sie können die Kontrollen in jedem Kontrollsatz erweitern oder reduzieren. Sie können auch nach dem Namen der Kontrolle suchen, wenn Sie nach einer bestimmten Kontrolle suchen möchten. Die folgenden Datenspalten werden in der Tabelle Kontrollen gruppiert nach Kontrollsätzen angezeigt:

- Nach Kontrollsätzen gruppierte Kontrollen – Der Name des Kontrollsatzes.
- Kontrollstatus – 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 Beweise hochladen. Dies ist die Standardeinstellung.
  - Überprüft bedeutet, dass die Beweise für diese Kontrolle überprüft wurden. Es werden jedoch immer noch Beweise gesammelt, und Sie können manuelle Beweise hochladen.
  - Inaktiv bedeutet, dass die automatische Beweiserhebung für diese Kontrolle gestoppt wurde. Sie können keine manuellen Beweise mehr hochladen.
- Delegiert an – Der Prüfer dieser Kontrolle, falls es einem Delegierten zur Überprüfung zugewiesen wurde.
- Beweise insgesamt – Die Anzahl der Beweise, die für diese Kontrolle gesammelt wurden.

Registerkarte „Auswahl für den Bewertungsbericht“



Auf dieser Registerkarte wird die Liste der Beweise, die in den Bewertungsbericht aufgenommen werden sollen, gruppiert nach Beweisordnern angezeigt. Diese Beweisordner sind auf der Grundlage des Erstellungsdatums organisiert und benannt. Sie können diese Ordner durchsuchen und auswählen, welche Beweise Sie in Ihren Bewertungsbericht aufnehmen möchten. Sie können auch die Suchleiste verwenden, um nach dem Namen des Beweisordners oder der Kontrolle zu suchen. Die Gesamtzahl der Beweise, die dem Bewertungsbericht hinzugefügt wurden, ist im Abschnitt Bewertungsdetails oben auf der Seite zusammengefasst.

Die Tabelle Auswahl für den Bewertungsbericht enthält eine Liste von Beweisordnern mit den folgenden Daten:

- Beweisordner – Der Name des Beweisordners. Der Ordnername basiert auf dem Datum, an dem die Beweise gesammelt wurden.
- Ausgewählte Beweise – Die Anzahl der Beweise innerhalb des Ordners, die im Bewertungsbericht enthalten sind.
- Kontrollname – Der Name der Kontrolle, die diesem Beweisordner zugeordnet ist.

Informationen zum Hinzufügen von Beweisen zu einem Bewertungsbericht finden Sie unter Generieren eines Bewertungsberichts.

AWS-Konten-Registerkarte

Diese Registerkarte zeigt eine Liste von AWS-Konten, die im Geltungsbereich der Bewertung enthalten sind. Die Gesamtzahl der Konten ist im Abschnitt mit den Bewertungsdetails oben auf der Seite zusammengefasst.

Die AWS-Konten-Tabelle enthält eine Liste von Konten mit den folgenden Daten:

- Konto-ID – Die ID des AWS-Konto.
- Konto-Name – Der Benutzername des AWS-Konto.
- E-Mail – Geben Sie die E-Mail-Adresse an, die dem AWS-Konto zugeordnet ist.

AWS-Services-Registerkarte

Diese Registerkarte zeigt eine Liste von AWS-Services, die im Geltungsbereich der Bewertung enthalten sind. Mit anderen Worten, dies sind diejenigen AWS-Services, über die Ihre Bewertung Beweise sammelt.

Die Gesamtzahl der Services ist im Abschnitt mit den Bewertungsdetails oben auf der Seite zusammengefasst.

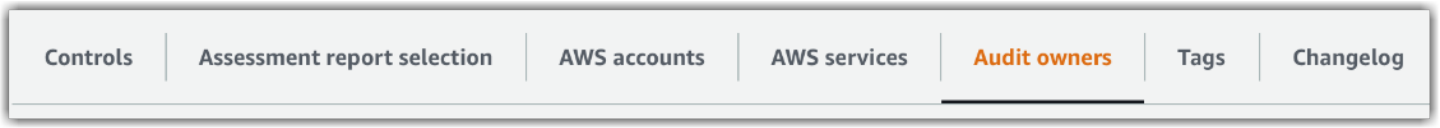
Die AWS-Services-Tabelle enthält eine Liste von Services mit den folgenden Daten:

- AWS-Service – Der Name des AWS-Service.
- Kategorie – Die Servicekategorie, z. B. Datenverarbeitung oder Datenbank.

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. Welche Beweise genau gesammelt werden, hängt von der Datenquelle einer Kontrolle ab. Wenn der Datenquellentyp beispielsweise AWS Config ist 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 Beweis. Weitere Informationen finden Sie unter Was ist der Unterschied zwischen einem Service im Umfang und einem Datenquellentyp? in dieser Anleitung.

> **Note**
>
> 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 Standard-Framework nur manuelle Kontrollen enthält, sind keine AWS-Services im Umfang enthalten. Wenn Sie die Liste der Services im Umfang bearbeiten müssen, können Sie die UpdateAssessment-API verwenden.

Registerkarte Audit-Verantwortliche

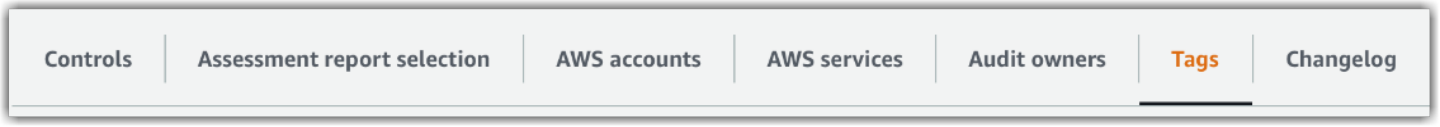


Auf dieser Registerkarte werden die Audit-Verantwortlichen für die Bewertung angezeigt. Die Gesamtzahl der Audit-Verantwortlichen ist ebenfalls im Abschnitt mit den Bewertungsdetails oben auf der Seite zusammengefasst.

Die Tabelle mit den Audit-Verantwortlichen enthält eine Liste von Konten mit den folgenden Daten:

- Audit-Verantwortliche – Der Namen des Audit-Verantwortlichen.
- AWS-Konto – Die E-Mail-Adresse, die dem Audit-Verantwortlichen zugeordnet ist.

Registerkarte „Tags“



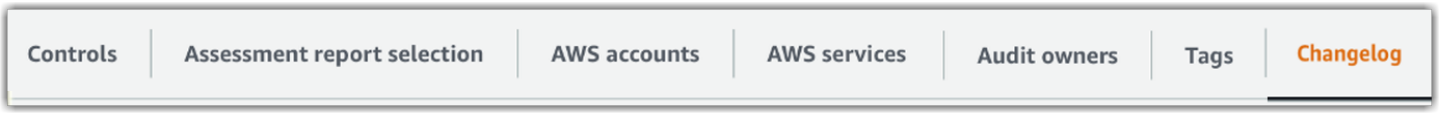
Auf dieser Registerkarte wird die Liste der vom Framework übernommenen Tags angezeigt, die zur Erstellung dieser Bewertung verwendet wurden. Die Gesamtzahl der Tags ist oben auf der Seite unter Bewertungsdetails zusammengefasst.

Die Tabelle mit den Tags enthält eine Liste von Stichwörtern mit den folgenden Daten:

- Schlüssel – Der Schlüssel des Tags, z. B. ein Konformitätsstandard, eine Vorschrift oder eine Kategorie.
- Wert – Der Wert des Tags.

Weitere Informationen zur Verwendung von Tags in Audit Manager finden Sie unter Markieren von AWS Audit Manager-Ressourcen.

Registerkarte „Änderungsprotokoll“



Auf dieser Registerkarte wird eine Liste der Benutzeraktivitäten im Zusammenhang mit der Bewertung angezeigt.

Die Tabelle Änderungsprotokoll enthält eine Liste von Konten mit den folgenden Daten:

- Datum – Das Datum der Aktivität.
- Benutzer – Der Benutzer, der die Aktion ausgeführt hat.
- 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.

Überprüfung der Kontrollen in einer Bewertung

Die Kontrollen in Audit Manager helfen Ihnen dabei, bei Ihren Audits sowohl allgemeine als auch einzigartige Compliance-Standards und -Vorschriften einzuhalten. Sie können die Kontrollen in Ihrer Audit Manager-Bewertung jederzeit öffnen und überprüfen.

Um eine Seite mit einer Kontrollübersicht zu öffnen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Bewertungen 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.

Wenn Sie eine Kontrolle öffnen, wird eine Übersichtsseite mit mehreren Abschnitten angezeigt. Die Abschnitte dieser Seite und ihr Inhalt werden in den folgenden Abschnitten beschrieben.

Abschnitte der Kontrollseite

- Kontrolldetails
- Status der Kontrolle aktualisieren
- Registerkarte „Beweisordner“
- Registerkarte „Datenquelle“
- Registerkarte „Kommentare“
- Registerkarte „Änderungsprotokoll“

Kontrolldetails

Der Abschnitt Kontrolldetails bietet einen Überblick über die Kontrolle.

Dazu gehören folgende Informationen:

1. Name des Kontrolle – Der Name, der dieser Kontrolle gegeben wurde.
2. Beschreibung der Kontrolle – Die Beschreibung, die für diese Kontrolle bereitgestellt wurde.
3. Testinformationen – Die empfohlenen Testverfahren für diese Kontrolle.

4. Aktionsplan – Die empfohlenen Maßnahmen, die durchgeführt werden müssen, wenn die Kontrolle nicht erfüllt wird.

Status der Kontrolle aktualisieren

Im Bereich Status der Kontrolle aktualisieren auf der Seite können Sie den Status der Bewertungskontrolle überprüfen und aktualisieren.

Die folgenden Statuswerte gibt es:

- Wird geprüft – Zeigt an, dass diese Kontrolle noch nicht überprüft wurde. Für diese Kontrolle werden noch Beweise gesammelt, und Sie können manuelle Beweise hochladen. Dies ist die Standardeinstellung.
- Überprüft – Zeigt an, dass die Beweise für diese Kontrolle überprüft wurden. Beweise werden noch gesammelt, und Sie können manuelle Beweise hochladen.
- Inaktiv – bedeutet, dass die automatische Beweiserhebung für diese Kontrolle gestoppt wurde. Sie können keine manuellen Beweise mehr hochladen.

> **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.

Registerkarte „Beweisordner“

Auf der Registerkarte Beweisordner sind die Beweise aufgeführt, die für diese Kontrolle automatisch gesammelt wurden. Sie wird täglich in Ordnern organisiert.

Die Tabelle mit den Beweisordnern enthält eine Liste von Ordnern mit den folgenden Daten:

- Beweisordner – Der Name des Beweisordners. Der Name basiert auf dem Datum, an dem die Beweise gesammelt oder manuell hinzugefügt wurden.
- Konformitätsprüfung – Die Anzahl der Probleme, die im Beweisordner gefunden wurden. Diese Zahl steht für die Gesamtzahl der Sicherheitsprobleme, die direkt von AWS Security Hub, AWS Config oder beiden gemeldet wurden. Wenn Sie die Option Nicht zutreffend sehen, bedeutet dies,

dass entweder AWS Security Hub oder AWS Config nicht aktiviert ist, oder dass die Beweise von einem anderen Datenquellentyp stammen.

- Beweise insgesamt – Die Gesamtzahl der Beweiselemente im Ordner.
- Auswahl des Bewertungsberichts – Die Anzahl der Beweiselemente innerhalb des Ordners, die im Bewertungsbericht enthalten sind.

Auf der Registerkarte Beweisordner können Sie die folgenden Aktionen ausführen:

- Einzelne Beweise überprüfen – Wählen Sie einen Beweisordner aus, um ihn zu öffnen. Auf der Übersichtsseite des Beweisordners können Sie dann die einzelnen Beweise auswählen, die Sie überprüfen möchten.
- Manuelle Beweise hinzufügen – Weitere Informationen finden Sie unter Manuelle Beweise in AWS Audit Manager hinzufügen .
- Beweise zu einem Bewertungsbericht hinzufügen – Weitere Informationen finden Sie unter Generieren eines Bewertungsberichts.

Registerkarte „Datenquelle“

Diese Registerkarte zeigt Informationen über die Datenquellen für die Kontrolle an. Dazu gehören folgende Informationen:

- Name der Datenquelle – Dies gilt nur für benutzerdefinierte Kontrollen. Er bezieht sich auf den beschreibenden Namen, den Sie jeder Datenquelle gegeben haben. Sie können diesen Namen verwenden, um zwischen mehreren Datenquellen zu unterscheiden, die unter denselben Datenquellentyp fallen.
- Datenquellentyp – Dieser gibt an, woher die Beweisdaten stammen.
  - Wenn Audit Manager die Beweise sammelt, kann es sich bei der Datenquelle um einen von vier Typen handeln: AWS Security Hub, AWS Config, AWS CloudTrail, oder AWSAPI-Aufrufe.
  - Wenn Sie Ihre eigenen Beweise hochladen, ist der Datenquellentyp Manuell. Eine Beschreibung gibt an, ob es sich bei den erforderlichen manuellen Beweisen um einen Datei-Upload oder eine Textantwort handelt.
- Zuordnung – Dies ist das Zuordnungsattribut, das verwendet wird, um Daten aus einer automatisierten Datenquelle zu identifizieren und abzurufen.

  - Wenn der Datenquellentyp AWS Config ist, ist die Zuordnung der Name einer bestimmten AWS Config Regel (z. B. `EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager verwendet diese Zuordnung, um das Ergebnis der Regelprüfung direkt von AWS Config zu melden.
  - Wenn der Datenquellentyp AWS Security Hub ist, ist die Zuordnung der Name einer bestimmten Security Hub-Kontrolle (z. B. `1.1 – Avoid the use of the "root" account`). Audit Manager verwendet diese Zuordnung, um das Ergebnis dieser Sicherheitsprüfung direkt vom Security Hub aus zu melden.
  - Handelt es sich bei dem Datenquellentyp um AWS-API-Aufrufe, entspricht die Zuordnung dem Namen eines bestimmten API-Aufrufs (z. B. `ec2_DescribeSecurityGroups`). Audit Manager verwendet diese Zuordnung, um die API-Antwort zu sammeln.
  - Wenn der Datenquellentyp AWS CloudTrail ist, ist die Zuordnung der Name eines bestimmten CloudTrail-Ereignisses (z. B. `CreateAccessKey`). Audit Manager verwendet diese Zuordnung, um die entsprechenden Benutzeraktivitäten aus Ihren CloudTrail-Protokollen zu erfassen.
- Häufigkeit – Die Häufigkeit der Erfassung von Beweisen aus dieser Datenquelle. Die Häufigkeit variiert je nach Datenquelle. Weitere Informationen finden Sie, wenn Sie den Wert in der Spalte auswählen oder unter Häufigkeit der Beweissuche.

Registerkarte „Kommentare“

Auf der Registerkarte Kommentare können Sie einen Kommentar zu der Kontrolle und ihren Beweisen hinzufügen. Außerdem wird eine Liste früherer Kommentare angezeigt.

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 der Registerkarte Änderungsprotokoll wird eine Liste der Benutzeraktivitäten im Zusammenhang mit der Kontrolle angezeigt. 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.

Unter Änderungsprotokoll werden in einer Tabelle die folgenden Datenspalten angezeigt:

- Datum – Das Datum und die Uhrzeit der Aktivität, dargestellt in UTC (koordinierter Weltzeit).

- Benutzer – Der Benutzer oder die Rolle, der/die die Aktivität ausgeführt hat.
- Aktion – Eine Beschreibung der Aktivität.
- Typ – Das zugehörige Attribut, das die Aktivität näher beschreibt.
- Ressource – Die zugehörige Ressource, falls zutreffend.

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

Überprüfung der Beweise in einer Bewertung

Bei einer aktiven Bewertung in Audit Manager werden automatisch Beweise aus einer Reihe von Datenquellen gesammelt. Weitere Informationen finden Sie unter Wie AWS Audit Manager Beweise sammelt. Sie können die Beweise für die Kontrollen in Ihren Bewertungen jederzeit öffnen und überprüfen.

Um Beweise für eine Kontrolle zu öffnen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Bewertungen 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 Kontrollen, und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.
4. Wählen Sie auf der Kontrollseite die Registerkarte Beweisordner aus. In der Tabelle Beweisordner wird eine Liste aller Beweisordner für diese Kontrolle angezeigt. Diese Ordner

sind auf der Grundlage des Datums angeordnet und benannt, an dem die Beweise im Ordner gesammelt wurden.

5. Wählen Sie den Namen eines Beweisordners, um ihn zu öffnen.

Von hier aus können Sie nun die Beweisordner für diese Kontrolle überprüfen und bei Bedarf weitere Informationen einholen, um einzelne Beweiselemente zu überprüfen.

Themen

- Beweisordner überprüfen
- Überprüfung einzelner Beweise

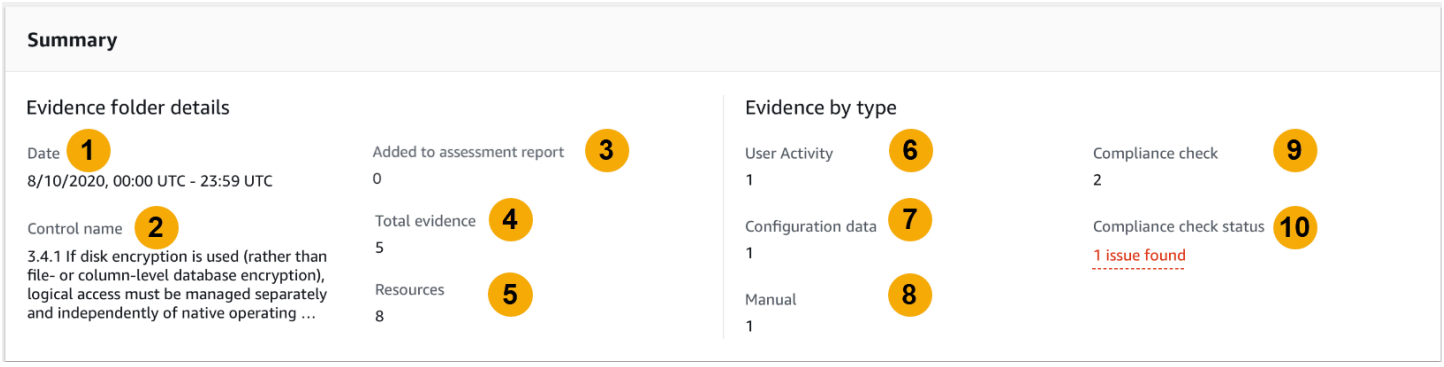
Beweisordner überprüfen

Wenn Sie einen Beweisordner öffnen, wird eine Übersichtsseite für den Beweisordner angezeigt, die zwei Abschnitte enthält: einen Abschnitt mit einer Zusammenfassung und eine Tabelle mit Beweisen. Diese Abschnitte und ihr Inhalt werden wie folgt beschrieben.

- Übersicht der Beweismappe
- Beweistabelle

Übersicht der Beweismappe

Der Abschnitt Zusammenfassung der Seite bietet einen allgemeinen Überblick über die Beweise im Beweisordner.



Dazu gehören folgende Informationen:

1. Datum – Die Uhrzeit und das Datum der Erstellung des Beweisordners, dargestellt in UTC (koordinierter Weltzeit).

2. Kontrollname – Der Name der Kontrolle, die dem Beweisordner zugeordnet ist.
3. Zum Bewertungsbericht hinzugefügt – Die Anzahl der Beweise, die manuell für die Aufnahme in den Bewertungsbericht ausgewählt wurden.
4. Beweise insgesamt – Die Gesamtzahl der Beweiselemente im Beweisordner.
5. Ressourcen – Die Gesamtzahl der AWS-Ressourcen, die bei der Generierung der Beweise in diesem Ordner bewertet wurden.
6. Benutzeraktivität – Die Anzahl der Beweiselemente, die unter die Kategorie Benutzeraktivität fallen. Diese Beweise werden aus AWS CloudTrail-Protokollen gesammelt.
7. Konfigurationsdaten – Die Anzahl der Beweiselemente, die unter die Kategorie der Konfigurationsdaten fallen. Diese Beweise stammen aus Konfigurations-Snapshots von anderen AWS-Services wie Amazon EC2, Amazon S3 oder IAM.
8. Manuell – Die Anzahl der Beweiselemente, die unter die Kategorie „Manuell“ fallen. Diese Beweise werden manuell hochgeladen.
9. Konformitätsprüfung – Die Anzahl der Beweise, die unter die Kategorie Konformitätsprüfung fallen. Diese Beweise werden von AWS Config oder AWS Security Hub gesammelt.
10. Status der Konformitätsprüfung – Die Gesamtzahl der Probleme, die direkt von AWS Security Hub, AWS Config, oder beiden gemeldet wurden.

> **Tip**
>
> Weitere Informationen zu den verschiedenen Beweisarten (Benutzeraktivität, Konfigurationsdaten, Konformitätsprüfung und manuell) finden Sie unter Beweise.

Beweistabelle

In der Beweistabelle sind die einzelnen Beweise aufgeführt, die in der Beweismappe enthalten sind.

Dazu gehören folgende Informationen:

1. Zeit – Gibt an, wann die Beweise gesammelt wurden, und dient auch als Name der Beweise. Die Zeit wird im UTC-Format (Coordinated Universal Time) dargestellt. Wenn Sie eine Uhrzeit aus dieser Spalte auswählen, wird eine Seite mit den Beweisdetails geöffnet. Diese Seite wird im folgenden Abschnitt beschrieben.
2. Beweise nach Art – Die Kategorie der Beweise.

- Die Beweise für die Konformitätsprüfung werden von AWS Config oder AWS Security Hub gesammelt.
- Beweise über Benutzeraktivitäten werden anhand von AWS CloudTrail-Protokollen gesammelt.
- Der Beweis von Konfigurationsdaten wird anhand von Snapshots anderer Services wie Amazon EC2, Amazon S3 oder IAM gesammelt.
- Manuelle Beweise sind Beweise, die Sie manuell hochladen.

3. Konformitätsprüfung – Der Bewertungsstatus für Beweise, die unter die Kategorie Konformitätsprüfung fallen.
   - Bei Beweisen, die von AWS Security Hub gesammelt wurden, wird das Ergebnis Bestanden oder Nicht bestanden direkt von AWS Security Hub gemeldet.
   - Bei Beweisen, die von AWS Config gesammelt wurden, wird das Ergebnis Konform oder Nicht konform direkt von AWS Config gemeldet.
   - Wenn Nicht zutreffend angezeigt wird, bedeutet dies, dass Sie entweder nicht die Option AWS Security Hub oder AWS Config aktiviert haben oder dass der Beweis von einem anderen Datenquellentyp stammt.
4. Datenquelle – Die Datenquelle, aus der die Beweise gesammelt wurden.
5. Ereignisname – Der Name des Ereignisses, das in den Beweisen enthalten ist.
6. Ressourcen – Die Anzahl der Ressourcen, die zur Generierung der Beweise bewertet wurden.
7. Auswahl des Bewertungsberichts – Gibt an, ob diese Beweise manuell für die Aufnahme in den Bewertungsbericht ausgewählt wurden.
   - 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.

Um manuelle Beweise in den Beweisordner hochzuladen, wählen Sie Manuelle Beweise hochladen, geben Sie die S3-URI der Beweise ein und wählen Sie dann Hochladen aus. Weitere Informationen finden Sie unter Hochladen manueller Beweise unter AWS Audit Manager.

Um Details zu einzelnen Beweiselementen anzuzeigen, wählen Sie in der Spalte Zeit den Namen des mit einem Hyperlink versehenen Beweises aus. Dadurch wird eine Detailseite für Beweise geöffnet, die im folgenden Abschnitt beschrieben wird.

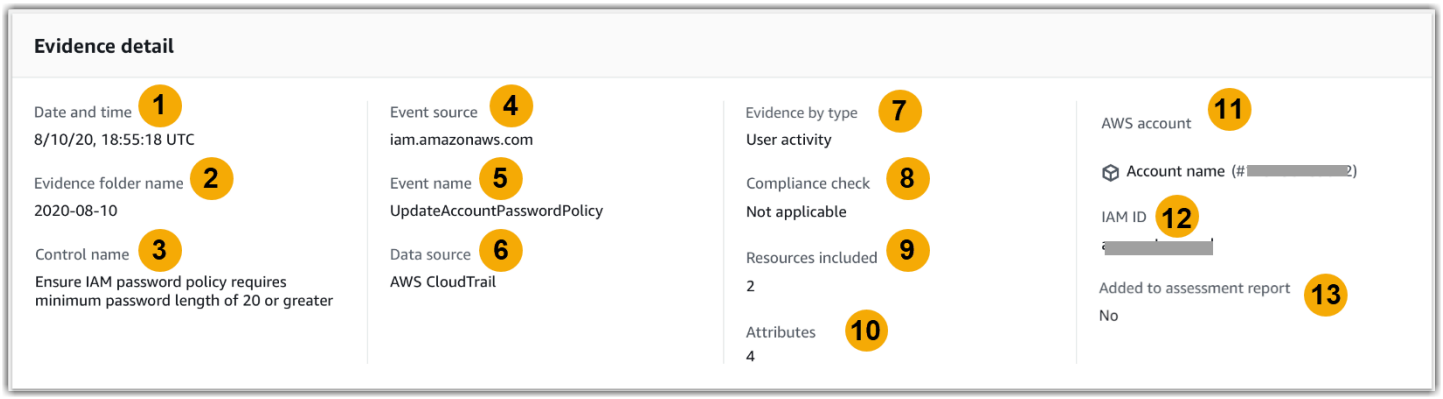
Überprüfung einzelner Beweise

Wenn Sie ein einzelnes Beweiselement öffnen, wird eine Seite mit den Beweisdetails angezeigt, die drei Abschnitte enthält: den Abschnitt mit den Beweisdetails, die Tabelle Attribute und die Tabelle Enthaltene Ressourcen. Diese Abschnitte und ihr Inhalt werden wie folgt beschrieben.

- Beweisdetails
- Attribute
- Enthaltene Ressourcen

Beweisdetails

Im Abschnitt mit den Beweisdetails auf der Seite wird eine Übersicht über die Beweise angezeigt.



Dazu gehören folgende Informationen:

1. Datum und Uhrzeit – Das Datum und die Uhrzeit der Erfassung der Beweise in koordinierter Weltzeit (UTC).
2. Name des Beweisordners – Der Name des Beweisordners, der die Beweise enthält.
3. Kontrollname – Der Name der Kontrolle, die den Beweisen zugeordnet ist.
4. Ereignisquelle – Der Name der Ressource, die das Beweisereignis ausgelöst hat.
5. Ereignisname – Der Name des Beweisereignisses.
6. Datenquelle – Die Datenquelle, aus der die Beweise gesammelt werden.
7. Beweise nach Art – Die Art der Beweise.
   - Die Beweise für die Konformitätsprüfung werden von AWS Config oder AWS Security Hub gesammelt.

- Beweise über Benutzeraktivitäten werden anhand von AWS CloudTrail-Protokollen gesammelt.
- Beweise für Konfigurationsdaten werden anhand von Snapshots anderer Systeme AWS-Services wie Amazon EC2, Amazon S3 oder IAM gesammelt.
- Manuelle Beweise sind Beweise, die Sie manuell hochladen.

8. Konformitätsprüfung – Der Bewertungsstatus für Beweise, die unter die Kategorie Konformitätsprüfung fallen.
   - Bei Beweisen, die von AWS Security Hub gesammelt wurden, wird das Ergebnis Bestanden oder Nicht bestanden direkt von AWS Security Hub gemeldet.
   - Bei Beweisen, die von AWS Config gesammelt wurden, wird das Ergebnis Konform oder Nicht konform direkt von AWS Config gemeldet.
   - Wenn Nicht zutreffend angezeigt wird, bedeutet dies, dass Sie entweder nicht die Option AWS Security Hub oder AWS Config aktiviert haben oder dass die Beweise aus einer anderen Datenquelle stammen.
9. Enthaltene Ressourcen – Die Anzahl der Ressourcen, die zur Generierung der Beweise bewertet werden.
10. Attribute – Die Gesamtzahl der Attribute, die von dem Ereignis in den Beweisen verwendet werden.
11. AWSKonto – Das AWS-Konto, von dem die Beweise gesammelt wurden.
12. IAM-ID – Der entsprechende Benutzer oder die entsprechende Rolle, falls zutreffend.
13. Zum Bewertungsbericht hinzugefügt – Gibt an, ob Sie sich dafür entschieden haben, die Beweise in den Bewertungsbericht aufzunehmen.

Attribute

In der Tabelle Attribute werden die Namen und Werte angezeigt, die von dem Ereignis in diesem Beweis verwendet werden. Dazu gehören folgende Informationen:

- Attributname – Die Anforderung für den Beweis, z. B. AllowUsersToChangePassword.
- Wert – Der Wert des Attributs, z. B. wahr oder falsch.

Enthaltene Ressourcen

In der Tabelle Enthaltene Ressourcen wird die Liste der Ressourcen angezeigt, die zur Generierung dieser Beweise bewertet wurden. Sie enthält eines oder mehrere der folgenden Felder:

- ARN – Der Amazon-Ressourcenname (ARN) der Ressource. Ein ARN ist möglicherweise nicht für alle Beweisarten verfügbar.
- Wert – Der Wert dieser Ressource, falls zutreffend.
- JSON – Der Link zum Anzeigen der JSON-Datei für diese Ressource.

Manuelle Beweise in AWS Audit Manager hinzufügen

Audit Manager kann automatisch Beweise für viele Kontrollen sammeln. Bei einigen Kontrollen müssen Sie jedoch 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 Beweis hochladen. 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 Beweis speichern.

Sie können auch die 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 On-Premises-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.

Weitere Informationen zu den verschiedenen Arten von Beweisen in Audit Manager finden Sie unter Beweise im Abschnitt Konzepte und Terminologie dieses Handbuchs.

Wie füge ich manuelle Beweise hinzu

Sie können jede der folgenden Methoden verwenden, um einer Bewertungskontrolle Ihre eigenen manuellen Beweise hinzuzufügen.

Beachten Sie Folgendes:

- Sie können jeweils nur eine Methode verwenden, um manuelle Beweise hinzuzufügen.
- Die maximal unterstützte Größe für eine einzelne Datei mit manuellen Beweisen beträgt 100 MB.
- Die Unterstützte Dateiformate für manuelle Beweise sind weiter unten auf dieser Seite aufgeführt.
- Jeder AWS-Konto kann täglich nur 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 Beweise hinzuzufügen, müssen Sie zunächst den Status der Kontrolle entweder auf Wird geprüft oder geprüft ändern. Detaillierte Anweisungen finden Sie unter Status der Kontrolle aktualisieren.

Importieren einer Datei aus Amazon S3

Befolgen Sie diese Schritte, um manuelle Beweise aus einem S3-Bucket zu importieren.

AWS console

Importieren einer Datei aus S3 (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich die Option Bewertungen und dann den Namen Ihrer Bewertung aus, um sie zu öffnen.
3. Wählen Sie die Registerkarte Kontrolle, scrollen Sie nach unten zu Kontrollsätze, und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.
4. Wählen Sie auf der Registerkarte Beweisordner die Option Manuelle Beweise hinzufügen und dann Datei aus S3 importieren aus.
   - Wählen Sie alternativ auf der Registerkarte „Beweisordner“ einen Namen für den Beweisordner aus, um die Zusammenfassung des Beweisordners zu überprüfen, und wählen Sie dann Manuelle Beweise hinzufügen, 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 Hochladen.

AWS CLI

Ersetzen Sie im folgenden Verfahren den *Platzhaltertext* mit Ihren eigenen Informationen.

Importieren einer Datei aus S3 (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 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 `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://
example-bucket/example-file.extension
```

Audit Manager API

Importieren einer Datei aus S3 (API)

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 der Kontrolle, für die Sie Beweise hochladen möchten, und notieren Sie sich deren 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.

Für weitere Informationen wählen Sie einen der vorherigen Links, um mehr in der AWS Audit ManagerAPI-Referenz zu lesen. Dies beinhaltet Informationen zur Verwendung dieser Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

Laden Sie eine Datei von Ihrem Browser hoch

Gehen Sie wie folgt vor, um manuelle Beweise aus Ihrem Browser hochzuladen.

AWS console

Um eine Datei aus Ihrem Browser (Ihrer Konsole) hochzuladen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.

2. Wählen Sie im linken Navigationsbereich die Option Bewertungen und dann den Namen Ihrer Bewertung aus, um sie zu öffnen.
3. Scrollen Sie auf der Registerkarte Kontrollen nach unten zu Kontrollsätzen und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.

   Von hier aus gibt es drei Möglichkeiten, eine Datei hochzuladen:

   - (Option 1) Wählen Sie im blauen Benachrichtigungsbanner die Option Manuelle Beweise hochladen aus.
   - (Option 2) Wählen Sie auf der Registerkarte Beweisordner die Option Manuelle Beweise hinzufügen und dann Datei aus Browser hochladen aus.
   - (Option 3) Wählen Sie einen Namen für den Beweisordner aus, um eine Zusammenfassung dieses Ordners zu überprüfen, wählen Sie Manuelle Beweise hinzufügen und dann Datei aus Browser hochladen aus.
4. Wählen Sie die Datei aus, die Sie hochladen möchten.
5. Klicken Sie auf Hochladen.

AWS CLI

Ersetzen Sie im folgenden Verfahren den *Platzhaltertext* mit Ihren eigenen Informationen.

Um eine Datei aus Ihrem Browser (CLI) hochzuladen

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 nach dem Kontrollsatz und der Kontrolle, für die 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-Einstellungen Datenverschlüsselung 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 mit serverseitiger Verschlüsselung mit KMS-Schlüsseln, die in AWS Key Management Service (SSE-KMS) gespeichert sind, im Benutzerhandbuch von Amazon Simple Storage Service.

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

Um eine Datei aus Ihrem Browser (API) 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 nach dem Kontrollsatz und der Kontrolle, für die Sie Beweise hochladen möchten, und notieren Sie sich deren 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-Einstellungen Datenverschlüsselung 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 mit serverseitiger Verschlüsselung mit KMS-Schlüsseln, die in AWS Key Management Service (SSE-KMS) gespeichert sind, im Benutzerhandbuch von Amazon Simple Storage Service.

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 wählen Sie einen der vorherigen Links, um mehr in der AWS Audit ManagerAPI-Referenz zu lesen. Dies beinhaltet Informationen zur Verwendung dieser Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

Geben Sie eine Textantwort ein

Gehen Sie wie folgt vor, um eine Antwort auf eine Frage zur Risikobewertung einzugeben und Ihre Antwort als manuellen Beweis zu speichern.

AWS console

So geben Sie eine Textantwort ein (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich die Option Bewertungen und dann den Namen Ihrer Bewertung aus, um sie zu öffnen.
3. Wählen Sie die Registerkarte Kontrolle, scrollen Sie nach unten zu Kontrollsätze, und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.

   Von hier aus gibt es drei Möglichkeiten, eine Textantwort einzugeben:

- (Option 1) Wählen Sie im blauen Benachrichtigungsbanner die Option Antwort eingeben aus.
- (Option 2) Wählen Sie auf der Registerkarte Beweisordner die Option Manuelle Beweise hinzufügen und dann Textantwort eingeben aus.
- (Option 3) Wählen Sie einen Beweisordner aus, um eine Zusammenfassung dieses Ordners zu überprüfen, wählen Sie Manuelle Beweise hinzufügen und dann Textantwort eingeben aus.

4. Geben Sie in dem daraufhin angezeigten Popup-Fenster Ihre Antwort im Klartextformat ein.
5. Wählen Sie Bestätigen aus.

AWS CLI

Ersetzen Sie im folgenden Verfahren den *Platzhaltertext* mit Ihren eigenen Informationen.

So geben Sie eine Textantwort ein (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

Um eine Textantwort (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 deren 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.

Für weitere Informationen wählen Sie einen der vorherigen Links, um mehr in der AWS Audit ManagerAPI-Referenz zu lesen. Dies beinhaltet Informationen zur Verwendung dieser Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

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	Beschreibung	Unterstützte Dateierweiterungen
Komprimierung oder Archivieren	GNU-Zip-komprimierte Archive und ZIP-komprimierte Archive	`.gz`, `.zip`
Dokument	Allgemeine Dokumentdateien wie PDFs und 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-Dokumente und Markup-Sprachdateien	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Generieren eines Bewertungsberichts

Ein Bewertungsbericht fasst Ihre Bewertung zusammen und enthält Links zu einer Reihe von Ordnern, die zugehörige Beweise enthalten. Weitere Informationen finden Sie unter Bewertungsberichte.

Sie können auswählen, welche Beweise Sie in Ihren Bewertungsbericht aufnehmen möchten, bevor Sie den Bewertungsbericht erstellen. Neu gesammelte Beweise werden nicht automatisch in einen Bewertungsbericht aufgenommen.

Aufgaben

- Hinzufügen von Beweisen zu einem Bewertungsbericht
- Beweise aus einem Bewertungsbericht entfernen
- Generieren eines Bewertungsberichts

- Was soll ich als Nächstes tun?

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 einzelne Beweiselemente innerhalb eines Ordners hinzufügen.

Um Beweise zu einem Bewertungsbericht hinzuzufügen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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 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.

      - 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.

      - 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.

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.

Um Beweise aus einem Bewertungsbericht zu entfernen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.

      - 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.

      - 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.

Generieren eines Bewertungsberichts

Nachdem Sie Ihrem Bewertungsbericht Beweise hinzugefügt haben, können Sie den endgültigen 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.

> **Tip**
>
> Um sicherzustellen, dass Ihr Bewertungsbericht erfolgreich erstellt wurde, lesen Sie unseren Konfigurationstipps für das Ziel Ihres Bewertungsberichts.

Erstellen Sie einen Bewertungsbericht wie folgt:

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.
    - 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.

Der Bewertungsbericht enthält eine Dateiprüfsumme, um die Integrität des Bewertungsberichts sicherzustellen. Sie können dies mit dem API-Vorgang ValidateAssessmentReportIntegrity überprüfen, der von Audit Manager bereitgestellt wird.

Was soll ich als Nächstes tun?

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 API-Vorgang ValidateAssessmentReportIntegrity verwenden, um Ihren Bewertungsbericht zu validieren.
- Löschen eines unerwünschten Bewertungsberichts – Erfahren Sie, wie Sie einen unerwünschten Bericht aus dem Download-Center oder aus Amazon S3 löschen können.

Den Status einer Bewertung auf inaktiv ändern

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.

> **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

Um den Status einer Bewertung in inaktiv zu ändern (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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 auf „inaktiv“ (AWS CLI) zu ändern

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 Befehl Bewertungsstatus aktualisieren 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 den *`Platzhaltertext`* 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 auf „inaktiv“ (API) zu ändern

1. Verwenden Sie den Vorgang Bewertungen auflisten, um die Bewertung zu finden, die Sie deaktivieren möchten, und notieren Sie sich die Bewertungs-ID.
2. Verwenden Sie den Vorgang Bewertungsstatus aktualisieren 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.

Für weitere Informationen zu API-Befehlen klicken Sie auf einen der vorherigen Links in der AWS Audit ManagerAPI-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

Löschen einer Bewertung

Sie können jede nicht mehr benötigte Bewertung durch den Audit Manager löschen. 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

So löschen Sie eine Bewertung (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich Bewertungen aus.
3. Wählen Sie die Bewertung, die Sie löschen möchten, und wählen Sie Löschen.
   - Alternativ können Sie die Bewertung öffnen und dann oben rechts auf der Seite Löschen auswählen.

AWS CLI

Um eine Bewertung (AWS CLI) zu löschen

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 den *Platzhaltertext* durch Ihre eigenen Informationen.

```
aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Um eine Bewertung (API) zu löschen

1. Suchen Sie mit dem Vorgang Bewertungen auflisten die Bewertung, die Sie löschen möchten.

   Notieren Sie sich die Bewertungs-ID in der Antwort.
2. Verwenden Sie den Vorgang Bewertung löschen und geben Sie die Bewertungs-ID der Bewertung an, die Sie löschen möchten.

Für weitere Informationen zu API-Befehlen klicken Sie auf einen der vorherigen Links in der AWS Audit ManagerAPI-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

> **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.

Delegierungen in AWS Audit Manager

Audit-Verantwortliche nutzen AWS Audit Manager zur Erstellung von Bewertungen und sammeln Nachweise für die Kontrollen, die in dieser Bewertung aufgeführt sind. 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.

Allgemein betrachtet, umfasst der Delegierungsprozess Folgendes:

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.

In den folgenden Abschnitten dieses Handbuchs erfahren Sie mehr über die Verwaltung von Delegierungsaufgaben in AWS Audit Manager.

Themen

> **Note**
>
> Bei einem Konto kann es sich um einen Audit-Verantwortlichen oder einen Delegierten in verschiedenen AWS Regionen handeln.

Delegierungsaufgaben für Audit-Verantwortliche

Als Audit-Verantwortlicher in AWS Audit Manager benötigen Sie möglicherweise Unterstützung von einem Fachexperten, der Sie bei der Überprüfung von Kontrollen und Nachweisen unterstützt. In diesem Fall können Sie einen Kontrollsatz zur Überprüfung delegieren.

In den folgenden Themen wird beschrieben, wie Sie Delegierungen in AWS Audit Manager verwalten können.

Aufgaben zur Delegierung

- Delegieren eines Kontrollsatzes zur Überprüfung
- Zugriff auf Ihre aktiven und abgeschlossenen Delegierungen
- Löschen Ihrer aktiven und abgeschlossenen Delegierungen

Delegieren eines Kontrollsatzes zur Überprüfung

Wenn Sie Unterstützung von einem Fachexperten benötigen, können Sie das AWS-Konto auswählen, das Sie unterstützen soll, und dann einen Kontrollsatz zur Überprüfung delegieren.

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-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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 Delegierungen jederzeit anzeigen, indem Sie im linken Navigationsbereich der AWS Audit ManagerKonsole Delegierungen auswählen.

Delegieren eines Kontrollsatzes von der Delegationsseite aus

Um einen Kontrollsatz von der Delegationsseite aus zu delegieren

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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 Delegierungen jederzeit anzeigen, indem Sie im linken Navigationsbereich der AWS Audit ManagerKonsole Delegierungen auswählen.

Wenn Sie einen Kontrollsatz zur Überprüfung delegieren, erhält der Delegierte eine Benachrichtigung und kann dann mit der Prüfung des Kontrollsatzes beginnen. Der vom Delegierten zu beachtende Prozess wird in Delegierungsaufgaben für Delegierte beschrieben.

> **Tip**
>
> Delegierte können ein SNS-Thema abonnieren, um E-Mails zu erhalten, wenn eine Prüfungsaufgabe an sie delegiert wird. Weitere Informationen dazu, wie Sie das zu AWS

Audit Managerzugehörige SNS-Thema identifizieren und abonnieren, finden Sie unter Benachrichtigungen in AWS Audit Manager.

Zugriff auf Ihre aktiven und abgeschlossenen Delegierungen

Sie können jederzeit eine Liste Ihrer Delegierungen anzeigen, indem Sie im linken Navigationsbereich AWS Audit Manager Delegierungen auswählen. Die Delegationsseite enthält eine Liste Ihrer aktiven und abgeschlossenen Delegierungen mit den folgenden Details:

- Delegiert an – Das AWS-Konto, an das Sie den Kontrollsatz delegiert haben.
- Datum – Das Datum, an dem Sie den Kontrollsatz delegiert haben.
- Status – Der aktuelle Status der Delegierung.
- Bewertung – Der Name der Bewertung mit einem Link zu den Bewertungsdetails.
- Kontrollsatz – Der Name des Kontrollsatzes, der zur Überprüfung delegiert wurde.

Wenn eine Delegierung abgeschlossen ist, erhalten Sie eine Benachrichtigung in AWS Audit Manager. Möglicherweise erhalten Sie auch Kommentare mit Anmerkungen des Delegierten. Das folgende Verfahren erklärt, wie Sie Ihre Benachrichtigungen in Audit Manager überprüfen, nachdem eine Delegierung abgeschlossen ist, und wie Sie die Kommentare der Delegierten einsehen können.

Anzeige einer abgeschlossenen Delegierung und Suche nach Kommentaren

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich Benachrichtigungen. Oder wählen Sie in der blauen Flash-Leiste oben auf dem Bildschirm Benachrichtigungen, um die Benachrichtigungsseite zu öffnen.
3. Sehen Sie sich die Seite Benachrichtigungen an, die eine Tabelle mit folgenden Informationen enthält:

    - Datum – Das Datum der Benachrichtigung.
    - Bewertung – Der Name der Bewertung, die dem Kontrollsatz zugeordnet ist.
    - Kontrollsatz – Der Name des Kontrollsatzes.
    - Quelle – Der Benutzer oder die Rolle des Delegierten, der den fertigen Kontrollsatz an Sie zurückgeschickt hat.
    - Beschreibung – Allgemeine Anmerkungen des Delegierten.

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. 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.
6. Wählen Sie die Registerkarte Kommentare, um alle Anmerkungen anzuzeigen, die der Delegierte zu dieser bestimmten Kontrolle hinzugefügt hat.
7. Wenn Sie meinen, dass die Überprüfung eines Kontrollsatzes abgeschlossen ist, wählen Sie den Kontrollsatz aus und klicken Sie auf Überprüfung des Kontrollsatzes abschließen.

> **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 der Registerkarte Changelog auf der Kontrolldetailseite. Anhand dieses Zeitstempels können Sie feststellen, welche Nachweise Sie Ihren Bewertungsberichten hinzufügen.

Löschen Ihrer aktiven und abgeschlossenen Delegierungen

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 AWS Audit Manager löschen. Sie können auch abgeschlossene Delegierungen löschen, die nicht mehr auf der Delegationsseite angezeigt werden sollen.

So löschen Sie eine Delegierung

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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.

Delegierungsaufgaben für Delegierte

Die Delegierten verfügen in der Regel über spezialisiertes geschäftliches oder technisches Fachwissen in verschiedenen Bereichen. Dazu gehören Richtlinien zur Datenaufbewahrung, Trainingspläne, Netzwerkinfrastruktur und Identitätsmanagement. Sie können Audit-Verantwortlichen dabei helfen, die gesammelten Nachweise für die Kontrollen zu überprüfen, die in ihren Zuständigkeitsbereich fallen.

Als Delegierter erhalten Sie möglicherweise Anfragen von Audit-Verantwortlichen, die mit einem Kontrollsatz verbundenen Nachweise zu überprüfen. Diese Anfrage bedeutet, dass der Audit-Verantwortliche Ihre Unterstützung bei der Überprüfung dieser Nachweise benötigt. 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.

In den folgenden Themen wird beschrieben, wie Sie Delegierungen in AWS Audit Manager verwalten können.

> **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.

Aufgaben zur Delegierung

- Ihre Benachrichtigungen für eingehende Delegierungsanfragen anzeigen
- Überprüfung des delegierten Kontrollsatzes und der zugehörigen Nachweise
- Einen Kommentar zu einem Kontrollelement hinzufügen

- Um eine Kontrolle als überprüft zu markieren
- Rückgabe des 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.

> **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.

So zeigen Sie Ihre Benachrichtigungen an

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen. Oder wählen Sie in der blauen Flash-Leiste oben auf dem Bildschirm Benachrichtigungen anzeigen, um die Benachrichtigungsseite zu öffnen.
3. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze, die Ihnen zur Prüfung delegiert wurden. Die Tabelle enthält die folgenden Informationen:

   - 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 Audit-Verantwortlichen bereitgestellt werden.

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.

Um einen Kontrollsatz zu prüfen

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich Benachrichtigungen. Oder wählen Sie in der blauen Flash-Leiste Benachrichtigungen anzeigen, um die Benachrichtigungsseite zu öffnen.
3. Auf der Seite Benachrichtigungen wird eine Liste der Kontrollsätze angezeigt, 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 Kontrollen gruppiert nach Kontrollsatz den Namen des Kontrollsatzes zur Anzeige der Kontrollen. Wählen Sie den Namen einer Kontrolle, um die Detailseite zu öffnen.
6. (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.
7. Informationen zum Kontrollelement finden Sie in den Ordnern Nachweise, Datenquellen, Kommentare und Changelog. Informationen zu den einzelnen Registerkarten und zur Interpretation der Informationen finden Sie unter Überprüfen der Kontrollen in einer Bewertung.

So überprüfen Sie die Nachweise für eine Kontrolle

1. Wählen Sie auf der Kontrollseite die Registerkarte Nachweisordner aus.
2. Navigieren Sie zur Tabelle Nachweisordner. Dort wird eine Liste der Ordner angezeigt, die Nachweise für diese Kontrolle enthalten. Diese Ordner sind nach dem Datum geordnet, an dem die Nachweise erfasst wurden.
3. Wählen Sie den Namen eines Nachweisordners, um ihn zu öffnen. Sie sehen dann eine Zusammenfassung aller an diesem Datum gesammelten Nachweise. Diese Zusammenfassung enthält die Gesamtzahl der Konformitätswarnungen, die über AWS Security Hub, AWS Config oder beides gemeldet wurden. Anweisungen zur Interpretation der Daten auf dieser Seite finden Sie unter Nachweisordner überprüfen.

4. Navigieren Sie auf der Übersichtsseite der Nachweisordner zur Tabelle Nachweise. Wählen Sie in der Spalte Zeit eine Zeile aus, die geöffnet werden soll. Prüfen Sie dann die Einzelheiten zu dem Nachweis, der zu diesem Zeitpunkt erfasst wurde. Anweisungen zur Interpretation der Daten auf der Seite finden Sie unter Nachweisordner überprüfen.

> **Tip**
>
> Auch wenn AWS Audit Manager für viele Kontrollen automatisch Nachweise erfasst, müssen Sie in manchen Fällen weitere Nachweise erbringen, um die Compliance zu belegen. In diesen Fällen können Sie manuell Nachweise hochladen. Anweisungen dazu finden Sie unter Nachweise manuell hochladen.

Einen Kommentar zu einem Kontrollelement hinzufügen

Sie können Kommentare zu allen Kontrollelementen hinzufügen, die Sie überprüfen. Diese Kommentare sind für den Audit-Verantwortlichen sichtbar.

Um einen Kommentar zu einem Kontrollelement hinzufügen

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen. Oder wählen Sie in der blauen Flash-Leiste oben auf dem Bildschirm Benachrichtigungen anzeigen, um die Benachrichtigungsseite zu öffnen.
3. 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 dann den Namen der zugehörigen Bewertung.
4. Wählen Sie die Registerkarte Kontrolle, scrollen Sie nach unten zu Kontrollsätze, und wählen Sie dann den Namen einer Kontrolle aus, um sie zu öffnen.
5. Wählen Sie die Registerkarte Kommentare.
6. Geben Sie unter Kommentare senden Ihren Kommentar in das Textfeld ein.
7. Wählen Sie Kommentar abgeben aus, um Ihren Kommentar hinzuzufügen. Ihr Kommentar wird nun zusammen mit allen anderen Kommentaren zu diesem Steuerelement im Bereich Frühere Kommentare der Seite angezeigt.

Um eine Kontrolle als überprüft zu markieren

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.

Um eine Kontrolle als überprüft zu markieren

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich Benachrichtigungen. Oder wählen Sie in der blauen Flash-Leiste oben auf dem Bildschirm Benachrichtigungen anzeigen, um die Benachrichtigungsseite zu öffnen.
3. Prüfen Sie auf der Seite Benachrichtigungen die Liste der Kontrollsätze an, die Ihnen zur Prüfung delegiert wurden. Suchen Sie nach dem Kontrollsatz, den Sie als überprüft markieren möchten, und wählen Sie den Namen der zugehörigen Bewertung.
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. Wählen Sie den Namen einer Kontrolle, um die Kontrolldetailseite zu öffnen.
6. Wählen Sie Kontrollstatus aktualisieren und ändern Sie den Status zu Überprüft.
7. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option Kontrollstatus aktualisieren, um zu bestätigen, dass Sie die Überprüfung der Kontrolle abgeschlossen haben.

Rückgabe des überprüften Kontrollsatzes an den Audit-Verantwortlichen

Wenn Sie mit der Überprüfung der an Sie delegierten Kontrollen fertig sind, geben Sie den Kontrollsatz an den Audit-Verantwortlichen zurück. Damit ist der Delegierungsvorgang abgeschlossen.

Zur Rückgabe eines überprüften Kontrollsatzes an den Audit-Verantwortlichen

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.

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. Nachdem Sie die Kontrolle an den Audit-Verantwortlichen übermittelt haben, kann dieser alle Kommentare einsehen, die Sie hinterlassen haben.

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.

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 Dateien AssessmentReportSummary.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`) – 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.

Wie navigiere ich in einem Bewertungsbericht?

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.

Abschnitte des 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

- Übersichtsseite
- Seite mit dem Inhaltsverzeichnis
- Kontrollseite
- Nachweisübersichtsseite
- Seite mit den Nachweisdetails

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 ersetzt die *Platzhalter* 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.

- Berichtname – der Name des Berichts.
- Beschreibung – Die Beschreibung, die der Prüfungsverantwortliche bei der Erstellung des Berichts eingegeben hat.
- Generierungsdatum – Das Datum, an dem der Bericht generiert wurde. Es wird im UTC-Format (Coordinated Universal Time) dargestellt.
- Gesamtzahl der enthaltenen Kontrollen – Die Anzahl der Kontrollen, die im Bericht enthalten sind und für die Nachweise gesammelt wurden. Dies ist eine Teilmenge der Gesamtzahl der Kontrollen in der Bewertung.
- AWS-Konten enthalten – Die Anzahl der PersonenAWS-Konten, die im Bericht enthalten sind und für die Nachweise gesammelt wurden. Dies ist ein Teil der Gesamtzahl der AWS-Konten, die in der Bewertung enthalten sind.

- Auswahl des Bewertungsberichts – 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.

- Bewertungsname – Der Name der Bewertung, anhand derer der Bericht erstellt wurde.
- Status – Der Status der Bewertung zum Zeitpunkt der Erstellung des Berichts.
- Bewertungsregion – Die RegionAWS-Region, in der die Bewertung erstellt wurde.
- AWS-Konten im Geltungsbereich – Die vollständige Liste der AWS-Konten, die im Geltungsbereich der Bewertung enthalten sind.
- AWS-Services im Geltungsbereich – Die vollständige Liste der AWS-Services, die im Geltungsbereich der Bewertung enthalten sind.
- Framework-Name – Der Name des Frameworks, aus dem heraus die Bewertung erstellt wurde.
- Audit-Verantwortliche – 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.

- Kontrollname – Der Name der Kontrolle.
- Beschreibung – Die Beschreibung der Kontrolle.
- Kontrollsatz – Der Name des Kontrollsatzes, zu dem die Kontrolle gehört.
- Testinformationen – Die empfohlenen Testverfahren für diese Kontrolle.
- Aktionsplan – Die empfohlenen Maßnahmen, die durchgeführt werden müssen, wenn die Kontrolle nicht bestanden wurde.
- Auswahl des Bewertungsberichts – 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 Nachweise sind nach Ordnern gruppiert, die nach dem Datum der Nachweiserhebung geordnet und benannt sind. Neben dem Namen jedes Nachweisordners steht die Gesamtzahl der Probleme mit der Konformitätsprüfung für diesen Ordner.

Unter dem Namen jedes Nachweisordners befindet sich eine Liste aus Hyperlinks mit Nachweisnamen.

- Namen automatisierter Nachweise beginnen mit einem Zeitstempel für die Nachweiserhebung, 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 oder AWS Config gesammelt wurden, wird als Ergebnis Konform, Nicht konform oder Nicht schlüssig gemeldet.
- Bei automatisierten Nachweisen, die anhand von AWS CloudTrail API-Aufrufen gesammelt wurden, und bei allen manuellen Nachweisen wird das Ergebnis Nicht schlüssig angezeigt.

Nachweisübersichtsseite

Die Nachweisübersichtsseite enthält die folgenden Informationen:

- ID – Die eindeutige Kennung für die Nachweise.
- Datum der Erfassung – Das Datum, an dem die Nachweise erstellt oder hochgeladen wurden.
- Beschreibung – Eine Beschreibung der Nachweise, einschließlich der Konto-ID und des Datenquellentyps.
- Bewertungsname – Der Name der Bewertung, anhand derer der Bericht erstellt wurde.
- Framework-Name – Der Name des Frameworks, aus dem heraus die Bewertung erstellt wurde.
- Kontrollname – Der Name der Kontrolle, die durch die Nachweise unterstützt wird.
- Name des Kontrollsatzes – Der Name des Kontrollsatzes, zu dem die zugehörige Kontrolle gehört.
- Beschreibung der Kontrolle – Die Beschreibung der Kontrolle, die durch die Nachweise unterstützt wird.
- Testinformationen – Die empfohlenen Testverfahren für die Kontrolle.
- Aktionsplan – Die empfohlenen Maßnahmen, die durchgeführt werden müssen, wenn die Kontrolle nicht bestanden wurde.
- AWS-Region – Der Name des Geräts, das dem Nachweis zugeordnet ist.
- IAM-ID – Die ARN des Benutzers oder der Rolle, die mit den Nachweisen verknüpft ist.
- AWS-Konto – Die AWS-Konto-ID, die den Nachweisen zugeordnet ist.

- AWS-Service – Der Name des AWS-Service, der den Nachweisen zugeordnet ist.
- Enthaltene Ressourcen – Die AWS-Ressourcen, die zur Generierung der Nachweise bewertet wurden. Dieses Attribut gilt nicht für Nachweise zur Konformitätsprüfung von AWS Config. Für diesen Nachweistyp finden Sie alle Ressourcen tabellarisch aufgeführt in den Seite mit den Nachweisdetails der PDF-Datei mit den Nachweisen.
- Ereignisname – Der Name des Nachweisereignisses.
- Ereigniszeit – Die Zeit, zu der das Ereignis aufgetreten ist.
- Datenquelle – Woher die Nachweise gesammelt oder hochgeladen wurden. Der Datenquellentyp kann entweder AWS Config, Security Hub, AWS-API-Aufrufe, CloudTrail oder Manuell sein.
- Nachweise nach Art – Die Kategorie der Nachweise
  - Nachweise zur Konformitätsprüfung werden von AWS Config unserem Security Hub gesammelt.
  - Nachweise zu Benutzeraktivitäten werden aus CloudTrail-Protokollen gesammelt.
  - Nachweise für Konfigurationsdaten werden anhand von Schnappschüssen anderer AWS-Services gesammelt.
  - Manuelle Nachweise sind Nachweise, die Sie manuell hochladen.
- Status der Konformitätsprüfung – Der Bewertungsstatus für Nachweise, die unter die Kategorie Konformitätsprüfung fallen.
  - Bei automatisierten Nachweisen, die von AWS Security Hub oder AWS Config gesammelt wurden, wird als Ergebnis Konform, Nicht konform oder Nicht schlüssig gemeldet.
  - Bei automatisierten Nachweisen, die anhand von AWS CloudTrail API-Aufrufen gesammelt wurden, und bei allen manuellen Nachweisen wird das Ergebnis Nicht schlüssig 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.

Bewertungsberichts zur Integritätsprüfung

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 ValidateAssessmentReportIntegrity-API, die von Audit Manager bereitgestellt wird, um die Integrität eines Bewertungsberichts zu überprüfen.

Fehlerbehebung Bewertungsberichte

Antworten auf häufig gestellte Fragen und Probleme finden Sie unter Fehlerbehebung bei Problemen mit dem Bewertungsbericht im Abschnitt Fehlerbehebung dieses Handbuchs.

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 diese Feature in Ihren Audit Manager-Einstellungen aktivieren.

Themen

Verstehen, wie die Beweissuche mit CloudTrail Lake Featureiert

Die Beweissuche verwendet die Abfrage- und SpeicherFeatureen von AWS CloudTrail Lake. Bevor Sie de Beweissuche verwenden, ist es hilfreich, etwas mehr über die Featuresweise von CloudTrail Lake zu erfahren.

CloudTrail Lake fasst Daten in einem einzigen, durchsuchbaren Ereignisdatenspeicher zusammen, 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 SuchFeature 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 dieses Feature aktiviert ist, ist das Daten-Backfill-Verfahren kostenlos, sofern es bis November 2023 abgeschlossen ist.
> Wenn in Zukunft neue Beweisdaten zum Ereignisdatenspeicher hinzugefügt werden, fallen CloudTrail Lake-Gebühren für 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 für CloudTrail Lake finden Sie unter AWS CloudTrail Preise.

Beweissuche aktivieren

Sie können die Beweissuche in Ihren Audit Manager-Einstellungen aktivieren. Anweisungen finden Sie unter Beweissuche auf der AWS Audit Manager Einstellungsseite dieses Handbuchs.

Fehlerbehebung für die Beweissuche

Antworten zu häufig gestellten Fragen und Probleme finden Sie unter Fehlerbehebung für die Beweissuche im Abschnitt Fehlerbehebung dieses Handbuchs.

Suche nach Beweisen

Gehen Sie wie folgt vor, um über die Audit Manager-Konsole Beweise zu suchen.

> **Note**
>
> Sie können auch die CloudTrail-API verwenden, um Ihre Beweisdaten abzufragen. Weitere Informationen finden Sie unter StartQuery in der AWS CloudTrail-API-Referenz. Wenn Sie lieber AWS CLI verwenden möchten, finden Sie weitere Informationen unter Eine Abfrage starten im AWS CloudTrail-Benutzerhandbuch.

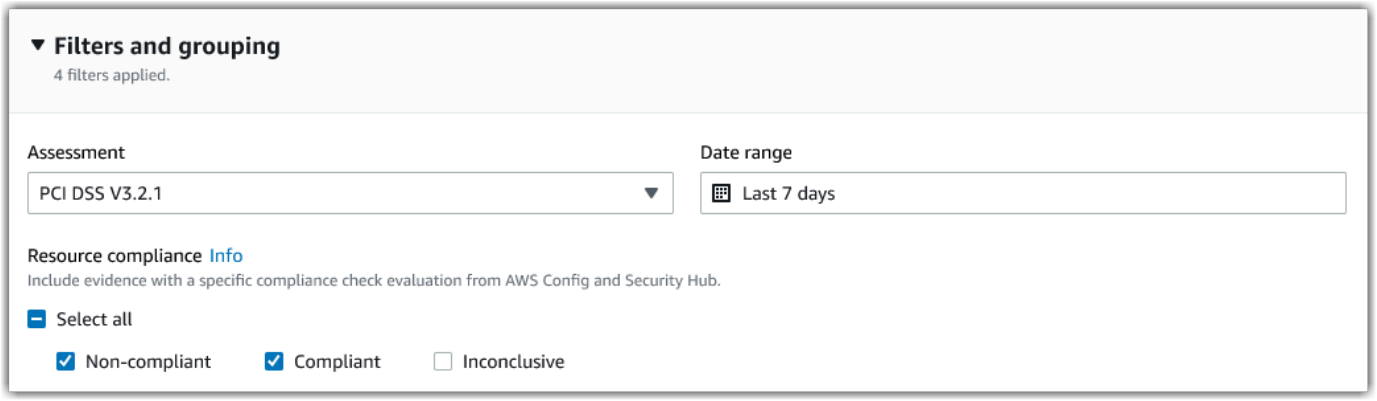
Auf dieser Seite

Durchführen einer Suchabfrage

Gehen Sie wie folgt vor, um eine Suchabfrage in der Beweissuche durchzuführen.

Um nach Beweisen zu suchen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.

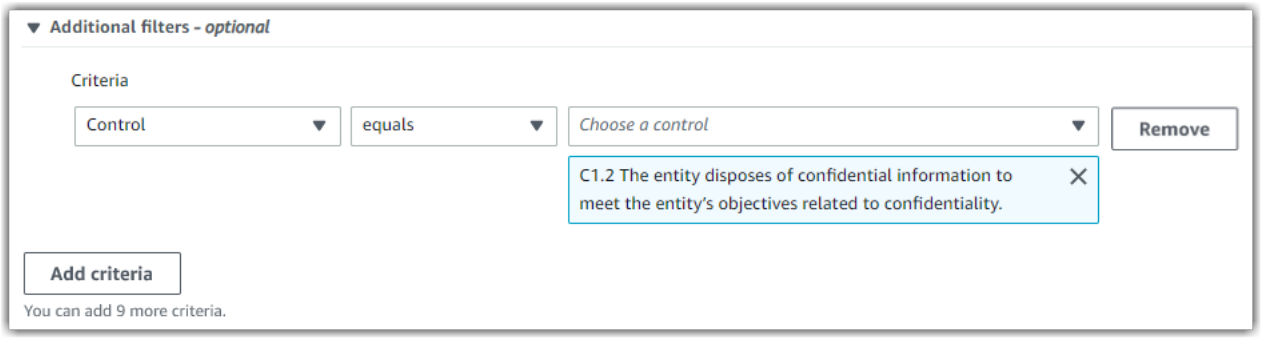


4. (Optional) Wählen Sie Zusätzliche Filter – optional, um die Suche noch weiter einzuschränken.

   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.

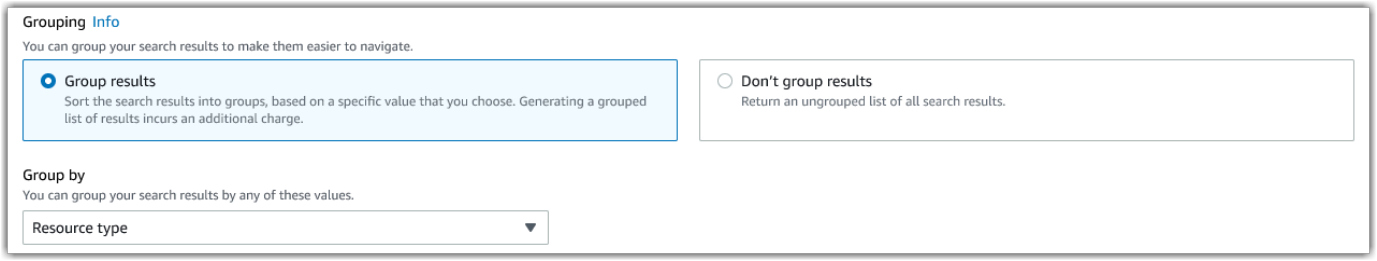
   c. Um einen Filter zu entfernen, wählen Sie Entfernen.



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.

> **Tip**
>
> Weitere Informationen zu den Filtern und Gruppierungen, die Sie in diesem Verfahren verwenden können, finden Sie unter Filter- und Gruppierungsoptionen.

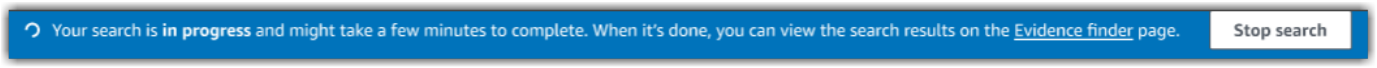
Eine Suchabfrage anhalten

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.

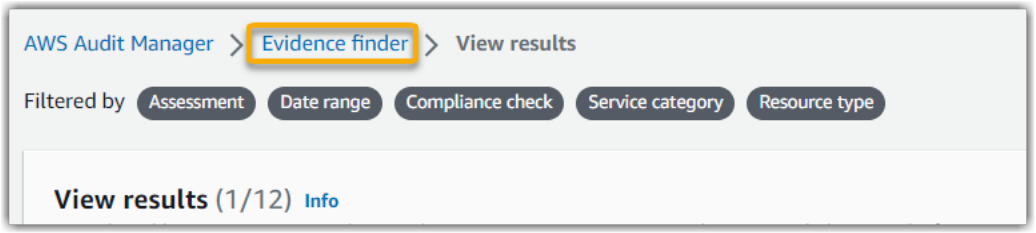
Bearbeiten von Suchfiltern

Sie können zu Ihrer letzten Suchabfrage zurückkehren und die Filter nach Bedarf ändern.

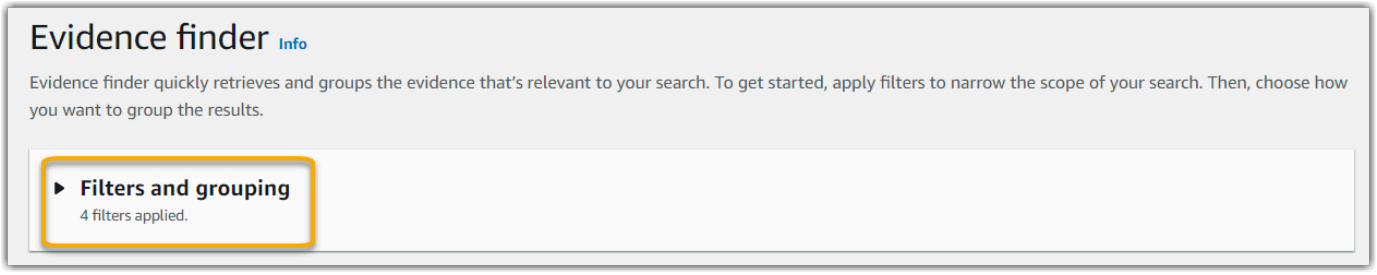
> **Note**
>
> Wenn Sie Ihre Filter bearbeiten und Suchen wählen, wird eine neue Suchabfrage gestartet.

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.

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 https://console.aws.amazon.com/cloudtrail/ einsehen. 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.

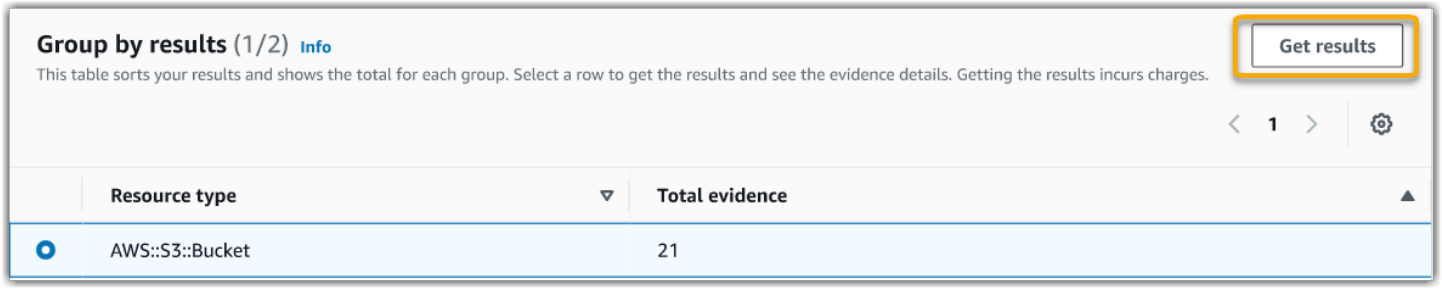
Auf dieser Seite

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.

Anzeigen der Ergebnisse

In der Tabelle Ergebnissen anzeigen werden Ihre Suchergebnisse angezeigt. Von hier aus können Sie folgende Aktionen ausführen:

- Verwalten Ihrer Anzeigeeinstellungen
- Vorschau der Ressourcenübersichten
- Generieren Sie aus Ihren Suchergebnissen einen Bewertungsbericht
- Exportieren Ihrer Suchergebnisse

Verwalten 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:
    a. Sichtbare Tabellenspalten auswählen – Verwenden Sie die Umschaltoption, um zu ändern, welche Spalten angezeigt werden.
    b. Seitengröße – Wählen Sie aus, wie viele Ergebnisse auf jeder Seite angezeigt werden.
    c. Zeilenumbruch – Aktivieren Sie das Kontrollkästchen, um lange Textzeilen zur besseren Lesbarkeit aufzuteilen.
3. Wählen Sie Bestätigen, um Ihre Einstellungen zu speichern.

Vorschau der Ressourcenübersichten

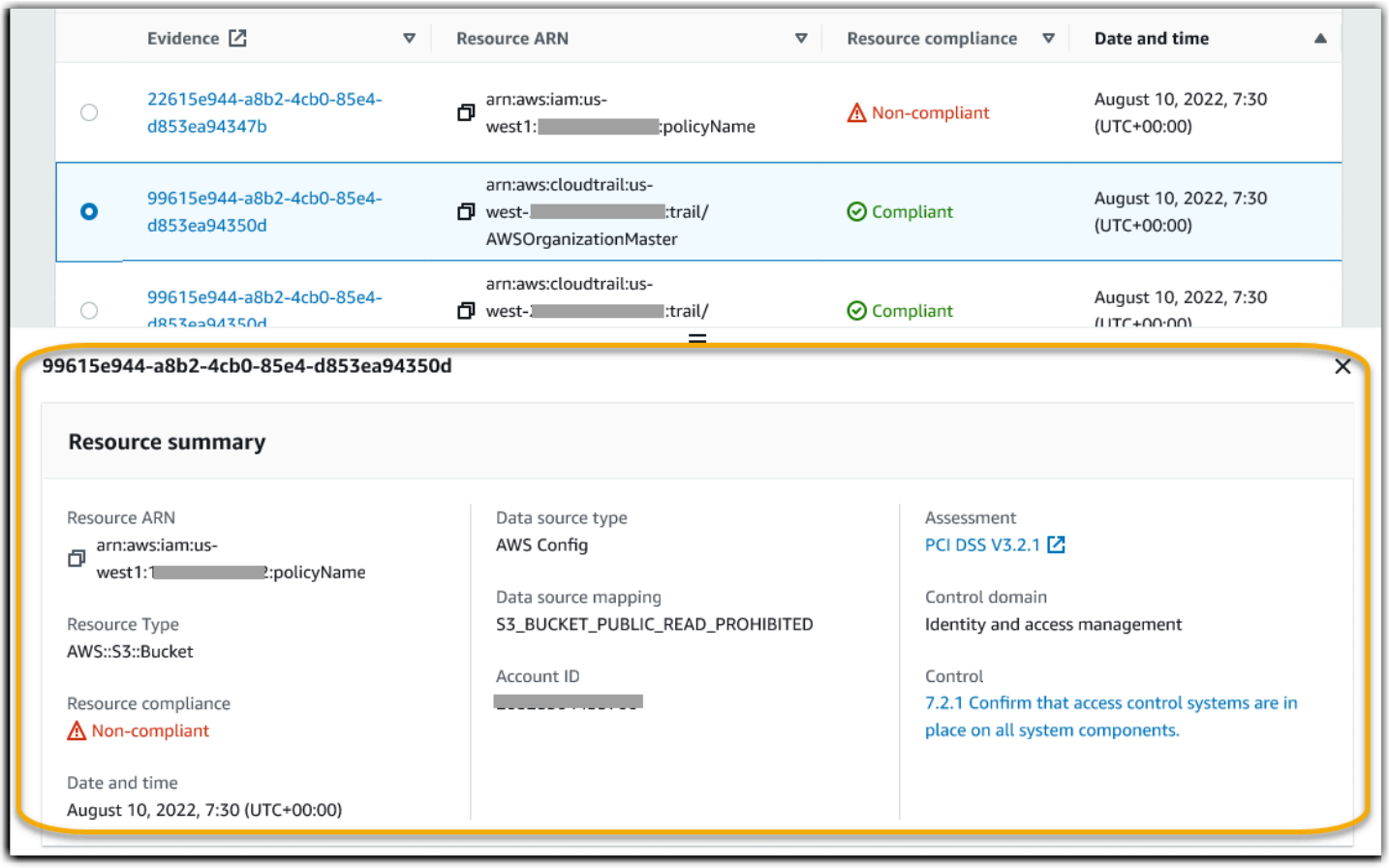
Sie können eine Vorschau der zugehörigen Ressourcen anzeigen, um die Beweise zu finden, die Ihrer Suchabfrage entsprechen. Auf diese Weise können Sie feststellen, ob die Suchabfrage die gewünschten Ergebnisse geliefert hat oder ob Sie Ihre Filter anpassen und die Suchabfrage erneut ausführen müssen.

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.



Generieren Sie aus Ihren Suchergebnissen einen Bewertungsbericht

Wenn Sie mit den Suchergebnissen zufrieden sind, erstellen Sie einen Bewertungsbericht.

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 Fehlerbehebung zur Beweissuche.

Exportieren Ihrer Suchergebnisse

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, um CSV-Dateien aus der Beweissuche zu exportieren und bereitzustellen. Die folgenden Faktoren definieren, wie der CSV-Exportprozess Featureiert:

- 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 unter Struktur der CloudTrail-Signaturdatei im AWS

CloudTrailDeveloper Guide. Um festzustellen, ob die Abfrageergebnisse geändert, gelöscht oder nicht verändert wurden, nachdem sie von CloudTrail übermittelt wurden, können Sie die Integritätsvalidierung für CloudTrail-Abfragen verwenden. 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. Ihr S3-Bucket muss außerdem über die erforderlichen Berechtigungsrichtlinien verfügen, damit CloudTrail die Exportdateien schreiben kann. 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 unter Konfigurationstipps für Ihr Exportziel. Wenn beim Exportieren einer CSV-Datei Probleme auftreten, finden Sie weitere Informationen unter Fehlerbehebung bei CSV-Exporten für die Beweissuche.

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

Um Ihre CSV-Datei zu finden und ihren Status zu überprüfen, gehen Sie zum Audit Manager Downloadcenter. 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
```

Filter- und Gruppenoptionen

Auf dieser Seite werden die Filter- und Gruppierungsoptionen beschrieben, die in der Beweissuche verfügbar sind.

Auf dieser Seite

Referenz filtern

Sie können die folgenden Filter verwenden, um Beweise zu finden, die bestimmten Kriterien entsprechen, z. B. eine Bewertung, Kontrolle oder AWS-Service.

Themen

Erforderliche Filter

Verwenden Sie diese Filter, wenn Sie einen allgemeinen Überblick zu den Beweisen zu einer Bewertung wünschen.

Name des Filters	Beschreibung	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`**).

Name des Filters	Beschreibung	Hinweise
		Oder Sie können einen absoluten Bereich verwenden, um einen bestimmten Datumsbereich anzugeben (z. B. **`June 27th - July 4th`**).

Name des Filters	Beschreibung	Hinweise
Ressourcen-Compliance	Gibt Ressourcen zurück, für die eine bestimmte Compliance-Überprüfung durchgeführt wurde.	Audit Manager sammelt Beweise zur Compliance-Überprüfung für Kontrollen, die AWS Config und Security Hub als Datenquellentyp verwenden. 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 ist der Fall, wenn Security Hub als Ergebnis Fehlgeschlagen oder wenn AWS Config ein nicht konformes Ergebnis meldet. • Konform – Dieser Filter findet Ressourcen, bei denen keine Probleme mit der Compliance-Überprüfung aufgetreten sind. Dies ist der Fall, wenn Security Hub als Ergebnis Bestanden oder wenn AWS Config ein konformes Ergebnis meldet. • Nicht eindeutig – Dieser Filter findet Ressourcen, für die keine Compliance-Überprüfung verfügbar oder anwendbar ist. Dies passiert, wenn eine Ressource AWS Config oder Security Hub als Datenquellentyp verwendet, diese Services jedoch nicht aktiviert sind. Dies ist auch der Fall, wenn die Ressource einen zugrunde liegenden Datenquellentyp verwendet, der keine Complianc

Name des Filters	Beschreibung	Hinweise
		e-Überprüfungen 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	Beschreibung	Wann sollten diese Kriterien verwendet werden
Konto-ID	Aufschlüsselung 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.
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 Identitäts- und Zugriffsmanagement, Protokollierung und Überwachung sowie Netzwerkmanagement.
Data source	Aufschlüsselung nach Datenquellentyp.	Verwenden Sie diese Kriterien, um sich auf eine bestimmte Datenquelle zu konzentrieren.

Name des Kriteriums	Beschreibung	Wann sollten diese Kriterien verwendet werden
type (Datenquellentyp)		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` oder`AWS API calls`).
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 von CloudTrail protokolliert wird, 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 zu bewertenden Ressource zu konzentrieren, beispielsweise eine Amazon EC2-Instance oder einen S3-Bucket.
Service	Aufschlüsselung nach AWS-Service-Namen.	Verwenden Sie diese Kriterien, um Beweise zu finden, die sich auf einen bestimmten AWS-Service beziehen, z. B. Amazon EC2, Amazon S3 oder AWS Config.

Name des Kriteriums	Beschreibung	Wann sollten diese Kriterien verwendet werden
Servicekategorie	Aufschlüsselung nach AWS-Service-Kategorien.	Verwenden Sie diese Kriterien, um sich auf eine bestimmte Kategorie von AWS-Service zu konzentrieren. Zu den Beispielen gehören Sicherheit, Identität und Compliance, Datenbank und Speicher.

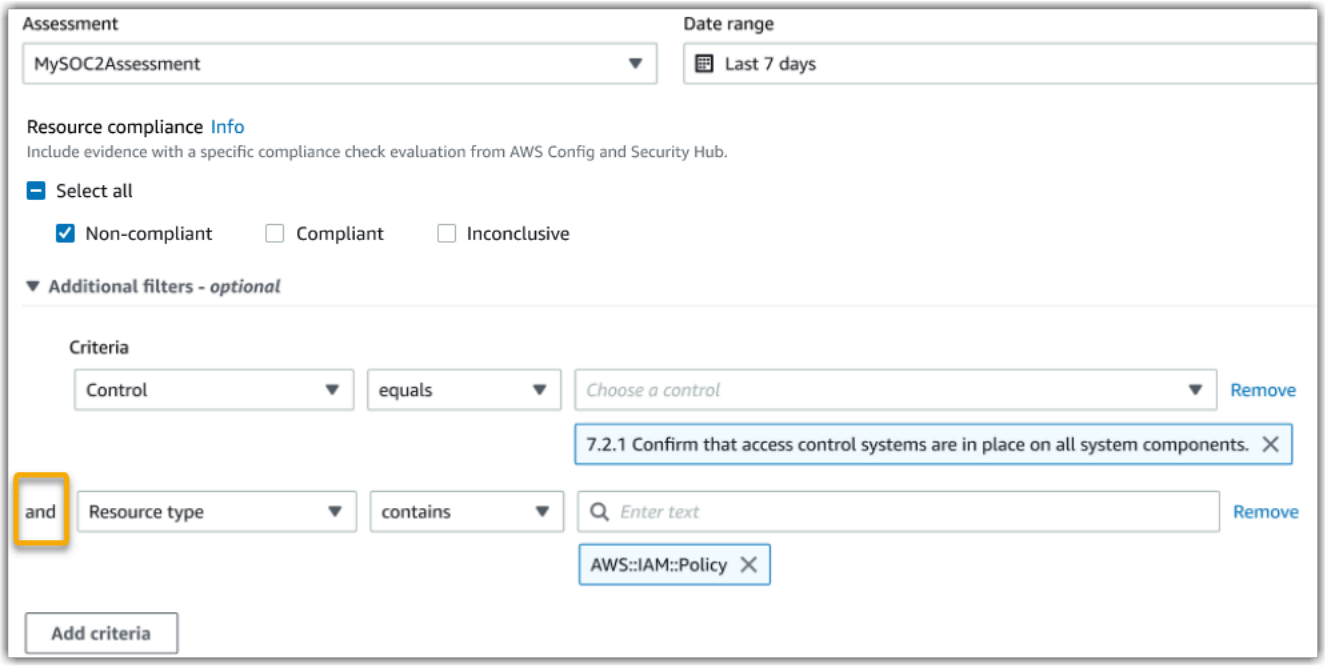
Kombinieren von Filtern

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.

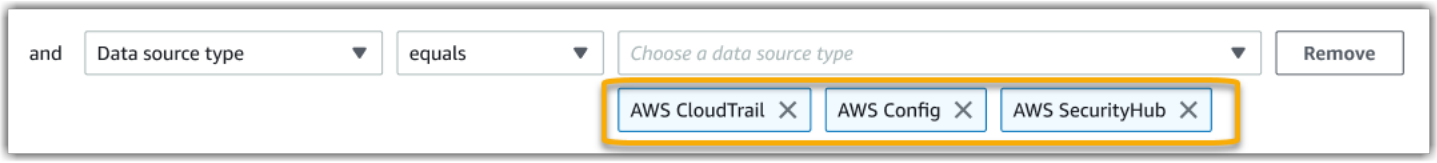


Verhalten des Kriterienwerts

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 die Beweissuche Suchergebnisse aus, die entweder aus AWS CloudTrail, AWS Config oder AWS Security Hub stammen.



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.

Group by (Gruppierung nach)	Beschreibung
Konto-ID	Gruppieren der Ergebnisse nach AWS-Konto.

Group by (Gruppierung nach)	Beschreibung
Kontrolle	Ergebnisse nach dem Namen der Kontrolle gruppieren.
Kontrolldomaine	Ergebnisse nach Kontrolldomäne 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.

Beispielanwendungsfälle

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 den benötigten Beweis gefunden haben, folgen Sie den Schritten, um aus den Suchergebnissen einen Bewertungsbericht zu erstellen. 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, wenn Sie in SecOps, IT/DevOps oder einer anderen Rolle arbeiten, 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 *<Platzhalter>* durch Ihre eigenen Werte.

```
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 Instanceen derselben Kriterien verantwortlich sind (z. B. wenn Sie mehrere AWS-Services besitzen), 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.

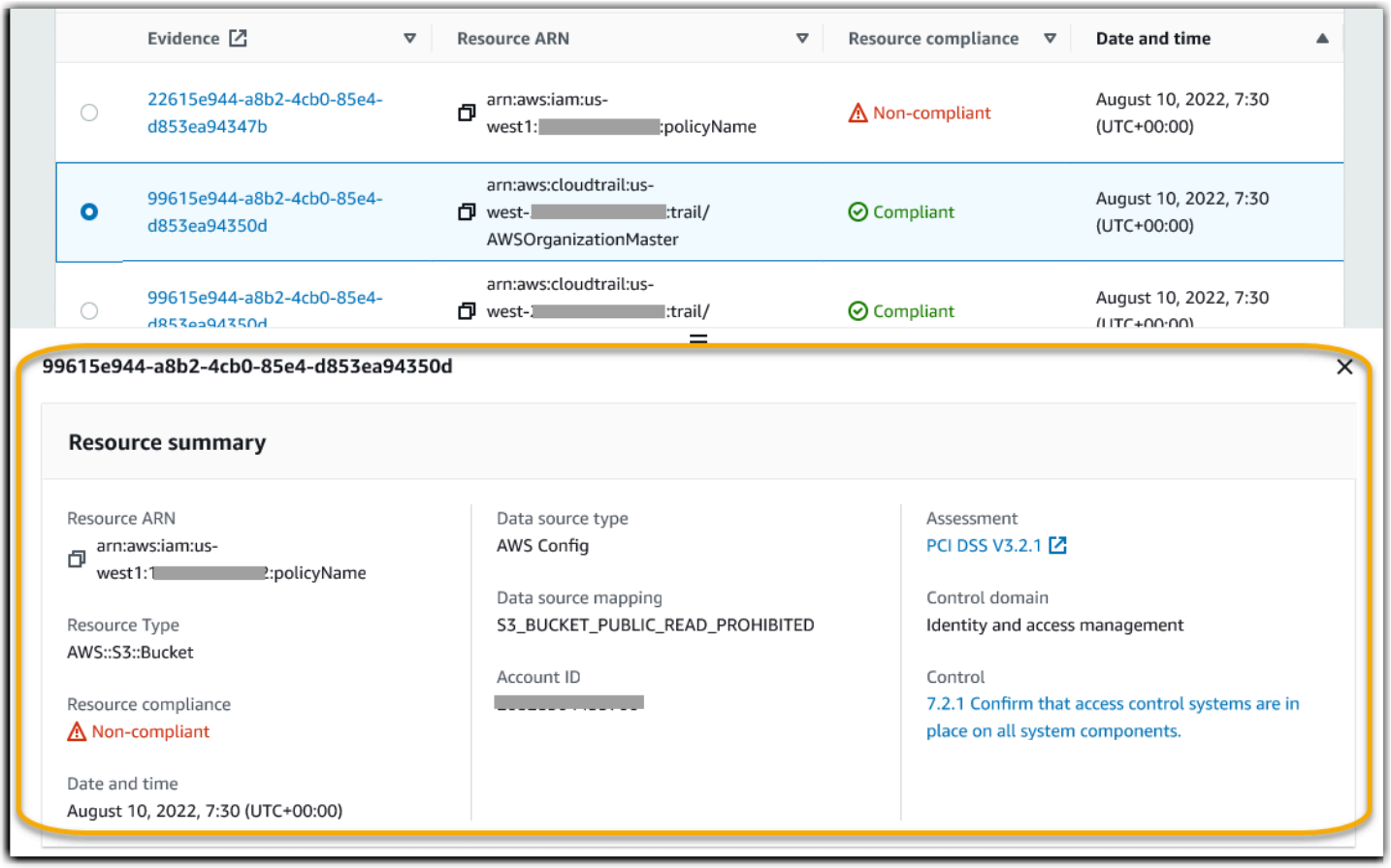
Anwendungsfall 3: Führen Sie eine kurze Vorschau der Ressourcen zu den Beweisen durch

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 der Ressourcenübersichten.



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.

Themen

Das Download-Center durchsuchen

Um das Download-Center aufzurufen, öffnen Sie die Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home und wählen Sie dann im linken Navigationsbereich die Option Download-Center aus.

Sie können zwischen den folgenden Registerkarten wechseln, um Ihre Dateien nach Kategorien zu durchsuchen.

Registerkarte „Bewertungsberichte“

Auf dieser Registerkarte werden alle 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:

- In Bearbeitung – Audit Manager erstellt derzeit den Bewertungsbericht.
- Bereit – Der Bewertungsbericht steht für Sie zum Herunterladen bereit.
- 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 unter Fehlersuche Bewertungsberichte.

Registerkarte „Exporte“

Auf dieser Registerkarte werden alle Nachweis-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:

- In Bearbeitung – Audit Manager bereitet derzeit 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 unter Fehlersuche bei Problemen mit dem CSV-Export.

> **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. Dazu gehören Abfragen, die in der CloudTrail-Konsole oder mithilfe der CloudTrail-API erstellt wurden. CloudTrail-Exporte werden auf dieser Registerkarte angezeigt, wenn Sie den Audit 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-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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 Herunterladen einer Datei aus Ihrem S3-Zielort-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-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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.

Framework-Bibliothek

Sie können über die Framework-Bibliothek in AWS Audit Manager auf Frameworks zugreifen und diese verwalten.

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 Vorlage verwenden, um Ihre AWS-Service-Nutzung zu überprüfen und mit der Automatisierung der Beweissuche zu beginnen.

Die Framework-Bibliothek enthält einen Katalog von Standard- und benutzerdefinierten Frameworks.

- Standard-Frameworks sind vorgefertigte Frameworks, die AWS bietet: Diese Frameworks basieren auf Best Practices von AWS für verschiedene Compliance-Standards und Vorschriften. Dazu gehören die DSGVO und HIPAA. Zu den Standard-Frameworks gehören in Gruppen organisierte Kontrollsätze, 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 jedes Standard-Framework anpassen, um ein neues Framework zu erstellen, das Ihren spezifischen Anforderungen entspricht.
- Benutzerdefinierte Frameworks sind auf Sie zugeschnittene Frameworks. Sie können ein benutzerdefiniertes Framework ganz neu erstellen oder ein vorhandenes individuell anpassen. Sie können benutzerdefinierte Frameworks verwenden, um Kontrollsätze so zu organisieren, dass sie Ihren spezifischen Anforderungen entsprechen. Weitere Informationen zum Verwalten von Kontrollen finden Sie unter Kontrollbibliothek.

Sie können eine Bewertung anhand eines Standard-Frameworks oder eines benutzerdefinierten Frameworks erstellen. Weitere Informationen zum Erstellen und Verwalten von Bewertungen finden Sie unter Bewertungen in AWS Audit Manager.

> **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 Beweise AWS Audit Manager enthalten möglicherweise nicht alle Informationen über Ihre AWS-Nutzung, die für Audits erforderlich sind. AWS Audit Manager ist kein Ersatz für Rechtsbeistand oder Compliance-Experten.

In diesem Abschnitt wird beschrieben, wie Sie benutzerdefinierte Frameworks in Audit Manager erstellen und verwalten können.

Themen

Zugriff auf die verfügbaren Frameworks in AWS Audit Manager

Sie können alle verfügbaren Frameworks auf der Framework-Bibliotheksseite über die Audit Manager-Konsole öffnen. Von hier aus können Sie auch eine Bewertung anhand eines Frameworks erstellen, ein benutzerdefiniertes Framework erstellen oder ein vorhandenes Framework anpassen.

Sie können auch alle verfügbaren Frameworks mithilfe der Audit Manager-API oder der AWS Command Line Interface (AWS CLI) anzeigen.

Audit Manager console

So öffnen Sie die verfügbaren Frameworks (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.
4. Wählen Sie einen Framework-Namen aus, um die Details dieses Frameworks anzuzeigen.

AWS CLI

So öffnen Sie die verfügbaren Frameworks (AWS CLI)

Um Frameworks in Audit Manager zu öffnen, verwenden Sie den Befehl list-assessment-frameworks und geben Sie einen `--framework-type` an. 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

So öffnen Sie die verfügbaren Frameworks (API)

Nutzen Sie den Befehl ListAssessmentFrameworks und geben Sie einen Framework-Typ 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 ManagerAPI-Referenz zu erfahren. Dies beinhaltet Informationen zur Verwendung des `ListAssessmentFrameworks` Vorgangs und der Parameter in einem der sprachspezifischen AWS-SDKs.

Anzeige der Details eines Frameworks

Sie können die Details eines Frameworks mithilfe der Audit Manager-Konsole, der Audit Manager-API oder der AWS Command Line Interface (AWS CLI) überprüfen.

Audit Manager console

So öffnen Sie Framework-Details (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.

Beim Öffnen eines Frameworks wird eine Framework-Detailseite angezeigt. Die Abschnitte dieser Seite und ihr Inhalt werden wie folgt beschrieben.

Abschnitt Framework-Details

Dieser Abschnitt zeigt die Frameworks im Überblick. Dazu gehören folgende Informationen:

- Framework-Name – Der Name des Frameworks.
- Konformitätstyp – Der Konformitätsstandard oder die -vorschrift, die durch das Framework unterstützt wird.
- Beschreibung – Eine Beschreibung des Frameworks, sofern vorhanden.
- Framework-Typ – Gibt an, ob es sich bei dem Framework um ein Standard-Werk oder ein benutzerdefiniertes handelt.
- Kontrollgruppen – Die Anzahl der Kontrollsätze, die dem Framework zugeordnet sind.
- Kontrollen – Die Gesamtzahl der Kontrollen im Framework.
- Kontrollquellen – Die Anzahl der Kontrolldatenquellen, aus denen Audit Manager Beweise sammelt.
- Tags – Die Tags, die dem Framework zugeordnet sind.

Wenn Sie sich ein benutzerdefiniertes Framework ansehen, werden auch die folgenden Details angezeigt:

- Erstellt von – Das Konto, mit dem das benutzerdefinierte Framework erstellt wurde.
- Erstellt am – 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. Dazu gehören folgende Informationen:

- Nach Kontrollsätzen eingeteilte Kontrollen – Wählen Sie das Symbol in der Strukturansicht, um die Kontrollen zu sehen, die zu den einzelnen Kontrollsätzen gehören.
- Typ – Gibt an, ob es sich bei der Kontrolle um eine Standard-Kontrolle oder eine benutzerdefinierte handelt.
- Datenquelle – Gibt die Datenquelle an, aus der Audit Manager Beweise für diese Kontrolle sammelt.

Registerkarte „Tags“

Diese Registerkarte listet die Tags auf, die dem Framework zugeordnet sind. Dazu gehören folgende Informationen:

- Schlüssel – Der Tag-Schlüssel (z. B. ein Konformitätsstandard, eine Vorschrift oder eine Kategorie).
- Wert – Der Tag-Wert.

AWS CLI

So öffnen Sie Framework-Details (AWS CLI)

1. Um das Framework zu identifizieren, das Sie überprüfen möchten, verwenden Sie den Befehl list-assessment-frameworks und geben Sie einen `--framework-type` an. Sie können entweder eine Liste der Standard-Frameworks oder auch eine Liste der benutzerdefinierten Frameworks abrufen.

   Ersetzen Sie im folgenden Beispiel den *`Platzhaltertext`* 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 Befehl get-assessment-framework aus und geben Sie den `--framework-id` an.

Ersetzen Sie im folgenden Beispiel den *Platzhaltertext* durch Ihre eigenen Informationen.

```
aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Die Framework-Details werden im JSON-Format zurückgesandt. Informationen zu diesen Daten finden Sie in der AWS CLIBefehlsreferenz unter get-assessment-framework Output.

3. Um die Tags für ein Framework anzuzeigen, verwenden Sie den Befehl list-tags-for-resource und geben Sie den `--resource-arn` für das Framework an.

   Ersetzen Sie im folgenden Beispiel den *Platzhaltertext* 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

So öffnen Sie Framework-Details (API)

1. Um das zu überprüfende Framework zu identifizieren, verwenden Sie den Befehl ListAssessmentFrameworks und geben Sie einen Framework-Typ 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 GetAssessmentFramework, um die Framework-Details abzurufen. Geben Sie in der Anfrage die FrameworkID aus Schritt 1 an.

   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 den Befehl ListTagsForResource, um Tags für das Framework anzuzeigen. Geben Sie in der Anfrage die resourceArn aus Schritt 1 an.

Weitere Informationen zur Verwendung von Tags in Audit Manager finden Sie unter Markieren von AWS Audit Manager-Ressourcen.

Für weitere Informationen zu API-Befehlen klicken Sie auf einen der vorherigen Links in der AWS Audit ManagerAPI-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

Erstellen eines benutzerdefinierten Frameworks

Sie können über die Framework-Bibliothek in AWS Audit Manager auf Frameworks zugreifen und diese verwalten. Sie können benutzerdefinierte Frameworks erstellen, um Kontrollen so zu organisieren, dass sie Ihren spezifischen Anforderungen entsprechen.

Es gibt zwei Möglichkeiten, ein benutzerdefiniertes Framework zu erstellen. Sie können ein vorhandenes Framework anpassen oder ein ganz neues erstellen.

Themen

Erstellen eines neuen benutzerdefinierten Frameworks von Grund auf

Sie können benutzerdefinierte Frameworks in AWS Audit Manager verwenden, um Kontrollen so zu organisieren, dass sie Ihren spezifischen Anforderungen entsprechen. Sie können in der Framework-Bibliothek ein neues benutzerdefiniertes Framework ganz neu erstellen, indem Sie die folgenden Schritte ausführen.

Themen

Schritt 1: Framework-Details angeben

Geben Sie zunächst die Kontrollen an, die in Ihr benutzerdefiniertes Framework aufgenommen werden sollen.

Framework-Details spezifizieren

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek und dann Benutzerdefiniertes Framework erstellen aus.
3. Geben Sie unter Framework-Details einen Namen, einen Compliance-Standard oder eine Compliance-Vorschrift (optional) und eine Beschreibung für Ihr Framework (ebenfalls optional) ein. Geben Sie ein Schlüsselwort für Compliance-Standards oder Vorschriften wie PCI_DSS oder DSGVO ein, damit Sie dieses Keyword für die Suche nach Ihrem Framework verwenden können.
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 ihn als Suchkriterium verwenden, wenn Sie in der Framework-Bibliothek nach diesem Framework suchen. Weitere Informationen zu Tags in AWS Audit Manager finden Sie unter Markieren von AWS Audit Manager-Ressourcen.
5. Wählen Sie Weiter aus.

Schritt 2: Geben Sie die Kontrollen in den Kontrollsätzen 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. Um mehr Kontrollsätze hinzuzufügen, als die Konsole derzeit zulässt, verwenden Sie die API CreateAssessmentFramework, die Audit Manager bereitstellt.

Um Kontrollen in den Kontrollsätzen anzugeben

1. Geben Sie unter Name des Kontrollsatzes eine Bezeichnung ein.
2. Wählen Sie unter Neue Kontrolle zum Kontrollsatz hinzufügen die Option Kontrolltyp aus der Dropdownliste, um einen der beiden Kontrolltypen auszuwählen: Standar-dKontrollen oder Benutzerdefinierte Kontrollen. Standard-Kontrollen werden von Audit Manager bereitgestellt, benutzerdefinierte Kontrollen erstellen Sie.
3. Basierend auf der Option, die Sie im vorherigen Schritt ausgewählt haben, wird eine Liste mit Standard- oder benutzerdefinierten Kontrollen angezeigt. Sie können die Liste durchsuchen oder den Namen, die Konformität oder das Tag der Kontrolle in das Suchfeld eingeben. Wählen Sie eine oder mehrere Kontrollen und klicken Sie auf Zum Kontrollsatz hinzufügen, um sie zum Kontrollsatz hinzuzufügen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option Zum Kontrollsatz hinzufügen, um die Auswahl zu bestätigen.
5. Überprüfen Sie unter Ausgewählte Kontrollen im Kontrollsatz prüfen die Kontrollen, die in der Liste Ausgewählte Kontrollen angezeigt werden. Falls Sie weitere Kontrollen zu einem Kontrollsatz hinzufügen möchten, wiederholen Sie die Schritte 2 bis 4. Sie können unerwünschte Kontrollen aus dem Kontrollsatz entfernen, indem Sie ein oder mehrere Kontrollen auswählen und dann Kontrolle entfernen wählen.
6. Um dem Framework einen neuen Kontrollsatz hinzuzufügen, wählen Sie in der Fußzeile Kontrollsatz hinzufügen. Sie können unerwünschte Kontrollen entfernen, indem Sie Kontrollsatz entfernen wählen.
7. 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.

Was soll ich als Nächstes tun?

Nachdem Sie Ihr neues benutzerdefiniertes Framework erstellt haben, können Sie anhand Ihres Frameworks eine Bewertung erstellen. Weitere Informationen finden Sie unter Erstellen einer Bewertung.

Sie können auch ein benutzerdefiniertes Framework auf der Grundlage eines vorhandenen Frameworks erstellen. Weitere Informationen finden Sie unter Anpassen eines vorhandenen Frameworks.

Anweisungen zum Bearbeiten Ihres benutzerdefinierten Frameworks finden Sie unter Bearbeiten eines benutzerdefinierten Frameworks.

Anpassen eines vorhandenen Frameworks

Sie können benutzerdefinierte Frameworks in AWS Audit Manager verwenden, um Kontrollen so zu organisieren, dass sie Ihren spezifischen Anforderungen entsprechen. Anstatt ein benutzerdefiniertes Framework völlig neu zu erstellen, können Sie ein vorhandenes Framework als Vorlage verwenden und es anpassen. Somit verbleibt das vorhandene Framework in der Framework-Bibliothek, und ein neues benutzerdefiniertes Framework wird mit Ihren benutzerdefinierten Einstellungen erstellt.

Sie können jedes vorhandene Framework zur Anpassung auswählen. Es kann entweder ein Standard- oder ein benutzerdefiniertes Framework sein.

Wählen Sie in der Framework-Bibliothek in der Dropdownliste Benutzerdefiniertes Framework erstellen die Option Bestehendes Framework anpassen aus. Führen Sie die folgenden Schritte aus, um das Framework anzupassen.

Themen

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 Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich Framework-Bibliothek aus.

3. Wählen Sie das anzupassende Framework und aus der Dropdownliste Benutzerdefiniertes Framework erstellen die Option Bestehendes Framework anpassen aus.
4. Geben Sie im sich öffnenden Popup-Fenster einen Namen für das neue benutzerdefinierte Framework ein und wählen Sie Anpassen.
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 dieses Framework in der Framework-Bibliothek suchen. Weitere Informationen zu Tags in AWS Audit Manager finden Sie unter Markieren von AWS Audit Manager-Ressourcen.
7. Wählen Sie Weiter aus.

Schritt 2: Geben Sie die Kontrollen an, die zu den Kontrollsätzen hinzugefügt werden sollen

Die Kontrollsätze wurden aus dem ursprünglichen Framework übernommen. Passen Sie die aktuelle Konfiguration an, indem Sie nach Bedarf weitere Kontrollen hinzufügen oder vorhandene entfernen.

> **Note**
>
> Wenn Sie die AWS Audit Manager-Konsole verwenden, um ein Framework anzupassen, 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. Um mehr Kontrollsätze hinzuzufügen, als die Konsole derzeit zulässt, verwenden Sie die API CreateAssessmentFramework, die Audit Manager bereitstellt.

Um Kontrollen in den Kontrollsätzen anzugeben

1. Passen Sie unter Name des Kontrollsatzes den Namen nach Bedarf an.

2. Fügen Sie unter Neue Kontrolle zum Kontrollsatz hinzufügen eine neue Kontrolle hinzu, indem Sie in der Dropdownliste einen der beiden Kontrolltypen auswählen: Standard-Kontrollen oder Benutzerdefinierte Kontrollen.
3. Basierend auf der Option, die Sie im vorherigen Schritt ausgewählt haben, wird eine Liste mit Standard- oder benutzerdefinierten Kontrollen angezeigt. Sie können die Liste durchsuchen oder den Namen, die Konformität oder das Tag der Kontrolle in das Suchfeld eingeben oder die Tags zum Lokalisieren der Kontrollen hinzufügen. Wählen Sie eine oder mehrere Kontrollen und klicken Sie auf Zum Kontrollsatz hinzufügen, um sie zu diesem Kontrollsatz hinzuzufügen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option Zum Kontrollsatz hinzufügen, um die Auswahl zu bestätigen.
5. Überprüfen Sie unter Ausgewählte Kontrollen im Kontrollsatz prüfen die Kontrollen, die in der Liste Ausgewählte Kontrollen angezeigt werden. Falls Sie weitere Kontrollen zu einem Kontrollsatz hinzufügen möchten, wiederholen Sie die Schritte 2 bis 4. Sie können unerwünschte Kontrollen aus dem Kontrollsatz entfernen, indem Sie ein oder mehrere Kontrollen auswählen und dann Kontrolle entfernen wählen.
6. Um dem Framework einen neuen Kontrollsatz hinzuzufügen, wählen Sie in der Fußzeile Kontrollsatz hinzufügen. Sie können unerwünschte Kontrollen entfernen, indem Sie Kontrollsatz entfernen wählen.
7. 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.

Was soll ich als Nächstes tun?

Nachdem Sie Ihr neues benutzerdefiniertes Framework erstellt haben, können Sie anhand Ihres Frameworks eine Bewertung erstellen. Weitere Informationen finden Sie unter Erstellen einer Bewertung.

Anweisungen zum Bearbeiten Ihres benutzerdefinierten Frameworks finden Sie unter Bearbeiten eines benutzerdefinierten Frameworks.

Bearbeiten eines benutzerdefinierten Frameworks

Sie können benutzerdefinierte Frameworks in AWS Audit Manager verwenden, um Kontrollen so zu organisieren, sodass sie Ihren spezifischen Anforderungen entsprechen. Sie können die Framework-Bibliothek verwenden, um ein benutzerdefiniertes Framework zu finden und zu bearbeiten, indem Sie die folgenden Schritte ausführen.

Themen

Schritt 1: Framework-Details bearbeiten

Überprüfen und bearbeiten Sie zunächst die vorhandenen Framework-Details.

So bearbeiten Sie Framework-Details

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.
   - Alternativ können Sie ein benutzerdefiniertes Framework öffnen und oben rechts auf der Zusammenfassung der Bewertung Aktionen, 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 der Kontrollen im Kontrollsatz

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 API UpdateAssessmentFramework, um mehr Kontrollsätze hinzuzufügen, als die Konsole derzeit zulässt.

So bearbeiten Sie Kontrollen

1. Überprüfen und bearbeiten Sie unter Name des Kontrollsatzes nach Bedarf die Bezeichnung.
2. Unter Neue Kontrolle zum Kontrollsatz hinzufügen können Sie eine Kontrolle hinzufügen. Verwenden Sie die Dropdownliste, um einen der beiden Kontrolltypen auszuwählen: Standard-Kontrollen oder benutzerdefinierte Kontrollen.
3. Basierend auf der Option, die Sie im vorherigen Schritt ausgewählt haben, wird eine Tabelle mit Standard- oder benutzerdefinierten Kontrollen angezeigt. Sie können die Liste nach Kontrollsätzen durchsuchen. Oder Sie suchen durch Eingabe der Kontrolle, der Datenquelle oder des Tags nach den hinzuzufügenden Kontrollen. Wählen Sie eine oder mehrere Kontrollen und klicken Sie auf Zum Kontrollsatz hinzufügen, um sie zu diesem Kontrollsatz hinzuzufügen.
4. Wählen Sie im daraufhin angezeigten Popup-Fenster die Option Zum Kontrollsatz hinzufügen, um die Auswahl zu bestätigen.
5. Überprüfen und bearbeiten Sie unter Ausgewählte Kontrollen im Kontrollsatz prüfen die Kontrollen, die aktuell in der Liste Ausgewählte Kontrollen angezeigt werden. Falls Sie weitere Kontrollen zu einem Kontrollsatz hinzufügen möchten, wiederholen Sie die Schritte 2 bis 4. Entfernen Sie unerwünschte Kontrollen aus dem Kontrollsatz, indem Sie ein oder mehrere Kontrollen auswählen und dann Kontrolle entfernen wählen.
6. Um dem Framework einen neuen Kontrollsatz hinzuzufügen, wählen Sie in der Fußzeile Kontrollsatz hinzufügen. Entfernen Sie unerwünschte Kontrollen, indem Sie Kontrollsatz entfernen wählen.

7. Nach dem Hinzufügen von Kontrollen und Kontrollsätzen wählen Sie Weiter.

Schritt 3. Überprüfen und aktualisieren 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 Änderungen speichern aus.

Löschen eines benutzerdefinierten Frameworks

Sie können die Framework-Bibliothek verwenden, um ein unerwünschtes benutzerdefiniertes Framework zu finden und zu löschen. Sie können auch alle verfügbaren Frameworks mithilfe der Audit 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

So löschen Sie ein benutzerdefiniertes Framework (Konsole)

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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

So löschen Sie ein benutzerdefiniertes Framework (AWS CLI)

1. Identifizieren des benutzerdefinierten Frameworks, das Sie löschen möchten. Führen Sie dazu den Befehl list-assessment-frameworks aus und geben Sie `--framework-type` als `Custom` an.

   ```
   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 Befehl delete-assessment-framework aus und geben Sie den `--framework-id` des Frameworks an, das Sie löschen möchten.

   Ersetzen Sie im folgenden Beispiel den *`Platzhaltertext`* durch Ihre eigenen Informationen.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

So löschen Sie ein benutzerdefiniertes Framework (API)

1. Nutzen Sie den Befehl ListAssessmentFrameworks und geben Sie einen Framework-Typ als `Custom` an. Suchen Sie aus den Rückmeldungen das benutzerdefinierte Framework, das Sie löschen möchten, und notieren Sie sich die Framework-ID.
2. Verwenden Sie den Vorgang DeleteAssessmentFramework, um das Framework zu löschen. Verwenden Sie in der Anforderung den FrameworkID-Parameter, um das Framework anzugeben, das Sie löschen möchten.

Für weitere Informationen zu API-Befehlen klicken Sie auf einen der vorherigen Links in der AWS Audit ManagerAPI-Referenz. Dies beinhaltet Informationen zur Verwendung dieser Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

Freigeben eines benutzerdefinierten Frameworks

Sie können die Framework-FreigabeFeature von AWS Audit Manager verwenden, um die von Ihnen erstellten benutzerdefinierten Frameworks schnell zu replizieren. Sie können Ihre benutzerdefinierten Frameworks mit einem anderen AWS-Konto teilen oder Ihre Frameworks in einer anderen 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.

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-FreigabeFeature 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. Preisinformationen zu AWS Audit Manager finden Sie auf der Seite AWS Audit Manager-Preise.

> **Important**
>
> Sie dürfen ein benutzerdefiniertes Framework, das von einem Standard-Framework abgeleitet ist, nicht freigeben, wenn das Standard-Framework als nicht für die gemeinsame Nutzung durch AWS infrage kommt, es sei denn, Sie haben vom Verantwortlichen 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.

In den folgenden Abschnitten dieses Handbuchs werden die wichtigen Dinge beschrieben, die Sie über die gemeinsame Nutzung von Frameworks wissen sollten. Sie enthalten auch Anweisungen,

wie Sie Ihre benutzerdefinierten Frameworks teilen und auf Anfragen zur gemeinsamen Nutzung antworten können.

Themen

> **Tip**
>
> Wenn Sie mit benutzerdefinierten Frameworks von Audit Manager und deren Erstellung nicht vertraut sind, finden Sie auf der Seite Erstellen eines benutzerdefinierten Frameworks in diesem Handbuch weitere Informationen.

Framework-Konzepte und -Terminologie freigeben

Wenn Sie sich mit den folgenden Schlüsselkonzepten vertraut machen, können Sie mehr aus der Feature zur gemeinsamen Nutzung von AWS Audit Manager benutzerdefinierten Frameworks herausholen.

Absender

Dies ist der Ersteller einer Freigabeanfrage und das AWS-Konto, wo das benutzerdefinierte Framework vorliegt. Absender können benutzerdefinierte Frameworks mit jedem AWS-Konto teilen. Oder sie replizieren ein benutzerdefiniertes Framework für jede unterstützte AWS-Region unter ihrem eigenen Konto.

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 jedoch keine benutzerdefinierten Frameworks mit einem AWS Organizations-Verwaltungskonto freigeben.

Voraussetzungen für Frameworks

Sie können nur benutzerdefinierte Frameworks freigeben. Standardmäßig sind Standard-Frameworks bereits in allen AWS-Konten und AWS-Regionen vorhanden, bei denen AWS Audit Manager aktiviert ist. 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 AWS Audit Manager angebotenen Standard-Frameworks 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 freigeben, wenn das Standard-Framework als nicht für die gemeinsame Nutzung durch AWS infrage kommt, es sei denn, Sie haben vom Verantwortlichen 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 Australian Cyber Security Centre (ACSC)	 Ja

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
Handbuch zur Informationssicherheit des Australian Cyber Security Centre (ACSC)	 Ja
AWS Audit Manager Beispiel für ein Framework	 Ja
AWS Control Tower-Leitlinien	 Ja
AWS Best Practice-Framework für generative KI v1	 Ja
AWS License Manager	 Ja
AWS Foundational Security Best Practices	 Ja
Betriebliche Best Practices bei AWS	 Ja
AWS Well-Architected Framework	 Ja

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
Canadian Centre for Cyber Security - Medium	 Nein
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 1	 Nein
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 1 und 2	 Nein
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0, Level 1	 Nein
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0, Level 1 und 2	 Nein
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1	 Nein
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1 und 2	 Nein
CIS Controls v7.1 IG1	 Ja

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
CIS Controls v8 IG1	 Nein
FedRAMP Moderate Baseline	 Ja
DSGVO	 Ja
Gramm-Leach-Bliley Act (GLBA)	 Ja
GxP 21 CFR Teil 11	 Ja
GxP EU Anhang 11	 Ja
HIPAA-Sicherheitsvorschriften 2003	 Ja
HIPAA Final Omnibus Sicherheitsvorschriften 2013	 Ja

Name des Standard-Frameworks	Benutzerdefinierte Versionen, die geteilt werden können
ISO/IEC 27001:2013 Anhang A	 Nein
NIST 800-53 (5. Überarb.) Low-Moderate-High	 Ja
NIST-Cybersecurity-Framework, Version 1.1	 Ja
NIST SP 800-171 (2. Überarb.)	 Ja
PCI DSS v3.2.1	 Nein
PCI DSS v4.0	 Nein
SOC 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.

- Aktiv: Dies weist auf eine Freigabeanfrage hin, die erfolgreich an den Empfänger gesendet wurde und eine Antwort offen ist.
- Läuft ab – Dies weist auf eine Freigabeanfrage hin, die innerhalb der nächsten 30 Tage abläuft.
- Geteilt – Dies weist auf eine Freigabeanfrage hin, die der Empfänger akzeptiert hat.
- Inaktiv – Dies weist auf eine Freigabeanfrage hin, die widerrufen, 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 an den Empfänger gesendet werden konnte.

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 Freigabeanforderung erstellen, speichert Audit Manager einen Snapshot Ihres benutzerdefinierten Frameworks in der AWS-Region USA Ost (Nord-Virginia). Audit Manager speichert auch eine Sicherungskopie desselben Snapshots in der AWS-Region USA West (Oregon).

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 seinen AWS-Konto Unterordner der AWS-Region repliziert, der in der Freigabeanfrage angegeben wurde.

Versionsverwaltung des freigegebenen Frameworks

Wird ein benutzerdefiniertes Framework gemeinsam genutzt, erstellt Audit Manager eine unabhängige Kopie dieses Frameworks nach Angabe von AWS-Konto und 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 AWS-Konto teilen 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 AWS-Region löschen, 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.

Senden einer Freigabeanforderung für ein benutzerdefiniertes Framework

In diesem Tutorial wird beschrieben, wie Sie Ihre benutzerdefinierten Frameworks über AWS-Konten und AWS-Regionen gemeinsam nutzen können.

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.

Dieses Tutorial erklärt die folgenden Schritte:

1. Framework zum Freigeben auswählen: Durchsuchen Sie die Framework-Bibliothek, um das benutzerdefinierte Framework zu finden, das Sie teilen möchten.
2. Eine Freigabeanfrage senden: Geben Sie einen Empfänger an und senden Sie ihm eine Freigabeanfrage für das benutzerdefinierte Framework.
3. Gesendete Anfragen anzeigen: Sehen Sie sich den Verlauf Ihrer Freigabeanfragen an und überprüfen Sie den Status Ihrer gesendeten Anfragen.
4. (Optional) die Freigabeanfrage widerrufen: Widerrufen Sie die Freigabeanfrage, bevor sie abläuft.

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 bereits AWS Audit Manager im Bereich AWS-Region aktiviert, in dem Sie das benutzerdefinierte Framework freigeben möchten.
- Der Empfänger ist kein AWS Organizations-Verwaltungskonto.

> **Tip**
>
> Notieren Sie sich zuvor die AWS-Konto-ID, mit der Sie Ihr benutzerdefiniertes Framework teilen möchten. Dies kann Ihre eigene Konto-ID sein, wenn Sie das Framework auf eine andere AWS-Region unter Ihrem Konto replizieren möchten. Diese Informationen sind für den zweiten Schritt des Tutorials erforderlich.

> **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.

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.

Ihre verfügbaren benutzerdefinierten Frameworks aufrufen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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 Kontrollen verfügt, die benutzerdefinierte AWS Config-Regeln als Datenquelle verwenden, empfehlen wir Ihnen, den Empfänger zu informieren. Der Empfänger kann dann dieselben AWS Config-Regeln in seiner AWS Config-Instance erstellen und aktivieren. Weitere Informationen finden Sie unter Mein freigegebenes Framework verfügt über Kontrollen, 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 AWS-Konto teilen möchten, wird das Framework nur auf die angegebene AWS-Region repliziert. Nachdem der Empfänger die Freigabeanfrage akzeptiert hat, kann er das Framework nach Bedarf regionsübergreifend replizieren.
> - Wenn benutzerdefinierte Frameworks über AWS-Regionen freigegeben werden, kann es bis zu 10 Minuten dauern, bis die Freigabeanforderung bearbeitet wird. 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.

   - Aktiv – Dieser Filter zeigt Freigabeanfrage an, bei denen noch eine Antwort vom Empfänger aussteht.
   - Freigegeben – Dieser Filter zeigt Freigabeanfragen an, die vom Empfänger akzeptiert wurden. Das freigegebene, benutzerdefinierte Framework ist jetzt in der Framework-Bibliothek des Empfängers vorhanden.
   - Inaktiv – Dieser Filter weist auf eine Freigabeanfrage hin, die widerrufen, abgelehnt oder abgelaufen ist, bevor der Empfänger Maßnahmen ergriffen hat. Wählen Sie die Option Inaktiv aus, um weitere Details anzuzeigen.
   - Läuft ab – Dieser Filter zeigt Freigabeanfragen an, die in den nächsten 30 Tagen ablaufen.

- Fehlgeschlagen – Dieser Filter zeigt die Freigabeanfragen an, die nicht an den Empfänger gesendet werden konnte. 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.
> Informationen dazu, wie Sie vorgehen können, wenn ein Fehler auftritt, finden Sie unter Fehlerbehebung bei Freigabeanfragen.

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.

Wenn Frameworks über AWS-Regionen freigegeben werden, kann es bis zu 10 Minuten dauern, bis die Freigabeanforderung bearbeitet wird. Nach dem Widerruf einer regionsübergreifenden Freigabeanfrage empfehlen wir Ihnen, später zu prüfen, ob die Freigabeanfrage erfolgreich widerrufen wurde.

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. Wählen Sie von hier aus Aktionen und dann Benutzerdefiniertes Framework freigeben.

- Wählen Sie alternativ das benutzerdefinierte 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. Prüfen Sie den im Dialogfeld angezeigten Hinweis, geben Sie **`agree`** ein und wählen Sie Zustimmen, um fortzufahren.
3. 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.
4. Wählen Sie Freigeben aus, um die Freigabeanfrage erneut zu senden und zu aktualisieren.

Fehlerbehebung bei Freigabeanfragen

Lösungen zu Problemen, die beim Freigeben eines benutzerdefinierten Frameworks auftreten können, finden Sie Behebung von Problemen beim Teilen von Frameworks im Abschnitt Fehlerbehebung dieses Handbuchs.

Reaktion auf Freigabeanfragen

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.

Dieses Tutorial erklärt die folgenden Schritte:

1. Überprüfen der Benachrichtigungen über Freigabeanfragen – Überprüfen der Liste von Freigabeanfragen, die aktiv sind und bald ablaufen.

2. Ergreifen von Maßnahmen in Bezug auf Freigabeanfragen – Freigabeanfrage für das benutzerdefinierte Framework an- oder ablehnen.
3. Freigabeanfragen ansehen, die Sie von anderen erhalten haben – Ansehen des Verlaufs Ihrer Freigabeanfragen.

Voraussetzungen

Machen Sie sich zunächst in Audit Manager mit Framework-Konzepte und -Terminologie freigeben vertraut.

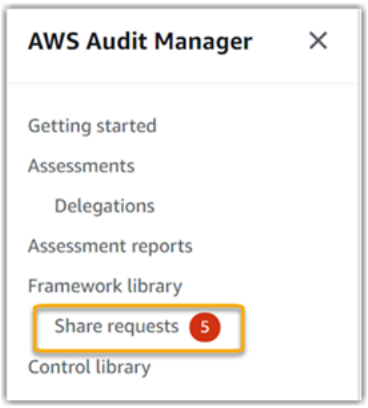
Schritt 1: Überprüfen Sie Ihre erhaltenen Benachrichtigungen über Anfragen

Überprüfen Sie zunächst Ihre Benachrichtigungen zu Freigabeanfragen. Hinter der Registerkarte Empfangene Anfragen verbirgt sich eine Liste der von AWS-Konten erhaltenen Freigabeanfragen. 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.

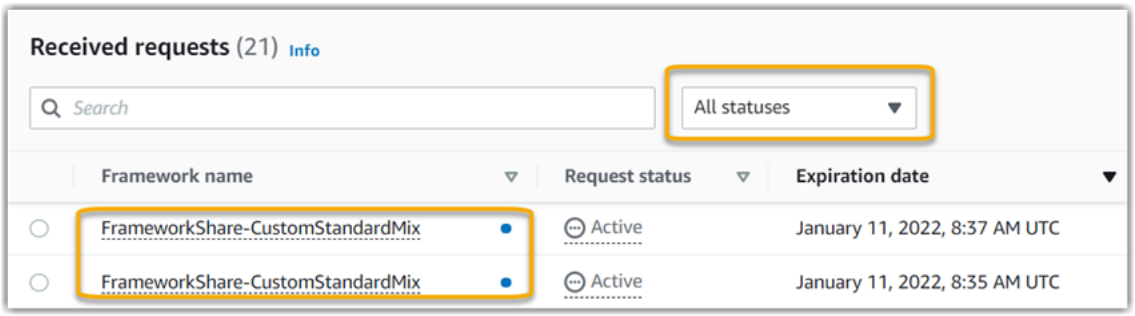
Eingegangene Anfragen anzeigen

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
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.

> **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.

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.

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 Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich Freigabeanfragen aus.
3. Wählen Sie die Registerkarte Empfangene Anfragen.
4. Wählen Sie die Dropdownliste Alle Status und einen der folgenden Filter.

   - Aktiv – Dieser Filter zeigt Freigabeanfrage an, die Sie noch nicht akzeptiert oder abgelehnt haben.
   - Läuft ab – Dieser Filter zeigt Freigabeanfragen an, die in den nächsten 30 Tagen ablaufen.
   - Freigegeben Dieser Filter zeigt Freigabeanfragen an, die Sie akzeptiert haben. Das freigegebene Framework ist jetzt in Ihrer Framework-Bibliothek verfügbar.
   - Inaktiv – Dieser Filter weist auf eine Freigabeanfrage hin, die abgelehnt oder abgelaufen ist.
   - Fehlgeschlagen Dieser Filter zeigt die Freigabeanfragen an, die nicht erfolgreich gesendet wurden. Wählen Sie die Option Fehlgeschlagen, um weitere Details anzuzeigen.

Was soll ich als Nächstes tun?

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 finden Sie unter Erstellen einer Bewertung. Anweisungen zum Bearbeiten Ihres neuen benutzerdefinierten Frameworks finden Sie unter Benutzerdefiniertes Framework bearbeiten.

Löschen von Freigabeanfragen

Sie können Freigabeanfragen löschen, die nicht mehr gewünscht oder benötigt werden.

> **Note**
>
> Sie können keine Freigabeanfragen löschen, die den Status Aktiv oder Replizieren haben. Wenn Sie eine Freigabeanfrage löschen, wird nur die Anfrage selbst gelöscht. Das freigegebene Framework selbst verbleibt in Ihrer Framework-Bibliothek.

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.

Unterstützte Frameworks in AWS Audit Manager

AWS Audit Manager bietet die folgenden Standard-Frameworks. Diese vorgefertigten Frameworks basieren auf Best Practices von AWS für verschiedene Compliance-Standards und Vorschriften. Sie können diese Frameworks bei der Vorbereitung Ihres Audits verwenden.

Themen

- Essential Eight des Australian Cyber Security Centre (ACSC)
- Handbuch zur Informationssicherheit des Australian Cyber Security Centre (ACSC)
- AWS Audit Manager Beispiel für ein Framework
- AWS Control Tower-Leitlinien

- AWS-Best Practices-Framework für generative KI v1
- AWS License Manager
- Bewährte AWS-Methoden für grundlegende Sicherheit
- Betriebliche Best Practices bei AWS
- AWS Well-Architected Tool
- Kontrollprofil für mittelgroße Clouds des Canadian Centre for Cyber Security
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0
- CIS Controls v7.1 Implementierungsgruppe 1
- CIS Controls v8 Implementierungsgruppe 1
- FedRAMP Moderate Baseline
- Datenschutz-Grundverordnung (DSGVO)
- Gramm-Leach-Bliley Act (GLBA)
- GxP 21 CFR Teil 11
- GxP EU Anhang 11
- Health Insurance Portability and Accountability Act (HIPAA) Sicherheitsvorschriften 2003
- Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Sicherheitsvorschriften 2013
- ISO/IEC 27001:2013 Anhang A
- NIST 800-53 (5. Überarb.) Low-Moderate-High
- NIST-Cybersecurity-Framework, Version 1.1
- NIST SP 800-171 (2. Überarbeitung)
- PCI DSS v3.2.1
- PCI DSS V4.0
- SOC 2

Essential Eight des Australian Cyber Security Centre (ACSC)

Zur Unterstützung bei der Audit-Vorbereitung bietet AWS Audit Manager ein vorgefertigtes Standard-Framework, das die Bewertungen für das Essential Eight-Framework strukturiert und automatisiert.

Themen

Was ist Essential Eight des Australian Cyber Security Centre (ACSC)?

Das Australian Cyber Security Centre (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).

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Essential Eight-Standard-Framework in AWS Audit Manager verwenden, 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	AWS-Services im Umfang
Essential Eight	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_EssentialEight.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, ob Ihre Systeme den Essential Eight-Kontrollen entsprechen. Darüber hinaus garantieren sie nicht, dass Sie ein Essential Eight-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden das Essential Eight-Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Essential Eight-Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für

dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung. Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere Ressourcen zu Essential Eight

- ACSC Essential Eight

Handbuch zur Informationssicherheit des Australian Cyber Security Centre (ACSC)

Zur Unterstützung bei der Audit-Vorbereitung gilt AWS Audit Manager als vorgefertigtes Standard-Framework, das die Bewertungen für das Framework-Handbuch ACSC Information Security strukturiert und automatisiert.

Themen

- Was ist das Handbuch zur Informationssicherheit (ISM) des Australian Cyber Security Centre (ACSC)?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere Quellen zum ACSC-Handbuch zur Informationssicherheit (ISM)

Was ist das Handbuch zur Informationssicherheit (ISM) des Australian Cyber Security Centre (ACSC)?

Das Australian Cyber Security Centre (ACSC) ist die führende Behörde der australischen Regierung für Cybersicherheit. Das ACSC erstellt das Handbuch für Informationssicherheit (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 Australian Cyber Security Centre unter einer Creative Commons Attribution 4.0 International License bereitgestellt. Informationen zum Urheberrecht finden Sie unter ACSC | Copyright. © Commonwealth of Australia 2022.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Standard-Framework ACSC Information Security Manual in AWS Audit Manager verwenden, um sich bei der Vorbereitung auf Audits Unterstützung zu holen. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den Anforderungen des ACSC-Handbuchs zur Informationssicherheit in Kontrollgruppen eingeteilt. 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 ACSC-Handbuch für Informationssicherheit 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-Services im Umfang
ACSC-Handbuch zur Informationssicherheit (ISM)	45	396	22	• Amazon Elastic Compute Cloud

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
				• AWS Config • AWS Identity and Access Management

> **Tip**
>
> Um die AWS Config Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, ob Ihre Systeme den ACSC-Kontrollen zur Informationssicherheit entsprechen. Darüber hinaus garantieren sie nicht, dass Sie ein ACSC-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden das Framework ACSC-Handbuch zur Informationssicherheit unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Frameworks ACSC-Handbuch zur Informationssicherheit. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung. Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen

Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere Quellen zum ACSC-Handbuch zur Informationssicherheit (ISM)

- ACSC-Handbuch zur Informationssicherheit (ISM)

AWS Audit Manager Beispiel für ein Framework

AWS Audit Manager bietet ein Beispiel-Framework, um Ihnen den Einstieg in Ihre Audit-Vorbereitung zu erleichtern.

Themen

- Was ist das AWS Audit Manager-Beispiel-Framework?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Was ist das AWS Audit Manager-Beispiel-Framework?

Das AWS Audit Manager-Beispiel-Framework ist ein einfaches Framework, das Sie für den Einstieg in Audit Manager verwenden können. Einige der anderen vorgefertigten Frameworks, die Audit Manager bietet, sind im Vergleich viel umfangreicher und enthalten zahlreiche Kontrollen. Wenn Sie das Beispiel-Framework anstelle dieser umfassenderen Frameworks verwenden, können Sie Beispiele für ein Framework einfacher überprüfen und untersuchen. Die Kontrollen in diesem Framework basieren auf einer Reihe von AWS Config- und AWS-API-Aufrufen.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können dieses Framework verwenden, um sich Ihren Einstieg in AWS Audit Manager zu erleichtern. Sie können dieses Framework und seine Kontrollen auch anpassen, um interne Audits mit spezifischen Anforderungen zu unterstützen.

Mit dem AWS Audit Manager-Beispiel-Framework als Vorlage können Sie eine Audit Manager-Bewertung 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. Als Nächstes erhebt es die relevanten Beweise und fügt sie dann den Kontrollen in Ihrer Bewertung bei.

Die Details zum AWS Audit Manager-Beispiel-Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
AWS Audit Manager Beispiel für ein Framework	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des AWS Audit Manager-Beispiel-Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

AWS Control Tower-Leitlinien

AWS Audit Manager bietet ein AWS Control Tower Leitlinien-Framework, das Sie bei der Vorbereitung Ihrer Audits unterstützt.

Themen

- Was ist AWS Control Tower?

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 Umgebung mit mehreren AWS-Konten verbunden sind, zurechtfinden können.

Mithilfe von AWS Control Tower können Sie mit wenigen Klicks neue AWS-Konten bereitstellen, die Ihren unternehmens- oder betriebsweiten Richtlinien entsprechen. AWS Control Tower erstellt in Ihrem Namen eine Orchestrierungsebene, die die Funktionen mehrerer anderer AWS-Dienste kombiniert und integriert. Zu diesen Diensten gehören AWS Organizations, AWS IAM Identity Center und der AWS-Service-Katalog. 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-Leitlinien-Framework enthält alles über die AWS-Config-Regeln, was auf Leitlinien von AWS Control Tower basiert.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

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 Kontrollen sind nach AWS-Config-Regeln gruppiert, die auf Leitlinien von AWS Control Tower basieren. 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 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 Leitlinien-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 AWS Control Tower-Leitlinien-Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
AWS Control Tower-Leitlinien	14	0	5	AWS Config

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, ob Ihre Systeme mit AWS Control Tower-Leitlinien konform sind. Darüber hinaus können sie nicht garantieren, dass Sie ein Audit bestehen.

Sie finden das AWS Control Tower-Leitlinien-Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen oder zu aktualisieren, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen der AWS Control Tower-Leitlinien. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere AWS Control Tower-Quellen

- AWS Control Tower-Serviceseite
- AWS Control Tower-Benutzerhandbuch

AWS-Best Practices-Framework für generative KI v1

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 anhand der von AWS empfohlenen Best Practices Featureiert.

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 Basismodelle (Foundation Models, FMs) und große Sprachmodelle (Large Language Models, 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.

Themen

- Was sind AWS Best Practices für generative KI für Amazon Bedrock?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Manuelles Überprüfen von Eingabeaufforderungen in Amazon Bedrock
- Weitere -Quellen

Was sind AWS Best Practices für 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 verpflichtet sich, 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 das AWSBest-Practices-Framework für generative KI v1 entwickelt. Dieses Framework bietet Ihnen ein speziell entwickeltes Tool zur Überwachung und Verbesserung der Kontrolle Ihrer generativen KI-Projekte auf Amazon Bedrock. 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-, Compliance- und Sicherheitsexperten bei AWS sowie mit Input von Deloitte entwickelt. Jede automatisierte Kontrolle 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 Featureiert
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-Best-Practices-Framework für generative KI 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 einer Ende-zu-Ende-Verschlüsselung für Eingabe- und Ausgabedaten der KI-Modelle gemäß den branchenüblichen Mindeststandards (Schutz)

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

> **Note**
>
> - Wenn Sie ein Amazon Bedrock-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 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 den Audit Manager Datenverschlüsselung-Einstellungen speichern.

- Dieses Framework verwendet den Amazon Bedrock-Befehl ListCustomModels, um Beweise über die Verwendung Ihres benutzerdefinierten Modells zu generieren. Dieser API-Befehl wird derzeit nur in den AWS-Regionen 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 bezüglich Ihrer Nutzung generativer KI auf Amazon Bedrock 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 Best-Practices-Framework für AWS-generative KI 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 Kontrollsätze	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	AWS-Services im Umfang
AWS-Best Practices-Framework für generative KI v1	8	34 vollautomatisiert 18 teilautomatisiert	58	• Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Weitere Informationen zu automatisierten und manuellen Kontrollen finden Sie unter Konzepte und Terminologie in Audit Manager. Hier finden Sie ein Beispiel dafür, wann es empfohlen wird, einer teilautomatisierten Kontrolle manuelle Beweise hinzuzufügen.
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_AWSGenerative-AI-Best-Practices.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, ob Ihre Systeme den Best Practices für generative KI entsprechen. Darüber hinaus geben sie keine Garantie, dass ein Audit über Ihre generative KI-Nutzung bestanden wird. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung. Anweisungen zum Erstellen einer änderbaren Kopie dieses Frameworks zur Unterstützung Ihrer spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

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 die Liste mit Eingabeaufforderungen erstellt haben, testen Sie jede einzelne mit dem von Amazon Bedrock bereitgestellten Vorgang invokeModel. 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 wird von AWS weder entwickelt noch unterstützt. 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 Befehl AWS CLI 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 Sie mit der AWS-CLI und der Eingabeaufforderung *„Story of Two Dogs“* und des *Anthropic Claude V2*Modells Text generieren. Im Beispiel werden bis zu *300* Token als Antwort zurückgegeben und in der Datei *invoke-model-output.txt* gespeichert:

```
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-Canary zur Überwachung Ihrer Modellantworten verwenden. Mit dieser Lösung können Sie das Ergebnis `InvokeModel` anhand einer Liste vordefinierter Eingabeaufforderungen überprüfen und dann CloudWatch verwenden, um das Verhalten des Modells für diese Eingabeaufforderungen zu 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-Feature ausführen. Wenn Sie sich für diese Lösung entscheiden, müssen Sie zuerst eine Lambda-Feature erstellen.

Beispielaufforderungen

Sie können diese Beispielaufforderungen als Vorlage verwenden, um die Antworten Ihres Modells zu testen. Ersetzen Sie in den folgenden Beispielen den *Platzhaltertext* durch Ihre eigenen Daten, um Ihre spezifischen Testanwendungsfälle widerzuspiegeln.

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, ******"
```

Weitere -Quellen

- Amazon Bedrock
- Amazon Bedrock 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 AWS License Manager-Leitlinien-Framework, das Sie bei der Vorbereitung Ihres Audits unterstützt.

Themen

- Was ist AWS License Manager?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere AWS License Manager-Quellen

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 On-Premises 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.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

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 Details zum AWS License Manager-Framework sind im Folgenden aufgeführt:

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

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

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des AWS License Manager-Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere AWS License Manager-Quellen

License Manager-Links

- AWS License Manager-Serviceseite
- 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-APIs auf:

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

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

Zum Beispiel: Nehmen wir an, Sie verwenden zwei lizenzierte Produkte (SQL Dienst 2017 und Oracle Database Enterprise Edition). Zunächst ruft die `GetLicenseManagerSummary`-Aktivität die API ListLicenseConfigurations auf, die Details zu den Lizenzkonfigurationen in Ihrem Konto bereitstellt. Als Nächstes werden zusätzliche Kontextdaten für jede Lizenzkonfiguration hinzugefügt, indem ListUsageForLicenseConfiguration und ListAssociationsForLicenseConfiguration aufgerufen werden. 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.

Bewährte AWS-Methoden für grundlegende Sicherheit

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

Themen

- Was bedeutet der AWS-Best Practices-Standard für grundlegende Sicherheit?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere AWS-Quellen zu den Best Practices für grundlegende Sicherheit

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

Der AWS Foundational Security Best Practices-Standard ist eine Reihe von Steuerelementen, die erkennen, wann Ihre bereitgestellten Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.

Dieser Standard ermöglicht es Ihnen, alle Ihre AWS-Konten und Workloads kontinuierlich auszuwerten, um Bereiche mit Abweichungen von den Best Practices schnell zu identifizieren. 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 SicherheitsFeature widerspiegelt, auf die die Kontrolle angewendet wird. Weitere Informationen finden Sie in den Kontrollkategorien im AWS Security Hub-Benutzerhandbuch.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das AWS Best Practices-Framework für grundlegende Sicherheit 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 für grundlegende Sicherheit 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 Ihrer AWS-Konten und Services. Dies geschieht auf der Grundlage der Kontrollen, die im AWS-Best-Practices-Framework für grundlegende Sicherheit 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 AWS-Best-Practices-Frameworks für grundlegende Sicherheit lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
Bewährte AWS-Methoden für grundlegende Sicherheit	154	0	29	AWS Security Hub

Die Kontrollen in diesem AWS Audit Manager-Framework sind nicht zur Überprüfung gedacht, ob Ihre Systeme den AWS-Best Practices für grundlegende Sicherheit entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein AWS-Audit mit den Best Practices für grundlegende Sicherheit bestehen.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen der AWS-Best Practices für grundlegende Sicherheit. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere AWS-Quellen zu den Best Practices für grundlegende Sicherheit

- AWSErfahren Sie mehr über den Best Practices-Standard für grundlegende Sicherheit im AWS Security Hub-Benutzerhandbuch.
- Kategorien von Kontrollen im AWS Security Hub-Benutzerhandbuch

Betriebliche Best Practices bei AWS

AWS Audit Manager bietet ein vorgefertigtes Framework für Betriebliches Best Practices (Operational Best Practices, OBP) bei AWS, das Sie bei der Audit-Vorbereitung unterstützt. Dieses Framework bietet eine Untergruppe von Kontrollen aus dem Best Practices-Standard für grundlegende Sicherheit von AWS. Diese Kontrollen dienen als grundlegende Prüfungen, um festzustellen, wann Ihre bereitgestellten Konten und Ressourcen von den bewährten Sicherheitsmethoden abweichen.

Themen

- Was bedeutet der AWS-Best Practices-Standard für grundlegende Sicherheit?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere AWS OBP-Ressourcen

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

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 SicherheitsFeature widerspiegelt, auf die die Kontrolle angewendet wird. Weitere Informationen finden Sie in den Kontrollkategorien im AWS Security Hub-Benutzerhandbuch.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework für Betriebliche Best Practices von AWSverwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den Anforderungen der Betrieblichen Best Practices von AWS 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 Ihrer AWS-Konten und Services. Dies geschieht auf der Grundlage der Kontrollen, die im Framework für Betriebliche Best Practices von AWS 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 Frameworks für Betriebliche Best Practices von AWS lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
Betriebliche Best Practices bei AWS	52	0	20	AWS Security Hub

Die Kontrollen in diesem Framework dienen nicht zur Überprüfung, ob Ihre Systeme dem Framework für Betriebliche Best Practices von AWS entsprechen. Darüber hinaus wird nicht garantiert, dass Sie ein AWS-Audit mit den Betrieblichen Best Practices bestehen.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen der Betrieblichen Best Practices von AWS. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere AWS OBP-Ressourcen

- AWSErfahren Sie mehr über den Best Practices-Standard für grundlegende Sicherheit im AWS Security Hub-Benutzerhandbuch.
- Kategorien von Kontrollen im AWS Security Hub-Benutzerhandbuch

AWS Well-Architected Tool

AWS Audit Manager bietet ein vorgefertigtes Framework, das Bewertungen für das Well-Architected Framework von AWS strukturiert und automatisiert, und zwar basierend auf AWS-Best Practices.

Themen

Was ist AWS Well-Architected?

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.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

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 Kontrollen, 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 des AWS Well-Architected Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
AWS Well-Architected Framework	16	0	2	AWS Config

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip herunter.

Die Kontrollen in diesem Framework dienen nicht zur Überprüfung, ob Ihre Systeme konform sind. Darüber hinaus garantieren sie nicht, dass Sie ein Audit bestehen, das mit dem AWS Well-Architected Framework verbunden ist.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des AWS Well-Architected Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für

dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere AWS Well-Architected-Ressourcen

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

Kontrollprofil für mittelgroße Clouds des Canadian Centre for Cyber Security

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das Bewertungen für das Canadian Centre for Cyber Security strukturiert und automatisiert.

Themen

- Was ist das Canadian Centre for Cyber Security?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Was ist das Canadian Centre for Cyber Security?

Das Canadian Centre for Cyber Security (kanadisches Zentrum für Cybersicherheit, CCCS) ist Kanadas maßgebliche Quelle für Beratung, Dienstleistungen und Unterstützung durch Cybersicherheitsexperten. 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

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das AWS Audit Manager-Framework für das Kontrollprofil für mittelgroße Clouds 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 Vorlage verwenden, können Sie eine Bewertung durch den Audit Manager erstellen und mit der Erfassung von Beweisen beginnen, die für ein CCCS-Kontrollprofil für mittelgroße Clouds relevant sind. In Ihrer Bewertung können Sie die AWS-Konten und Services angeben, die Sie in den Umfang Ihres Audits 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 Framework CCCS-Kontrollprofil für mittelgroße Clouds 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-Services im Umfang
Canadian Centre for Cyber Security - Medium	206	396	165	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, ob Ihre Systeme dem CCCS-Kontrollprofil für mittelgroße Clouds entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein CCCS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Frameworks des Canadian Centre for Cyber Security – Mittelgroßes Framework. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0

AWS Audit Manager bietet zwei vorgefertigte Frameworks, die den CIS AWS Foundations Benchmark v1.2.0 unterstützen:

- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 1
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 1 und 2

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version 1.3.0 unterstützen, finden Sie unterCIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0.
> - Informationen zu den Audit Manager-Frameworks, die Version 1.4.0 unterstützen, finden Sie unterCIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0.

Themen

- Was ist CIS?
- Verwenden Sie diese Frameworks zur Unterstützung Ihrer Audit-Vorbereitung

- Weitere CIS-Quellen

Was ist CIS?

Das Center for Internet Security (CIS) ist eine gemeinnützige Organisation, die den CIS AWS Foundations Benchmark entwickelt hat. Dieser Benchmark dient als Sammlung von Best Practices zur Sicherheitskonfiguration für AWS. Diese branchenweit anerkannten Best Practices gehen über die bereits verfügbaren allgemeinen Sicherheitsrichtlinien hinaus, da sie Ihnen klare, schrittweise Implementierungs- und Bewertungsverfahren bieten.

Weitere Informationen finden Sie in den CISAWS Foundations Benchmark Blog-Posts in 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 Amazon Web Services Foundations Benchmark v1.2.0 – 1.13 stellt 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 AWS-Umgebung eingerichtet werden kann.
- CIS Controls gilt unternehmensweit. Sie sind nicht nur für ein Produkt eines Anbieters spezifisch.

  Beispiel: CIS Controls v7.1 – Sub-Control 4.5 verwenden 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).

Verwenden Sie diese Frameworks zur Unterstützung Ihrer Audit-Vorbereitung

Sie können die CIS AWS Foundations Benchmark v1.2 Frameworks verwendenAWS 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	AWS-Services im Umfang
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0, Level 1	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
CIS Benchmark for CIS Amazon Web Services	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
Foundations Benchmark, v1.2.0, Level 1 und 2				• AWS Identity and Access Management • AWS Security Hub

Die Kontrollen in diesen Frameworks dienen nicht zur Überprüfung, ob Ihre Systeme dem CIS-Standard entsprechen. Darüber hinaus garantieren sie nicht, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden diese Frameworks unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit-Manager-Konsole verwenden, um eine Bewertung anhand dieser Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Geltungsbereich standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des CIS-Benchmarks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieser Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieser Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Voraussetzungen für die Verwendung dieser Frameworks

Viele Kontrollen in den AWS CIS-Frameworks Foundations Benchmark v1.2 verwenden AWS Config als Datenquellentyp. Um diese Kontrollen zu unterstützen, müssen Sie sie AWS-Region für alle AWS

Configaktivieren, in denen Sie Audit Manager aktiviert haben. Sie müssen außerdem sicherstellen, dass bestimmte AWS Config-Regeln aktiviert und diese korrekt konfiguriert sind.

Die folgenden AWS Config-Regeln und -Parameter sind erforderlich, um die korrekten Beweise zu erhalten 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 AWS Config-Regel	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
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.

Erforderliche AWS Config-Regel	Erforderliche Parameter
	• 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: Boolesch • Standard: True • Passwortanforderung: mindestens ein Kleinbuchstabe
IAM_PASSWORD_POLICY	**`RequireNumbers`** (Optional) • Verlangen Sie mindestens eine Zahl im Passwort. • Typ: Boolesch • Standard: True • Compliance-Anforderungen: mindestens eine Ziffer
IAM_PASSWORD_POLICY	**`RequireSymbols`** (Optional) • Verlangen Sie mindestens ein Symbol im Passwort. • Typ: Boolesch • Standard: True • Compliance-Anforderung: mindestens ein Sonderzeichen

Erforderliche AWS Config-Regel	Erforderliche Parameter
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (Optional) • Verlangen Sie mindestens einen Großbuchstaben im Passwort. • Typ: Boolesch • Standard: True • Compliance-Anforderung: mindestens ein Großbuchstabe
IAM_POLICY_IN_USE	**`policyARN`** • Ein zu überprüfender IAM-Richtlinien-ARN. • Typ: Zeichenfolge • Compliance-Anforderung: erstellt eine IAM-Rolle für die Verwaltung von Vorfällen bei 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

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

Erforderliche AWS Config-Regel	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

Erforderliche AWS Config-Regel	Erforderliche Parameter
	`blockedPort5` (Optional) • Blockierte TCP-Port-Nummer. • 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 des S3-Buckets für die CloudTrail-Protokollierung
S3_BUCKET_PUBLIC_READ_PROHIBITED	Nicht zutreffend
VPC_DEFAULT_SECURITY_GROUP_CLOSED	Nicht zutreffend

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

Weitere CIS-Quellen

- Die CIS AWS Foundations Benchmark v.1.2.0
- CIS AWS Benchmark Blog-Posts im AWSSecurity Blog

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0

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

- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0, Level 1
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0, Level 1 und 2

> **Note**
>
> Informationen über CIS AWS Foundations Benchmark v1.2.0 und die AWS Audit Manager Frameworks, die diese Version des Benchmarks unterstützen, finden Sie unter CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0.

Themen

Was ist CIS?

Das Center for Internet Security (CIS) hat den CIS AWSFoundations Benchmark v1.3.0 entwickelt, eine Reihe von Best Practices zur Sicherheitskonfiguration für AWS. Diese branchenweit anerkannten Best Practices gehen über die bereits verfügbaren allgemeinen Sicherheitsrichtlinien hinaus, da sie AWS Nutzern klare, schrittweise Implementierungs- und Bewertungsverfahren bieten.

Weitere Informationen finden Sie in den CISAWS Foundations Benchmark Blog-Posts in AWS Security Blog.

CIS AWS Foundations Benchmark v1.3.0 ist eine Richtlinie 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 Amazon Web Services Foundations Benchmark v1.3.0 – 1.5 stellt 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 AWS-Umgebung eingerichtet werden kann.

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

  Beispiel: CIS Controls v7.1 – Sub-Control 4.5 verwenden 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).

Verwenden Sie diese Frameworks zur Unterstützung Ihrer Audit-Vorbereitung

Sie können die CIS AWS Foundations Benchmark v1.3 Frameworks verwendenAWS 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	AWS-Services im Umfang
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0, Level 1	33	5	6	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0, Level 1 und 2	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

Um eine Liste der AWS Config-Regeln zu überprüfen, die als Datenquellenzuordnungen für diese Standard-Frameworks verwendet werden, laden Sie die folgenden Dateien herunter:

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip

- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip

Die Kontrollen in diesen Frameworks dienen nicht zur Überprüfung, ob Ihre Systeme dem CIS-Standard entsprechen. Darüber hinaus garantieren sie nicht, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden diese Frameworks unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit-Manager-Konsole verwenden, um eine Bewertung anhand dieser Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Geltungsbereich standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des CIS-Benchmarks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieser Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieser Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere CIS-Quellen

- CIS AWS Benchmark Blog-Posts im AWSSecurity Blog

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0

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

- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1
- CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1 und 2

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version 1.2.0 unterstützen, finden Sie unterCIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.2.0.
> - Informationen zu den Audit Manager-Frameworks, die Version 1.3.0 unterstützen, finden Sie unterCIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.3.0.

Themen

Was ist die CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0

Die CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1 und 2 ist ein präskriptiver Leitfaden 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 Amazon Web Services Foundations Benchmark v1.4.0 – 1.5 stellt 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 AWS-Umgebung eingerichtet werden kann.
- CIS Controls gelten für Ihr gesamtes Unternehmen und beziehen sich nicht nur auf ein Produkt eines Anbieters.

  Beispiel: CIS Controls v7.1 – Sub-Control 4.5 verwenden 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 Foundations Benchmark v1.40 Frameworks verwendenAWS 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	AWS-Services im Umfang
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, Level 1 und 2	50	8	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um eine Liste der AWS Config-Regeln zu überprüfen, die als Datenquellenzuordnungen für diese Standard-Frameworks verwendet werden, laden Sie die folgenden Dateien herunter:
>
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip

Die Kontrollen in diesen Frameworks dienen nicht zur Überprüfung, ob Ihre Systeme dem Standard CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4.0 entsprechen. Darüber hinaus garantieren sie nicht, dass Sie ein CIS-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden diese Frameworks unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit-Manager-Konsole verwenden, um eine Bewertung anhand dieser Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Geltungsbereich standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des CIS-Benchmarks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieser Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieser Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere CIS-Quellen

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

CIS Controls v7.1 Implementierungsgruppe 1

AWS Audit Manager stellt ein vorgefertigtes Framework bereit, das Center for Internet Security (CIS) Controls v7.1 Implementierungsgruppe 1 unterstützt.

> **Note**
>
> Informationen zu CIS Controls v8 IG1 und dem AWS Audit Manager-Framework, das diesen Standard unterstützt, finden Sie unter CIS Controls v8 Implementierungsgruppe 1.

AWS Audit Manager stellt ein vorgefertigtes Framework bereit, das das Center for Internet Security (CIS) unterstützt, um Sie bei der Vorbereitung Ihrer Prüfung zu unterstützen.

Themen

Was sind CIS Controls?

Bei CIS Controls handelt es sich um eine Reihe von Maßnahmen, die nach Prioritäten geordnet sind und zusammen eine Reihe Best Practices bilden, die eine umfassende Verteidigung ermöglichen. 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 Amazon Web Services Foundations Benchmark v1.2.0 – 1.13 stellt 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 AWS-Umgebung eingerichtet werden kann.
- CIS Controls gelten für Ihr gesamtes Unternehmen und beziehen sich nicht nur auf ein Produkt eines Anbieters.
  - Beispiel: CIS Controls v7.1 – Sub-Control 4.5 verwenden 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).

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das CIS Controls v7.1 IG1 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 v7.1 IG1 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 CIS Controls v7.1 IG1 Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
CIS Controls v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_CIS-Controls-v7.1-IG1.zip herunter.

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.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen von CIS Controls. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun.

Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere CIS-Quellen

- CIS Controls v7.1 IG1

CIS Controls v8 Implementierungsgruppe 1

AWS Audit Manager stellt ein vorgefertigtes Standard-Framework bereit, das Center for Internet Security (CIS) Controls v8 Implementierungsgruppe 1 unterstützt.

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

Themen

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 Cloud-basiertes Computing, Virtualisierung, Mobilität, Outsourcing, Homeoffice 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 Amazon Web Services Foundations Benchmark v1.2.0 – 1.13 stellt 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 AWS-Umgebung eingerichtet werden kann.
- CIS Controls gelten für Ihr gesamtes Unternehmen und beziehen sich nicht nur auf ein Produkt eines Anbieters.
  - Beispiel: CIS Controls v7.1 – Sub-Control 4.5 verwenden 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).

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das CIS Controls v8 IG1 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 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 des CIS Controls v8 Frameworks lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
CIS Controls v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip herunter.

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.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen von CIS Controls. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere CIS-Quellen

- CIS Controls v8

FedRAMP Moderate Baseline

AWS Audit Manager bietet ein FedRAMP Moderate Baseline-Framework, das Sie bei der Vorbereitung Ihrer Prüfung unterstützt.

Themen

- Was ist FedRAMP?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere FedRAMP-Ressourcen

Was ist FedRAMP?

Das Federal Risk and Authorization Management Program (FedRAMP) wurde 2011 eingerichtet. 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.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das FedRAMP Moderate Baseline-Framework verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den FedRAMP-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 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	AWS-Services im Umfang
FedRAMP Moderate Baseline	303	908	325	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip herunter.

Die Kontrollen in diesem Framework dienen nicht zur Überprüfung, ob Ihre Systeme FedRAMP-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.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des FedRAMP Moderate Baseline. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere FedRAMP-Ressourcen

- AWSCompliance-Seite für FedRAMP
- AWSFedRAMP-Blog-Posts

Datenschutz-Grundverordnung (DSGVO)

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das die Datenschutz-Grundverordnung (DSGVO) unterstützt. Standardmäßig enthält dieses Framework nur manuelle

Kontrollen. Bei diesen manuellen Kontrollen werden Beweise nicht automatisch gesammelt. Wenn Sie jedoch die Beweissuche für einige Kontrollen im Rahmen der DSGVO automatisieren möchten, können Sie die benutzerdefinierte KontrollFeature in AWS Audit Manager verwenden. Weitere Informationen finden Sie unter Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung.

Themen

Was ist die Datenschutz-Grundverordnung (DSGVO)?

Die Datenschutz-Grundverordnung (DSGVO) ist ein neues europäisches Datenschutzgesetz, das am 25. Mai 2018 in Kraft trat. 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 AWS Audit Manager. Weitere Informationen finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das DSGVO-Framework in AWS 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	AWS-Services im Umfang
DSGVO	0	371	10	None

Sie finden das DSGVO-Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager. Da dieses Standard-Framework nur manuelle Kontrollen enthält, fallen keine AWS-Services in den Umfang.

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 Kontrollen 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 als Datenquellen verwendet. Um erfolgreich Beweise aus diesen Datenquellen zu sammeln, sollten Sie unbedingt wie folgt vorgehen:

- Vergewissern Sie sich, dass Sie die Anweisungen zur Aktivierung und EinrichtungAWS Config und AWS Security Hub in Ihrem AWS-Konto befolgt haben.
- Vergewissern Sie sich, dass Sie AWS Config und Security Hub als Services in den Leistungsumfang aufgenommen haben. Eine Übersicht über die Services, die für Ihre Bewertung in Frage kommen, finden Sie unter Bewertung überprüfen (Registerkarte „AWS-Services“). Informationen zum Bearbeiten dieser Liste finden Sie unter Umfang von AWS-Services bearbeiten.

Nachdem Sie beide Services eingerichtet haben, sammelt Audit Manager bei jeder Bewertung einer festgelegten AWS Config-Regel oder Security Hub-Kontrolle Beweise.

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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und die folgenden Security-Hub-Kontrollen als Datenquellenzuordnungen aus: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 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) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 3.14 (CloudWatch.14) • 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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und die folgenden Security-Hub-Kontrollen als Datenquellenzuordnungen aus: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 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) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 3.14 (CloudWatch.14) • 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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und die folgenden Security-Hub-Kontrollen als Datenquellenzuordnungen aus: • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 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) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13)

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
		• 3.14 (CloudWatch.14) • Config.1
Artikel 30 Aufzeichnungen über Prozessaktivitäten.1	Kapitel 4 – Controller und Prozessor	Sie können eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und wählen Sie die folgende Security Hub-Kontrolle 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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und wählen Sie die folgende Security Hub-Kontrolle 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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und wählen Sie die folgende Security Hub-Kontrolle 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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und wählen Sie die folgende Security Hub-Kontrolle 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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle 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 Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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 als Datenquellentyp und wählen Sie die folgende Security Hub-Kontrolle 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 eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Datenverschlüsselung 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 Verschlüsselung im Ruhezustand • Amazon CloudWatch Warnungen zur AWS Config-Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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_ENABLED • 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_ENABLED_AND_ENCRYPTED

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 32 Sicherheit der Verarbeitung.2	Kapitel 4 – Controller und Prozessor	Sie können eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Datenverschlüsselung 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 Verschlüsselung im Ruhezustand • Amazon CloudWatch Warnungen zur AWS Config-Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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_ENABLED • 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_ENABLED_AND_ENCRYPTED

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 32 Sicherheit der Verarbeitung.3	Kapitel 4 – Controller und Prozessor	Sie können eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Datenverschlüsselung 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 Verschlüsselung im Ruhezustand • Amazon CloudWatch Warnungen zur AWS Config-Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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_ENABLED • 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_ENABLED_AND_ENCRYPTED

Name der Kontrolle	Kontrollsatz	Empfohlene Zuordnung der Kontrolldatenquellen
Artikel 32 Sicherheit der Verarbeitung.4	Kapitel 4 – Controller und Prozessor	Sie können eine benutzerdefinierte Kontrolle in AWS Audit Manager erstellen, die diese DSGVO-Kontrolle unterstützt. Wenn Sie die Kontrolldetails angeben, geben Sie unter Testinformationen Folgendes ein: • Datenverschlüsselung 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 Verschlüsselung im Ruhezustand • Amazon CloudWatch Warnungen zur AWS Config-Anzeige aller Änderungen und aller kommentierten Einstellungen • Alle Root-Aktivitäten Wenn Sie die Kontrolldatenquellen einrichten, empfehlen wir, die Folgende als Datenquellen einzubeziehen: Wählen Sie AWS Config als Datenquellentyp und wählen Sie die folgenden AWS Config verwalteten Regeln als Datenquellenzuordnung 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_ENABLED • 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_ENABLED_AND_ENCRYPTED

Nachdem Sie Ihre neuen benutzerdefinierten Kontrollen für die DSGVO erstellt haben, können Sie diese zu einem Framework für benutzerdefinierte DSGVO hinzufügen. Weitere Informationen erhalten Sie unter Erstellen eines benutzerdefinierten Frameworks und Bearbeiten eines benutzerdefinierten Frameworks. Sie können eine Bewertung aus einem benutzerdefiniertem DSGVO-Framework erstellen. Auf diese Weise kann AWS Audit Manager automatisch Beweise für die von Ihnen hinzugefügten benutzerdefinierten Kontrollen sammeln. Anweisungen zum Erstellen einer Bewertung eines Frameworks finden Sie unter Erstellen einer Bewertung.

Weitere DSGVO-Quellen

- Zentrum für die Datenschutz-Grundverordnung (DSGVO)
- AWSDSGVO-Blog-Posts

Gramm-Leach-Bliley Act (GLBA)

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

Themen

- Was ist der Gramm-Leach-Bliley Act (GLBA)?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Was ist der Gramm-Leach-Bliley Act (GLBA)?

Der Gramm-Leach-Bliley Act (GLB Act oder GLBA), auch bekannt als Financial Service Modernization Act von 1999, ist ein Bundesgesetz, das in den USA erlassen wurde, um zu kontrollieren, wie Finanzinstitute mit privaten Daten von Einzelpersonen umgehen. Das Gesetz besteht aus drei Abschnitten. Der erste ist die „Financial Privacy Rule“, die die Erfassung und Offenlegung privater Finanzinformationen regelt. Die zweite ist die „Safeguards Rule“, die vorsieht, dass Finanzinstitute Sicherheitsprogramme zum Schutz solcher Informationen implementieren müssen. Bei der dritten handelt es sich um die „Pretexting Provisions“, die das Vortäuschen von

falscher 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.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework für den Gramm-Leach-Bliley Act (GLBA) 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 die AWS-Konten und Services angeben, die Sie in den Umfang Ihres Audits 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 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 GLBA-Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
Gramm-Leach-Bliley Act (GLBA)	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
				• AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_GLBA.zip herunter.

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

Sie finden das GLBA-Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des GLBA. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

GxP 21 CFR Teil 11

AWS Audit Manager bietet ein vorgefertigtes Framework, das die Vorschriften des GxP CFR Teil 11 unterstützt und auf AWS-Best Practices basiert.

> **Note**
>
> Informationen zu GxP EU Anhang 11 und dem Audit Manager-Framework, das ihn unterstützt, finden Sie unter GxP EU Anhang 11.

Themen

Was ist GxP CFR Teil 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.

Der Begriff GxP umfasst ein breites Spektrum von Aktivitäten im Zusammenhang mit der Einhaltung von Vorschriften. Dazu gehören gute Laborpraktiken (Good Laboratory Practices, GLP), gute klinische Praktiken (Good Clinical Practices, GCP) und gute Herstellungspraktiken (Good Manufacturing Practices, GMP). Jede dieser verschiedenen Arten von Aktivitäten beinhaltet produktspezifische Anforderungen, die Unternehmen im Bereich Biowissenschaften umsetzen müssen. Dies hängt von der Art der Produkte ab, die die Unternehmen herstellen, sowie von dem Land, in dem ihre Produkte verkauft werden. Wenn Unternehmen der Biowissenschaften Computersysteme zur Durchführung bestimmter GxP-Aktivitäten verwenden, müssen sie sicherstellen, dass das computergestützte GxP-System für den vorgesehenen Verwendungszweck des Systems entwickelt, validiert und betrieben wird.

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

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework Gxp 21 CFR Teil 11 verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den GxP-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 GxP 21 CFR Teil 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 von Framework GxP CFR Teil 11 lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
GxP 21 CFR Teil 11	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_GxP-21-CFR-Part-11.zip herunter.

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

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des GxP CFR Teil 11 Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere GxP-Quellen

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

GxP EU Anhang 11

AWS Audit Manager bietet ein vorgefertigtes Framework, das die Vorschriften des GxP EU Anhang 11 unterstützt und auf AWS-Best Practices basiert.

> **Note**
>
> Informationen zu GxP 21 CFR Teil 11 und dem Audit Manager-Framework, das ihn unterstützt, finden Sie unter GxP 21 CFR Teil 11.

Themen

Was ist GxP EU Anhang 11?

Das GxP EU Anhang 11 Framework ist das europäische Äquivalent zum FDA 21 CFR Teil 11 Framework in den USA. 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 Featureen 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 des Europäischen Gremiums festgelegten Richtlinien sind nicht allzu weit von der FDA entfernt (21 CFR Teil 11). In Anhang 11 sind die Kriterien festgelegt, nach denen elektronische Aufzeichnungen und elektronische Signaturen als verwaltet gelten.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework GxP EU Anhang 11 verwenden, um sich auf Audits vorzubereiten. Dieses Framework umfasst eine vorgefertigte Sammlung von Kontrollen mit Beschreibungen und Testverfahren. Diese Kontrollen sind gemäß den GxP-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 GxP EU 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 Framework GxP EU Anhang 11 lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
GxP EU Anhang 11	19	13	3	• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_GxP-EU–Annex-11.zip herunter.

Die Kontrollen in diesem Framework dienen nicht zur Überprüfung, ob Ihre Systeme die Anforderungen von GxP EU Anhang 11 erfüllen. Darüber hinaus können sie nicht garantieren, dass

Sie ein GxP-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des GxP EU Anhang 11 Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Health Insurance Portability and Accountability Act (HIPAA) Sicherheitsvorschriften 2003

AWS Audit Manager bietet ein vorgefertigtes Framework, das HIPAA-Vorschriften unterstützt, um Sie bei der Vorbereitung Ihrer Prüfung zu unterstützen.

> **Note**
>
> Dieses Framework hatte in der Framework-Bibliothek die Bezeichnung HIPAA. Am 8. März 2023 haben wir den Namen dieses Frameworks in HIPAA-Sicherheitsvorschriften 2003 geändert, um es von den HIPAA Final Omnibus Sicherheitsvorschriften 2013 zu unterscheiden.
> Informationen zu den HIPAA Final Omnibus Sicherheitsvorschriften 2013 und zum Audit Manager-Framework, das diesen Standard unterstützt, finden Sie unter Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Sicherheitsvorschriften 2013.

Themen

Was ist HIPAA und was sind die HIPAA Sicherheitsvorschriften 2003?

Der Health Insurance Portability and Accountability Act of 1996 (HIPAA) ist ein Gesetz, das US-Arbeitnehmern hilft, den Krankenversicherungsschutz aufrechtzuerhalten, 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 verwenden nutzungsbasierte AWS Cloud-Dienste zur Verarbeitung, Speicherung und Übertragung von geschützten Gesundheitsdaten (PHI). AWS ermöglicht es betroffenen Einrichtungen und ihren Geschäftspartnern,

die der HIPAA unterliegen, die sichere AWS-Umgebung zu verwenden, um geschützte Gesundheitsdaten zu verarbeiten, zu verwalten und zu speichern.

Anweisungen zur Verarbeitung und Speicherung von Gesundheitsdaten finden Sie im AWS Whitepaper Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

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 des Frameworks HIPAA-Sicherheitsvorschriften 2003 lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
HIPAA-Sicherheitsvorschriften 2003	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
				• AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-2003.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, 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 Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des HIPAA-Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere HIPAA-Ressourcen

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

Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Sicherheitsvorschriften 2013

AWS Audit Manager bietet ein vorgefertigtes Framework, das HIPAA-Vorschriften unterstützt, um Sie bei der Vorbereitung Ihrer Prüfung zu unterstützen.

> **Note**
>
> Informationen zu den HIPAA Sicherheitsvorschriften 2003 und zum AWS Audit Manager-Framework, das diesen Standard unterstützt, finden Sie unter Health Insurance Portability and Accountability Act (HIPAA) Sicherheitsvorschriften 2003.

Themen

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

Der Health Insurance Portability and Accountability Act of 1996 (HIPAA) ist ein Gesetz, das US-Arbeitnehmern hilft, den Krankenversicherungsschutz aufrechtzuerhalten, 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 verwenden nutzungsbasierte AWS Cloud-Dienste zur Verarbeitung, Speicherung und Übertragung von geschützten Gesundheitsdaten (PHI). AWS ermöglicht es betroffenen Einrichtungen und ihren Geschäftspartnern, die der HIPAA unterliegen, die sichere AWS-Umgebung zu verwenden, um geschützte Gesundheitsdaten zu verarbeiten, zu verwalten und zu speichern. Anweisungen zur Verarbeitung und Speicherung von Gesundheitsdaten finden Sie im AWS Whitepaper Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework HIPAA Final Omnibus Sicherheitsvorschriften 2013 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 des Frameworks HIPAA Final Omnibus Sicherheitsvorschriften 2013 lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
HIPAA Final Omnibus Sicherheitsvorschriften 2013	39	46	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_HIPAA-Final–Omnibus-Security-Rule-2013.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, 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 Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des HIPAA-Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere HIPAA-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
- AWSCompliance-Seite für HIPAA

ISO/IEC 27001:2013 Anhang A

AWS Audit Manager bietet ein vorgefertigtes Standard-Framework, das die Bewertungen gemäß ISO/IEC 27001:2013 Anhang A strukturiert und automatisiert.

Themen

- Was ist ISO/IEC 27001:2013 Anhang A?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere Ressourcen zu ISO/IEC 27001:2013 Anhang A

Was ist ISO/IEC 27001:2013 Anhang A?

Die Internationale Elektrotechnische Kommission (IEC) und die Internationale Organisation für Normung (International Organization for Standardization, ISO) sind beide unabhängige, nichtstaatliche, gemeinnützige Organisationen, die internationale Normen auf Konsensbasis entwickeln und veröffentlichen.

ISO/IEC 27001:2013 Anhang A ist ein Sicherheitsmanagement-Standard, der Best Practices für das Sicherheitsmanagement und umfassende Sicherheitskontrollen festlegt, die den ISO/IEC 27002-Leitlinien für bewährte Verfahren entsprechen. 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.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das AWS Audit Manager-Framework für ISO/IEC 27001:2013 Anhang A verwenden, um sich auf Audits 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 Vorlage verwenden, können Sie eine Audit Manager-Bewertung erstellen und mit der Erfassung von Beweisen beginnen, die für ein Audit gemäß ISO/IEC 27001:2013 Anhang A relevant sind. In Ihrer Bewertung können Sie die AWS-Konten und Services angeben, die Sie in den 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 Framework ISO/IEC 27001:2013 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	AWS-Services im Umfang
ISO/IEC 27001:2013 Anhang A	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, 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 Beweissuche erfordern.

Sie finden das Framework ISO/IEC 27001:2013 Anhang A unter der Registerkarte Standard-Frameworks von Framework-Bibliothek im Audit Manager.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Frameworks ISO-IEC 27001:2013 Anhang A. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung. Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere Ressourcen zu ISO/IEC 27001:2013 Anhang A

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

NIST 800-53 (5. Überarb.) Low-Moderate-High

AWS Audit Manager bietet ein vorgefertigtes Framework, das Bewertungen für NIST 800-53 Compliance-Standards strukturiert und automatisiert, und zwar basierend auf AWS-Best Practices.

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version NIST 800-171 unterstützen, finden Sie unter NIST SP 800-171 (2. Überarbeitung).
> - Informationen zu den Audit Manager-Frameworks, die Version NIST Cybersecurity-Framework unterstützen, finden Sie unter NIST-Cybersecurity-Framework, Version 1.1.

Themen

- Was ist NIST 800-53?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere NIST-Ressourcen

Was ist NIST 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 nach NIST 800-53 gelten generell für die 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 800-53 Low-Moderate-High-Framework (5. Überarb.) stellt die Sicherheitskontrollen und die zugehörigen Bewertungsverfahren dar, die in NIST SP 800-53 (5. Überarb.) empfohlenen Sicherheitskontrollen für Federal Information Systems und Organisationen 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.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework NIST 800-53 Low-Moderate-High (5. Überarb.) 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-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 800-53 Low-Moderate-High-Framework (5. Überarb.) 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 NIST 800-53 Low-Moderate-High Frameworks (5. Überarb.) lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
NIST 800-53 (5. Überarb.) Low-Moderate-High	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, 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 Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des NIST 800-53 Low-Moderate-High-Frameworks (5. Überarb.). Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere NIST-Ressourcen

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

NIST-Cybersecurity-Framework, Version 1.1

AWS Audit Manager bietet ein vorgefertigtes Framework, das Bewertungen für das NIST Cybersecurity Framework strukturiert und automatisiert, und zwar basierend auf AWS-Best Practices.

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version NIST 800-53 (Rev. 5) Low-Moderate-High unterstützen, finden Sie unter NIST 800-53 (5. Überarb.) Low-Moderate-High.
> - Informationen zu den Audit Manager-Frameworks, die Version NIST SP 800-171 (2. Überarb.) unterstützen, finden Sie unter NIST SP 800-171 (2. Überarbeitung).

Themen

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 Featureieren 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.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das NIST Cybersecurity Framework Version 1.1 verwenden, um sich auf Audits vorzubereiten. 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, indem er 56 automatisierte Kontrollen und 52 manuelle Kontrollen bietet. Diese Kontrollen sind 23 Cybersicherheitskategorien zugeordnet, die im Framework-Kern definiert sind. Audit Manager unterstützt das Profil und die Implementierungskomponenten in diesem Framework nicht.

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 Cybersecurity Framework 1.1 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 für NIST Cybersecurity Framework Version 1.1 lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
NIST-Cybersecurity-Framework, Version 1.1	56	52	23	• AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 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 zur Überprüfung, ob Ihre Systeme dem NIST Cybersecurity Framework entsprechen. Darüber hinaus können sie nicht garantieren, dass Sie ein NIST Cybersecurity-Audit bestehen. AWS Audit Manager überprüft nicht automatisch Verfahrenskontrollen, die eine manuelle Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Frameworks NIST Cybersecurity Framework Version 1.1. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere NIST-Ressourcen

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

NIST SP 800-171 (2. Überarbeitung)

AWS Audit Manager bietet ein vorgefertigtes Framework, das Bewertungen für NIST SP 800-171 Compliance-Standards strukturiert und automatisiert, basierend auf AWS-Best Practices.

> **Note**
>
> - Informationen zu den Audit Manager-Frameworks, die Version NIST 800-53 (Rev. 5) Low-Moderate-High unterstützen, finden Sie unter NIST 800-53 (5. Überarb.) Low-Moderate-High.
> - Informationen zu den Audit Manager-Frameworks, die Version NIST Cybersecurity-Framework Version 1.1 unterstützen, finden Sie unter NIST-Cybersecurity-Framework, Version 1.1.

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 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 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 800-171 gilt nur für die Bereiche des Netzwerks eines Auftragnehmers, in denen CUI präsent ist.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

Sie können das Framework NIST SP 800-171 (2. Überarb.) 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 (2. Überarb.) 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 NIST SP 800-171 Frameworks (2. Überarb.) lauten wie folgt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
NIST SP 800-171 (2. Überarb.)	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
				• AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_NIST-SP-800-171-Rev.2.zip herunter.

Die AWS Audit Manager-Kontrollen in diesem Framework dienen nicht zur Überprüfung, 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.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Informationen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des NIST SP 800-171 Frameworks (2. Überarb.). Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere NIST-Ressourcen

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

PCI DSS v3.2.1

AWS Audit Manager bietet ein vorgefertigtes Framework, das 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?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere PCI DSS-Ressourcen

Was ist PCI DSS?

Der Payment Card Industry Data Security Standard (PCI-DSS) ist ein festgelegter proprietärer Standard für Informationssicherheit. Er wird vom PCI Security Standards Council verwaltet, das von American Express, Discover Financial Services, JCB International, MasterCard Worldwide und Visa Inc. gegründet wurde. PCI DSS gilt für Unternehmen, die Karteninhaberdaten (Cardholder Data, CHD) oder sensible Authentifizierungsdaten (Sensitive Authentication Data, 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 Serviceanbieter 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 Attestation of Compliance (AOC) und die Zusammenfassung der Verantwortlichkeiten

finden Sie unter. AWS Artifact Dies ist ein Self-Service-Portal für den On-Demand-Zugriff auf AWS Compliance-Berichte. Melden Sie sich AWS Artifactin der AWS Management-Konsole an oder erfahren Sie mehr unter Erste Schritte bei 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 PCI DSS v3.2.1 Framework sind im Folgenden aufgeführt:

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
PCI DSS v3.2.1	175	487	12	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
				• AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> 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 zur Überprüfung, 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 Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Informationen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des PCI DSS V3.2.1-Frameworks. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere PCI DSS-Ressourcen

- PCI Security Standards Council
- Dokumentenbibliothek des PCI Security Standards Council.
- AWSCompliance-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?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere PCI DSS-Ressourcen

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.

Weitere Informationen zu den Änderungen finden Sie in der Zusammenfassung der Änderungen von PCI DSS Version 3.2.1 bis 4.0.

Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung

> **Note**
>
> Dieses Standard-Framework verwendet konsolidierte Kontrollen von Security Hub als Datenquelle. Um erfolgreich Beweise aus konsolidierten Kontrollen zu erfassen, stellen Sie sicher, dass Sie die Einstellung für Ergebnisse konsolidierter Kontrollen in Security Hub aktiviert haben. Weitere Informationen zur Verwendung von Security Hub als Datenquellentyp finden Sie unter AWS Security Hub-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	AWS-Services im Umfang
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Amazon OpenSearch Service • Amazon Redshift • Amazon Relational Database Service • Amazon SageMaker

Name des Frameworks in AWS Audit Manager	Anzahl der automatisierten Kontrollen	Anzahl der manuellen Kontrollen	Anzahl der Kontrollsätze	AWS-Services im Umfang
				• Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

> **Tip**
>
> 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.zip herunter.

Die Kontrollen in diesem AWS Audit Manager-Framework dienen nicht zur Überprüfung, 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 Beweissuche erfordern.

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Informationen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Frameworks PCI DSS V4. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere PCI DSS-Ressourcen

- PCI DSS v4.0 Resource Hub
- PCI Security Standards Council
- Dokumentenbibliothek des PCI Security Standards Council.
- AWSCompliance-Seite für PCI DSS
- Payment Card Industry Data Security Standard (PCI DSS) v4.0 im AWS-Compliance-Handbuch
- Zusammenfassung der Änderungen von PCI DSS Version 3.2.1 auf 4.0

SOC 2

SOC 2 ist ein Prüfverfahren, das sicherstellt, dass die Daten eines Unternehmens sicher verwaltet werden. AWS Audit Manager bietet ein vorgefertigtes Framework, das SOC 2 unterstützt.

Themen

- Was ist SOC 2?
- Verwenden Sie dieses Framework zur Unterstützung Ihrer Audit-Vorbereitung
- Weitere SOC 2-Ressourcen

Was ist SOC 2?

Das System and Organization Controls (SOC), definiert vom American Institute of Certified Public Accountants (AICPA), ist der Name einer Reihe von Berichten, die während 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 durch unabhängige Dritte erstellte Prüfberichte, die nachweisen, wie AWS wichtige Compliance-Kontrollen und -Ziele erfüllt. Der Zweck dieser Berichte besteht darin, Ihnen und Ihren Prüfern die AWS-Kontrollen zu veranschaulichen, die für die Unterstützung von Betrieb und Compliance eingerichtet wurden. Es gibt fünf AWS-SOC-Berichte:

- AWSSOC 1-Bericht, erhältlich für AWS-Kunden in AWS Artifact.
- AWS SOC 2-Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit, erhältlich für AWS Kunden in AWS Artifact.
- AWS SOC 2-Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit, erhältlich für AWS Kunden in AWS Artifact (nur Geltungsbereich Amazon DocumentDB).
- AWS SOC 2 Datenschutz-Typ I Report, erhältlich für AWS Kunden in AWS Artifact.
- AWSSOC 3-Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit, öffentlich verfügbar als Whitepaper.

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	AWS-Services im Umfang
SOC 2	20	41	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Um die AWS Config-Regeln zu überprüfen, die in diesem Standard-Framework als Datenquellenzuordnungen verwendet werden, laden Sie die Datei AuditManager_ConfigDataSourceMappings_SOC2.zip herunter.

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

Sie finden das Framework unter der Registerkarte Standard-Frameworks von Framework-Bibliothek in Audit Manager.

Anweisungen zum Erstellen einer Bewertung mithilfe dieses Frameworks finden Sie unter Erstellen einer Bewertung.

Wenn Sie die Audit Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Umfang standardmäßig ausgewählt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den SOC 2-Anforderungen. Wenn Sie die Liste der Services bearbeiten müssen, die für dieses Framework gelten, können Sie dies mithilfe der API-Operationen CreateAssessment oder UpdateAssessment tun. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Anweisungen zum Anpassen dieses Frameworks an Ihre spezifischen Anforderungen finden Sie unter Anpassen eines vorhandenen Frameworks und Anpassen einer vorhandenen Kontrolle.

Weitere SOC 2-Ressourcen

- AWSCompliance-Seite für SOC

Kontrollbibliothek

Sie können über die Kontrollbibliothek in Audit Manager auf Kontrollen zugreifen und diese verwalten. Sie können jederzeit zur Kontrollbibliothek wechseln, indem Sie im Navigationsbereich der Audit Manager-Konsole die Option Kontrollbibliothek auswählen.

Die Kontrollbibliothek enthält einen Katalog mit Standard-Kontrollen und benutzerdefinierten Kontrollen.

- Standard-Kontrollen sind vordefinierte Kontrollen, die von AWSbereitgestellt werden. Sie können die Konfigurationsdetails von Standard-Kontrollen anzeigen, sie jedoch nicht bearbeiten oder löschen. Sie können jedoch jede Standard-Kontrolle anpassen, um eine neue zu erstellen, die Ihren spezifischen Anforderungen entspricht.
- Benutzerdefinierte Kontrollen sind benutzerdefinierte Kontrollelemente, die Sie besitzen und definieren. Mit einer benutzerdefinierten Kontrolle können Sie angeben, aus welchen Datenquellen Sie Beweise sammeln möchten. Anschließend können Sie einem benutzerdefinierten Framework benutzerdefinierte Kontrollen hinzufügen.

  Weitere Informationen zum Hinzufügen einer benutzerdefinierten Kontrolle zu einem benutzerdefinierten Framework finden Sie unter Framework-Bibliothek. Weitere Informationen zum Erstellen einer Bewertung aus einem Audit Manager-Framework finden Sie unter Bewertungen in AWS Audit Manager.

In diesem Abschnitt wird beschrieben, wie Sie benutzerdefinierte Kontrollen in Audit Manager erstellen und verwalten können.

Themen

Zugriff auf die verfügbaren Kontrollen in AWS Audit Manager

Sie können alle verfügbaren Kontrollen auf der Seite Kontrollbibliothek in der Audit Manager-Konsole anzeigen. Von hier aus können Sie auch eine benutzerdefinierte Kontrolle erstellen oder eine vorhandene Kontrolle anpassen.

Sie können alle verfügbaren Kontrollen auch über die Audit Manager-API oder die AWS Command Line Interface (AWS CLI) anzeigen.

Audit Manager console

So zeigen Sie verfügbare Kontrollen an (Konsole)

1. Öffnen Sie die AWS Audit-Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie die Registerkarte Standard-Kontrolle oder die Registerkarte Benutzerdefinierte Kontrollen, um die verfügbaren Kontrollen zu durchsuchen.
4. Um die Details für eine Kontrolle anzuzeigen, wählen Sie den Namen der Kontrolle aus.

AWS CLI

Um die verfügbaren Kontrollen anzuzeigen (AWS CLI)

Führen Sie den Befehl Kontrollen auflisten aus und geben Sie einen `--control-type` an. Sie können entweder eine Liste der Standard-Kontrollen abrufen, oder Sie können eine Liste der benutzerdefinierten Kontrollen abrufen.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

Um die verfügbaren Kontrollen (API) anzuzeigen

Verwenden Sie die -ListControlsOperation und geben Sie einen controlType an. Sie können entweder eine Liste von Standard-Kontrollen zurückgeben, oder Sie können eine Liste der benutzerdefinierten Kontrollen zurückgeben.

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 `ListControls` Operation und der Parameter in einem der sprachspezifischen AWS SDKs.

Überprüfung der Details einer Kontrolle

Sie können die Details einer Kontrolle mithilfe der Audit Manager-Konsole, der Audit Manager-API oder der AWS Command Line Interface (AWS CLI) überprüfen.

Audit Manager console

Anzeigen von Kontrolldetails (Konsole)

1. Öffnen Sie die AWS Audit-Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek, um eine Liste der verfügbaren Kontrollen anzuzeigen.
3. Wählen Sie die Registerkarte Standard-Kontrolle oder die Registerkarte Benutzerdefinierte Kontrollen, um die verfügbaren Kontrollen zu durchsuchen.
4. Um die Details für eine Kontrolle anzuzeigen, wählen Sie den Namen der Kontrolle aus.

Wenn Sie eine Kontrolle öffnen, wird eine Seite mit den Kontrolldetails angezeigt. Die Abschnitte dieser Seite und ihr Inhalt werden im Folgenden beschrieben.

Abschnitt „Zusammenfassung“

Dieser Abschnitt bietet eine Übersicht über die Kontrolle. Dazu gehören folgende Informationen:

- Kontrollname – Der Name der Kontrolle.
- Kontrolltyp – Gibt an, ob es sich bei der Kontrolle um eine Standard-Kontrolle oder eine benutzerdefinierte Kontrolle handelt.
- Tags – Gibt die Anzahl der Tags an, die de Kontrolle zugeordnet sind.
- Datenquellentypen – Die Anzahl der Datenquellentypen, die für diese Kontrolle verwendet werden.
- Zuordnungen – Die Anzahl der Zuordnungsattribute, die zum Abrufen von Daten aus einer Datenquelle verwendet werden.

Wenn Sie eine benutzerdefinierte Kontrolle anzeigen, werden auch die folgenden Details angezeigt:

- Erstellt von – Das Konto, mit dem die benutzerdefinierte Kontrolle erstellt wurde.
- Erstellungsdatum – Das Datum, an dem die benutzerdefinierte Kontrolle erstellt wurde.
- Letzte Aktualisierung – Das Datum, an dem die benutzerdefinierte Kontrolle zuletzt bearbeitet wurde.

Registerkarte „Details“

Diese Registerkarte bietet eine allgemeine Übersicht über die Kontrolle. Dazu gehören folgende Informationen:

- Der Abschnitt Beschreibung enthält eine Beschreibung de Kontrolle.
- Der Abschnitt mit den Testinformationen enthält eine Beschreibung der empfohlenen Testverfahren für die Kontrolle.
- Im Abschnitt Aktionsplan werden die empfohlenen Maßnahmen beschrieben, die durchgeführt werden sollten, falls die Kontrolle behoben werden muss.

Registerkarte „Datenquelle“

Diese Registerkarte zeigt Informationen über die Datenquellen für die Kontrolle an. Dazu gehören folgende Informationen:

- Name der Datenquelle – Dies gilt nur für benutzerdefinierte Kontrollen. Er bezieht sich auf den beschreibenden Namen, den Sie jeder Datenquelle gegeben haben. Sie können diesen Namen verwenden, um zwischen mehreren Datenquellen zu unterscheiden, die unter denselben Datenquellentyp fallen.
- Datenquellentyp – Dieser gibt an, woher die Beweisdaten stammen.
  - Wenn Audit Manager die Beweise sammelt, kann es sich bei der Datenquelle um einen von vier Typen handeln: AWS Security Hub, AWS Config, AWS CloudTrail, oder AWS API-Aufrufe.
  - Wenn Sie Ihre eigenen Beweise hochladen, ist der Datenquellentyp Manuell. Eine Beschreibung gibt an, ob es sich bei den erforderlichen manuellen Beweisen um einen Datei-Upload oder eine Textantwort handelt.
- Zuordnung – Dies ist das Zuordnungsattribut, das verwendet wird, um Daten aus der Datenquelle zu identifizieren und abzurufen.
  - Wenn der Datenquellentyp ist AWS Config, ist die Zuordnung der Name einer bestimmten AWS Config Regel (z. B. `EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager verwendet

diese Zuordnung, um das Ergebnis dieser Regelprüfung direkt von zu melden AWS Config.

- Wenn der Datenquellentyp ist AWS Security Hub, ist die Zuordnung der Name eines bestimmten Security Hub-Steuerelements (z. B. `1.1 – Avoid the use of the "root" account`). Audit Manager verwendet diese Zuordnung, um das Ergebnis dieser Sicherheitsprüfung direkt vom Security Hub aus zu melden.
- Wenn der Datenquellentyp AWS API-Aufrufe ist, ist die Zuordnung der Name eines bestimmten API-Aufrufs (z. B. `ec2_DescribeSecurityGroups`). Audit Manager verwendet diese Zuordnung, um die API-Antwort zu sammeln.
- Wenn die Datenquelle ist AWS CloudTrail, ist die Zuordnung der Name eines bestimmten CloudTrail Ereignisses (z. B. `CreateAccessKey`). Audit Manager verwendet diese Zuordnung, um die zugehörigen Benutzeraktivitäten aus Ihren CloudTrail Protokollen zu erfassen.

- Häufigkeit – Dies gibt an, wie oft Audit Manager Beweise aus der Datenquelle sammelt. Die Häufigkeit variiert je nach Datenquellentyp. Weitere Informationen finden Sie, wenn Sie den Wert in der Spalte auswählen oder unter Häufigkeit der Beweissuche.

Registerkarte „Tags“

Diese Registerkarte listet die Tags auf, die der Kontrolle zugeordnet sind. Dazu gehören folgende Informationen:

- Schlüssel – Der Tag-Schlüssel (z. B. ein Konformitätsstandard, eine Vorschrift oder eine Kategorie).
- Wert – Der Tag-Wert.

AWS CLI

Um Kontrolldetails (AWS CLI) anzuzeigen

1. Um die Kontrolle zu identifizieren, die Sie überprüfen möchten, führen Sie den Befehl Kontrollen auflisten aus und geben Sie einen `--control-type` an. Sie können entweder eine Liste der Standard-Kontrollen abrufen, oder Sie können eine Liste der benutzerdefinierten Kontrollen abrufen.

   Ersetzen Sie im folgenden Beispiel den *`Platzhaltertext`* durch `Custom` oder `Standard`.

   ```
   aws auditmanager list-controls --control-type Custom/Standard
   ```

Die Antwort gibt eine Liste von Kontrollen zurück. Suchen Sie nach der Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den Amazon-Ressourcennamen (ARN).

2. Um die Kontrolldetails abzurufen, führen Sie den Befehl Kontrolle erhalten aus und geben Sie den `--control-id` an.

   Ersetzen Sie im folgenden Beispiel den *`Platzhaltertext`* durch Ihre eigenen Informationen.

   ```
   aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Die Kontrolldetails werden im JSON-Format zurückgegeben. Informationen zu diesen Daten finden Sie unter get-control Output in der AWS CLI Befehlsreferenz.

3. Um die Tags für ein Steuerelement anzuzeigen, verwenden Sie den list-tags-for-resource Befehl und geben Sie die `--resource-arn` für das Steuerelement an.

   Ersetzen Sie im folgenden Beispiel den *`Platzhaltertext`* 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
   ```

   Weitere Informationen zur Verwendung von Tags in Audit Manager finden Sie unter Markieren von AWS Audit Manager -Ressourcen.

Audit Manager API

Um Kontrolldetails (API) anzuzeigen

1. Um die Kontrolle zu identifizieren, die Sie überprüfen möchten, verwenden Sie die -ListControlsOperation und geben Sie einen controlType an. Sie können entweder eine Liste von Standard-Kontrollen zurückgeben, Oder Sie können eine Liste der benutzerdefinierten Kontrollen zurückgeben.

   Suchen Sie in der Antwort nach der Kontrolle, die Sie überprüfen möchten, und notieren Sie sich die Kontroll-ID und den zugehörigen Amazon-Ressourcennamen (ARN).

2. Um die Kontrolldetails abzurufen, verwenden Sie die -GetControlOperation. Geben Sie in der Anfrage die Kontroll-ID an, die Sie aus Schritt 1 erhalten haben.

   Die Kontrolldetails werden im JSON-Format zurückgegeben. Informationen zu diesen Daten finden Sie unter GetControl Antwortelemente in der APIAWS Audit Manager -Referenz zu .
3. Um Tags für die Kontrolle anzuzeigen, verwenden Sie die -ListTagsForResourceOperation. Geben Sie in der Anfrage die Kontrolle resourceArn an, die Sie aus Schritt 1 erhalten haben.

Weitere Informationen zur Verwendung von Tags in Audit Manager finden Sie unter Markieren von AWS Audit Manager -Ressourcen.

Für weitere Informationen zu API-Befehlen klicken Sie auf einen der vorherigen Links in der AWS Audit Manager API-Referenz. Dies enthält Informationen zur Verwendung dieser Operationen und Parameter in einem der sprachspezifischen AWS SDKs.

Erstellen einer benutzerdefinierten Kontrolle

Sie können benutzerdefinierte Kontrollen verwenden, um Beweise aus bestimmten, von Ihnen definierten Datenquellen 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:

Verwenden Sie eine vorhandene Kontrolle als Ausgangspunkt

Sie können jede Kontrolle in Audit Manager anpassen. Dies ist eine gute Option, wenn eine vorhandene Kontrolle mehr oder weniger Ihrem Ziel entspricht, Sie aber die Leitlinien erweitern oder einige Attribute an Ihre spezifischen Bedürfnisse anpassen möchten. Sie können beispielsweise ändern, wie oft eine Kontrolle Beweise sammelt, und dann den Namen der Kontrolle ändern, um dies widerzuspiegeln.

Erstellen Sie eine benutzerdefinierte Kontrolle für interne Audits

Zur Unterstützung interner Audits können Sie ein speziell entwickeltes benutzerdefiniertes Kontrollsystem einrichten, das keinen Bezug zu einem bestimmten Compliance-Framework

oder einer bestimmten Verordnung hat. Auf diese Weise haben Sie die Freiheit, Ihre Kontrollanforderungen auf einen bestimmten Bereich zuzuschneiden oder Beweise anhand einer unternehmensspezifischen Ressource zu sammeln. Sie können beispielsweise eine benutzerdefinierte Kontrolle erstellen, die die benutzerdefinierten AWS Config Regeln Ihrer Organisation als Datenquelle für die Beweissuche verwendet.

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. In diesem Fall kann der Kontrollname eine Frage sein, und Sie können eine Antwort geben, indem Sie eine Datei hochladen oder eine Textantwort als manuellen Beweis eingeben.

Es gibt zwei Möglichkeiten, eine benutzerdefinierte Kontrolle zu erstellen. Sie können eine neue Kontrolle von Grund auf neu erstellen oder eine vorhandene Kontrolle anpassen.

Themen

Erstellen einer neuen benutzerdefinierten Kontrolle von Grund auf

Sie können eine neue benutzerdefinierte Kontrolle von Grund auf neu erstellen, indem Sie die folgenden Schritte ausführen.

> **Important**
>
> Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Kontrolldetails, Testinformationen oder Aktionsplan keine sensiblen personenbezogenen Daten einzugeben. Wenn Sie benutzerdefinierte Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

Themen

Schritt 1: Geben Sie die Kontrolldetails an

Geben Sie zunächst die Details Ihrer benutzerdefinierten Kontrolle an.

Um Kontrolldetails anzugeben

1. Öffnen Sie die AWS Audit-Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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: Einrichten von Datenquellen

Definieren Sie als Nächstes bis zu 10 Datenquellen. Eine Datenquelle bestimmt, woher Ihre benutzerdefinierte Kontrolle Beweise sammelt.

Wenn Sie automatisierte Beweise sammeln möchten, muss jede Datenquelle einen Datenquellentyp und eine Datenquellenzuordnung enthalten. Diese Details sind Ihrer - AWS Nutzung zugeordnet und teilen Audit Manager mit, woher die Beweise gesammelt werden sollen. Wenn Sie stattdessen Ihre eigenen Beweise vorlegen möchten, geben Sie Ihrer Datenquelle einen Namen und wählen dann eine Option für manuelle Beweise.

> **Important**
>
> Um AWS Config und Security Hub erfolgreich als automatisierte Datenquellen zu verwenden, stellen Sie sicher, dass Sie Folgendes tun:
>
> - Folgen Sie den Anweisungen, um AWS Config einzurichten sowie Security Hub einzurichten für die Verwendung mit Audit Manager.
> - Nehmen Sie AWS Config sowohl als auch Security Hub als Services in Ihre Bewertung auf.
>
> Audit Manager kann dann jedes Mal Beweise sammeln, wenn eine Bewertung für die AWS Config Regeln oder die Security Hub-Steuerelemente erfolgt, die Sie in diesem Schritt angeben.

So richten Sie Datenquellen ein

1. Ersetzen Sie unter Datenquellenname den Platzhaltertext durch einen beschreibenden Namen für die Datenquelle.
2. Wählen Sie unter Methode zur Erfassung von Beweisen aus, wie Sie Beweise für diese Kontrolle sammeln möchten.

   a. Wenn Sie möchten, dass Audit Manager Beweise sammelt, wählen Sie Automatisiert und gehen Sie wie folgt vor:

      - Geben Sie unter Datenquellentyp an, woher Audit Manager automatisierte Beweise sammelt.
        - Wählen Sie für AWS CloudTrail ein Schlüsselwort für den Ereignisnamen aus der Dropdownliste aus.
        - Wählen Sie für AWS Config einen Regeltyp und dann ein Schlüsselwort für die Regel-ID aus der Dropdownliste aus.

- Wählen Sie für AWS Security Hub eine Security Hub-Kontrolle aus der Dropdownliste aus.
- Wählen Sie für AWS API-Aufrufe einen API-Aufruf und anschließend eine Häufigkeit für die Erfassung von Beweisen aus.

> **Tip**
>
> Eine Übersicht über die einzelnen Datenquellentypen und zugehörige Tipps zur Fehlerbehebung finden Sie unter Überblick über automatisierte Datenquellen. Wenn Sie Ihre Datenquellenkonfiguration mit einem Fachexperten überprüfen müssen, legen Sie die Methode zur Beweiserhebung vorerst auf Manuell fest. Auf diese Weise können Sie die Kontrolle jetzt erstellen und zu einem Framework hinzufügen und die Kontrolle dann später nach Bedarf bearbeiten.

b. Wenn Sie Ihre eigenen Beweise vorlegen möchten, wählen Sie Manuell und anschließend die Option Manuelle Beweise aus.

- Datei-Upload – Wählen Sie diese Option, wenn für die Kontrolle Unterlagen als Beweis erforderlich sind.
- Textantwort – Wählen Sie diese Option, wenn die Kontrolle eine Antwort auf eine Frage zur Risikobewertung benötigt.

3. (Optional) Geben Sie unter Zusätzliche Details eine Beschreibung der Datenquelle und eine Beschreibung der Fehlerbehebung ein.
4. (Optional) Um eine weitere Datenquelle hinzuzufügen, wählen Sie Quelle hinzufügen und wiederholen Sie dann die Schritte 1-3.
5. (Optional) Um eine Datenquelle zu entfernen, wählen Sie oben im Feld für die Datenquellenkonfiguration die Option Entfernen aus.
6. 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.

Um einen Aktionsplan zu definieren

1. Geben Sie unter Titel einen aussagekräftigen Titel für den Aktionsplan ein.

2. Geben Sie unter Anweisungen für den Aktionsplan 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.

Was soll ich als Nächstes tun?

Nachdem Sie eine neue benutzerdefinierte Kontrolle erstellt haben, können Sie es einem benutzerdefinierten Framework hinzufügen. Weitere Informationen hierzu finden Sie unter Erstellen eines benutzerdefinierten Frameworks oder Bearbeiten eines benutzerdefinierten Frameworks.

Nachdem Sie die benutzerdefinierte Kontrolle zu einem benutzerdefinierten Framework hinzugefügt haben, können Sie anhand dieses benutzerdefinierten Frameworks eine Bewertung erstellen und mit der Erfassung von Beweisen beginnen. Weitere Informationen hierzu finden Sie unter Erstellen einer Bewertung.

Tipps zur Fehlerbehebung finden Sie unter Behebung von Problemen mit Kontrollen und Kontrollsätzen.

Anpassen eine vorhandenen Kontrolle

Anstatt eine benutzerdefinierte Kontrolle von Grund auf neu zu erstellen, können Sie eine vorhandene Kontrolle als Ausgangspunkt verwenden und es an Ihre Bedürfnisse anpassen. Wenn Sie dies tun, verbleibt die vorhandene Kontrolle in der Kontrollbibliothek, und es wird eine neue benutzerdefinierte Kontrolle mit Ihren benutzerdefinierten Einstellungen erstellt.

Sie können jede vorhandene Kontrolle zum Anpassen auswählen. Es kann sich entweder um eine Standard-Kontrolle oder um eine benutzerdefinierte Kontrolle handeln.

> **Important**
>
> Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Kontrolldetails, Testinformationen oder Aktionsplan keine sensiblen personenbezogenen Daten einzugeben. Wenn Sie

benutzerdefinierte Kontrollen erstellen, die vertrauliche Informationen enthalten, können Sie keines Ihrer benutzerdefinierten Frameworks, die diese Kontrollen enthalten, mit anderen teilen.

Themen

Schritt 1: Geben Sie die Kontrolldetails an

Die Kontrolldetails werden von der ursprünglichen Kontrolle übernommen. Überprüfen und ändern dieser Details nach Bedarf.

Um Kontrolldetails anzugeben

1. Öffnen Sie die AWS Audit-Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek aus.
3. Wählen Sie die Kontrolle aus, die Sie anpassen möchten, und klicken Sie dann auf Vorhandene Kontrolle anpassen.
4. Geben Sie den neuen Namen der Kontrolle an und wählen Sie Anpassen.
5. Passen Sie unter Kontrolldetails die Kontrolldetails nach Bedarf an.
6. Passen Sie unter Testinformationen die Testinformationen nach Bedarf an.
7. Passen Sie unter Tags die Tags nach Bedarf an.
8. Wählen Sie Weiter aus.

Schritt 2: Einrichten von Datenquellen

Datenquellen werden von ursprünglichen Kontrolle vererbt. Sie können Datenquellen nach Bedarf ändern, hinzufügen oder entfernen.

> **Important**
>
> Um AWS Config und Security Hub erfolgreich als automatisierte Datenquellen zu verwenden, stellen Sie sicher, dass Sie Folgendes tun:
>
> - Folgen Sie den Anweisungen, um AWS Config einzurichten sowie Security Hub einzurichten für die Verwendung mit Audit Manager.
> - Nehmen Sie AWS Config sowohl als auch Security Hub als Services in Ihre Bewertung auf.
>
> Audit Manager kann dann jedes Mal Beweise sammeln, wenn eine Bewertung für die AWS Config Regeln oder die Security Hub-Steuerelemente erfolgt, die Sie in diesem Schritt angeben.

So richten Sie Datenquellen ein

1. Passen Sie unter Datenquellenname den Datenquellennamen nach Bedarf an.
2. Passen Sie unter Methode zur Erfassung von Beweisen die Auswahl nach Bedarf an.

   a. Wenn Sie möchten, dass Audit Manager Beweise sammelt, wählen Sie Automatisiert und gehen Sie wie folgt vor:

      - Prüfen Sie unter Datenquellentyp, woher Audit Manager automatisierte Beweise sammelt, und ändern Sie sie nach Bedarf.
        - Wählen Sie für AWS CloudTrail ein Schlüsselwort für den Ereignisnamen aus der Dropdownliste aus.
        - Wählen Sie für AWS Config einen Regeltyp und dann ein Schlüsselwort für die Regel-ID aus der Dropdownliste aus.
        - Wählen Sie für AWS Security Hub eine Security Hub-Kontrolle aus der Dropdownliste aus.
        - Wählen Sie für AWS API-Aufrufe einen API-Aufruf und anschließend eine Häufigkeit für die Erfassung von Beweisen aus.

        > **Tip**
        >
        > Eine Übersicht über die einzelnen Datenquellentypen und zugehörige Tipps zur Fehlerbehebung finden Sie unter Überblick über automatisierte Datenquellen.

Wenn Sie Ihre Datenquellenkonfiguration mit einem Fachexperten überprüfen müssen, legen Sie die Methode zur Beweiserhebung vorerst auf Manuell fest. Auf diese Weise können Sie die Kontrolle jetzt erstellen und zu einem Framework hinzufügen und die Kontrolle dann später nach Bedarf bearbeiten.

b. Wenn Sie Ihre eigenen Beweise vorlegen möchten, wählen Sie Manuell und anschließend die Option Manuelle Beweise aus.

   - Datei-Upload – Wählen Sie diese Option, wenn für die Kontrolle Unterlagen als Beweis erforderlich sind.
   - Textantwort – Wählen Sie diese Option, wenn die Kontrolle eine Antwort auf eine Frage zur Risikobewertung benötigt.

3. (Optional) Nehmen Sie unter Zusätzliche Details alle erforderlichen Änderungen an der Beschreibung der Datenquelle oder der Beschreibung der Fehlerbehebung vor.
4. (Optional) Zum Hinzufügen einer weiteren Datenquelle wählen Sie Datenquelle hinzufügen aus.
5. (Optional) Zum Entfernen einer Datenquelle wählen Sie Entfernen aus.
6. Wählen Sie Weiter aus.

Schritt 3 (optional): Definieren Sie einen Aktionsplan

Der Aktionsplan wird von der ursprünglichen Kontrolle übernommen. Sie können diesen Aktionsplan nach Bedarf bearbeiten.

Um einen Aktionsplan zu definieren

1. Überprüfen Sie unter Titel den Titel des Aktionsplans und passen Sie ihn nach Bedarf an.
2. Überprüfen Sie unter Anweisungen zum Aktionsplan die Anweisungen und passen Sie sie nach Bedarf an.
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.

Was soll ich als Nächstes tun?

Nachdem Sie eine neue benutzerdefinierte Kontrolle erstellt haben, können Sie es einem benutzerdefinierten Framework hinzufügen. Weitere Informationen hierzu finden Sie unter Erstellen eines benutzerdefinierten Frameworks oder Bearbeiten eines benutzerdefinierten Frameworks.

Nachdem Sie eine benutzerdefinierte Kontrolle zu einem benutzerdefinierten Framework hinzugefügt haben, können Sie anhand dieses benutzerdefinierten Frameworks eine Bewertung erstellen und mit der Erfassung von Beweisen beginnen. Weitere Informationen hierzu finden Sie unter Erstellen einer Bewertung.

Wenn Sie eine benutzerdefinierte Kontrolle bearbeiten müssen, finden Sie weitere Informationen unter Bearbeiten einer benutzerdefinierten Kontrolle .

Tipps zur Fehlerbehebung finden Sie unter Behebung von Problemen mit Kontrollen und Kontrollsätzen.

Bearbeiten einer benutzerdefinierten Kontrolle

Sie können eine benutzerdefinierte Kontrolle in Audit Manager bearbeiten, indem Sie die folgenden Schritte ausführen.

Themen

Schritt 1: Bearbeiten der Kontrolldetails

Überprüfen und bearbeiten Sie zunächst die Kontrolldetails nach Bedarf.

So bearbeiten Sie Kontrolldetails

1. Öffnen Sie die AWS Audit-Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek und dann die Registerkarte Benutzerdefinierte Kontrollen 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 empfohlenen Testinformationen nach Bedarf.
6. Wählen Sie Weiter aus.

> **Tip**
>
> Um die Tags für eine Kontrolle zu bearbeiten, öffnen Sie die Kontrolle und wählen Sie die Registerkarte „Tags“. Dort können Sie die mit der Kontrolle verknüpften Tags anzeigen und bearbeiten.

Schritt 2: Bearbeiten von Datenquellen

Als Nächstes können Sie Datenquellen für die Kontrolle bearbeiten, entfernen oder hinzufügen.

> **Important**
>
> Um AWS Config und Security Hub erfolgreich als automatisierte Datenquellen zu verwenden, stellen Sie sicher, dass Sie Folgendes tun:
>
> - Folgen Sie den Anweisungen, um AWS Config einzurichten sowie Security Hub einzurichten für die Verwendung mit Audit Manager.
> - Nehmen Sie AWS Config sowohl als auch Security Hub als Services in Ihre Bewertung auf.
>
> Audit Manager kann dann jedes Mal Beweise sammeln, wenn eine Bewertung für die AWS Config Regeln oder die Security Hub-Steuerelemente erfolgt, die Sie in diesem Schritt angeben.

So bearbeiten Sie Datenquellen

1. Überprüfen Sie unter Datenquellenname den aktuellen Namen und bearbeiten Sie ihn nach Bedarf.
2. Überprüfen Sie unter Methode zur Erfassung von Beweisen die aktuelle Auswahl und bearbeiten Sie sie nach Bedarf.

a. Wenn Sie möchten, dass Audit Manager Beweise sammelt, wählen Sie Automatisiert und gehen Sie wie folgt vor:

- Prüfen Sie unter Datenquellentyp, woher Audit Manager automatisierte Beweise sammelt, und bearbeiten Sie sie nach Bedarf.
  - Wählen Sie für AWS CloudTrail ein Schlüsselwort für den Ereignisnamen aus der Dropdownliste aus.
  - Wählen Sie für AWS Config einen Regeltyp und dann ein Schlüsselwort für die Regel-ID aus der Dropdownliste aus.
  - Wählen Sie für AWS Security Hub eine Security Hub-Kontrolle aus der Dropdownliste aus.
  - Wählen Sie für AWS API-Aufrufe einen API-Aufruf und anschließend eine Häufigkeit für die Erfassung von Beweisen aus.

> **Tip**
>
> Eine Übersicht über die einzelnen Datenquellentypen und zugehörige Tipps zur Fehlerbehebung finden Sie unter Überblick über automatisierte Datenquellen.

b. Wenn Sie Ihre eigenen Beweise vorlegen möchten, wählen Sie Manuell und anschließend die Option Manuelle Beweise aus.

- Datei-Upload – Wählen Sie diese Option, wenn für die Kontrolle Unterlagen als Beweis erforderlich sind.
- Textantwort – Wählen Sie diese Option, wenn die Kontrolle eine Antwort auf eine Frage zur Risikobewertung benötigt.

3. (Optional) Nehmen Sie unter Zusätzliche Details alle erforderlichen Änderungen an der Beschreibung der Datenquelle oder der Beschreibung der Fehlerbehebung vor.
4. (Optional) Zum Hinzufügen einer weiteren Datenquelle wählen Sie Datenquelle hinzufügen aus.
5. (Optional) Zum Entfernen einer Datenquelle wählen Sie Entfernen aus.
6. Wählen Sie Weiter aus.

Schritt 3: (Optional) Bearbeiten eines Aktionsplans

Überprüfen und bearbeiten Sie als nächstes den optionalen Aktionsplan.

Um einen Aktionsplan zu bearbeiten

1. Bearbeiten Sie den Titel unter Titel nach Bedarf.
2. Bearbeiten Sie unter Anweisungen für den Aktionsplan die Anweisungen nach Bedarf.
3. Wählen Sie Weiter aus.

Schritt 4: Überprüfen und Aktualisieren 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 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.

Löschen eines benutzerdefinierten Steuerelements

Sie können die Kontrollbibliothek verwenden, um eine unerwünschte benutzerdefinierte Kontrolle zu löschen. Nachdem Sie eine Kontrolle gelöscht haben, wird sie nicht mehr in der Kontrollbibliothek angezeigt. Sie können benutzerdefinierte Kontrollen auch über die Audit Manager-API oder die 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

Eine benutzerdefinierte Kontrolle löschen (Konsole)

1. Öffnen Sie die AWS Audit-Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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 eine benutzerdefinierte Kontrolle (AWS CLI) zu löschen

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 den *`Platzhaltertext`* durch Ihre eigenen Informationen.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

Eine benutzerdefiniertes Kontrolle (API) löschen

1. Verwenden Sie die -ListControlsOperation und geben Sie den controlType als an`Custom`. Suchen Sie in der Antwort die Kontrolle, die Sie löschen möchten, und notieren Sie sich die Kontrollelement-ID.
2. Verwenden Sie die -DeleteControlOperation, um die benutzerdefinierte Kontrolle zu löschen. Verwenden Sie in der Anforderung den Parameter controlId, um die Kontrolle anzugeben, 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 enthält Informationen zur Verwendung dieser Operationen und Parameter in einem der sprachspezifischen AWS SDKs.

Änderung der Häufigkeit der Beweiserhebung für eine Kontrolle

AWS Audit Manager sammelt Beweise aus mehreren Datenquellen mit unterschiedlichen Häufigkeiten. Die Häufigkeit der Sammlung unterstützter Beweise hängt von der Art der Beweise ab, die für die Kontrolle gesammelt werden.

- 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).
- Für meldet AWS ConfigAudit Manager das Ergebnis einer Compliance-Prüfung direkt von AWS Config. Die Häufigkeit richtet sich nach den Auslösern, die in der AWS Config -Regel definiert sind.
- Für AWS Security Hub meldet Audit Manager das Ergebnis einer Compliance-Überprüfung direkt aus Security Hub. Die Frequenz folgt dem Zeitplan der Security Hub-Überprüfung.
- Für sammelt AWS CloudTrailAudit Manager kontinuierlich Beweise von CloudTrail. Sie können die Häufigkeit für diese Beweisart nicht ändern.

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

- Konfigurations-Snapshots von AWS API-Aufrufen

- Konformitätsprüfungen von AWS Config
- Konformitätsprüfungen von Security Hub
- Benutzeraktivitätsprotokolle von AWS CloudTrail

Konfigurations-Snapshots von AWS API-Aufrufen

> **Note**
>
> Das Folgende gilt nur für benutzerdefinierte Kontrollen. Sie können die Häufigkeit der Beweiserhebung für eine Standard-Kontrolle, die API-Aufrufe als Datenquelle verwendet, nicht ändern.

Wenn eine benutzerdefinierte Kontrolle AWS API-Aufrufe als Datenquellentyp verwendet, können Sie die Häufigkeit der Beweiserhebung in Audit Manager ändern, indem Sie diese 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-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im Navigationsbereich die Option Kontrollbibliothek und dann die Registerkarte Benutzerdefinierte Kontrollen 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 nach dem Datenquellenfeld, das Sie bearbeiten möchten, und überprüfen Sie, ob die folgenden Informationen korrekt sind:
   - Die Methode zur Beweiserhebung ist Automatisiert.
   - Der Datenquellentyp sind AWS -API-Aufrufe.
   - Der ausgewählte API-Aufruf ist der, für den Sie die Häufigkeit ändern möchten.
6. Wählen Sie unter Häufigkeit aus, wie oft Sie Beweise für die benutzerdefinierte Kontrolle sammeln möchten.

7. Wiederholen Sie die Schritte 5 bis 6 nach Bedarf für alle weiteren API-Aufruf-Datenquellen, die Sie bearbeiten möchten.
8. Wählen Sie Weiter aus.
9. Wählen Sie auf der Seite Einen Aktion bearbeiten Weiter aus.
10. Überprüfen Sie auf der Seite Kontrolle überprüfen und aktualisieren die Informationen für die benutzerdefinierte Kontrolle. Um die Informationen für einen Schritt zu ändern, wählen Sie Bearbeiten.
11. Wenn Sie fertig sind, wählen Sie Änderungen speichern aus.

Nachdem Sie eine Kontrolle mit AWS -API-Aufrufen als Datenquellentyp bearbeitet haben, werden die Änderungen am Folgetag um 00:00 Uhr UTC in allen aktiven Bewertungen wirksam, die die Kontrolle enthalten.

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 eine Kontrolle AWS Config als Datenquellentyp verwendet, können Sie die Häufigkeit der Beweiserhebung nicht direkt in Audit Manager ändern. Dies liegt daran, dass die Frequenz den Auslösern folgt, die in der AWS Config Regel definiert sind.

Es gibt zwei Arten von Auslösern für AWS-Config-Regeln:

1. Konfigurationsänderungen – AWS Config führt Bewertungen für die Regel aus, wenn bestimmte Arten von Ressourcen erstellt, geändert oder gelöscht werden.
2. Führt regelmäßig AWS Config Bewertungen für die Regel mit einer von Ihnen gewählten Häufigkeit aus (z. B. alle 24 Stunden).

Weitere Informationen zu den Auslösern für AWS-Config-Regelnfinden Sie unter Auslösertypen im AWS Config -Entwicklerhandbuch.

Anweisungen zur Verwaltung von finden Sie AWS-Config-Regelnunter Verwalten Ihrer AWS Config -Regeln.

Konformitätsprüfungen von Security Hub

> **Note**
>
> Das Folgende gilt sowohl für Standard-Kontrollen als auch für benutzerdefinierte Kontrollen, die Security Hub-Prüfungen als Datenquelle verwenden.

Wenn eine Kontrolle Security Hub 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-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 nach Möglichkeit durch Änderungen ausgelöste Regeln.

Weitere Informationen finden Sie im AWS Security Hub -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 von CloudTrail als Datenquellentyp verwenden, nicht ändern. Audit Manager sammelt diesen Beweistyp CloudTrail kontinuierlich aus . Die Häufigkeit ist kontinuierlich, da Benutzeraktivitäten zu jeder Tageszeit auftreten können.

Unterstützte Kontrolldatenquellen für automatisierte Beweise

Wenn Sie eine benutzerdefinierte Kontrolle in erstellen AWS Audit Manager, können Sie Ihre Kontrolle einrichten, um automatisierte Beweise aus den folgenden Datenquellentypen zu sammeln:

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS API-Aufrufe

Die folgenden Themen fassen jeden dieser automatisierten Datenquellentypen zusammen und listen die spezifischen AWS Security Hub Kontrollen, AWS Config Regeln und AWS API-Aufrufe auf, die von Audit Manager unterstützt werden.

Themen

Überblick über automatisierte Datenquellen

Die folgende Tabelle bietet eine Übersicht über jeden automatisierten Datenquellentyp.

Datenquellentyp	Beschreibung	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	Fortlaufend.	Wählen Sie aus der Liste der unterstützten Ereignisnamen aus.	Audit Manager filtert Ihre CloudTrail Protokolle nach dem von Ihnen ausgewähl	In meiner Bewertung werden

Datenquellentyp	Beschreibung	Häufigkeit der Beweissuche	Um diesen Datenquellentyp zu verwenden ...	Wenn diese Kontrolle in einer Bewertung aktiv ist ...	Verwandte Tipps zur Fehlerbehebung
	Benutzeraktivität.			ten Schlüsselwort. Die Ergebnisse werden als Beweis für Benutzeraktivitäten importiert.	von AWS CloudTrail keine Beweise für Benutzeraktivitäten gesammelt

Datenquellentyp	Beschreibung	Häufigkeit der Beweissuche	Um diesen Datenquellentyp zu verwenden ...	Wenn diese Kontrolle in einer Bewertung aktiv ist ...	Verwandte Tipps zur Fehlerbehebung
AWS Config	Erfasst einen Snapshot Ihres Ressourcensicherheitsstatus, indem Ergebnisse von gemeldet werden AWS Config.	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 ruft die Ergebnisse für diese Regel direkt von ab AWS Config. Das Ergebnis wird als Beweis für die Konformitätsprüfung importiert.	In meiner Bewertung werden keine Beweise für die Konformitätsprüfung von AWS Config gesammelt. AWS Config - Integrationsprobleme

Datenquellentyp	Beschreibung	Häufigkeit der Beweissuche	Um diesen Datenquellentyp zu verwenden ...	Wenn diese Kontrolle in einer Bewertung aktiv ist ...	Verwandte Tipps zur Fehlerbehebung
AWS Security Hub	Erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem Ergebnisse aus dem Security Hub gemeldet werden.	Basierend auf dem Zeitplan der Security Hub-Prüfung.	Wählen Sie aus der Liste der unterstützten Kontroll-IDs in Security Hub aus.	Audit Manager erhält das Ergebnis der Sicherheitsprüfung direkt von Security Hub. Das Ergebnis wird als Beweis für die Konformitätsprüfung importiert.	In meiner Bewertung werden keine Beweise für die Konformitätsprüfung von AWS Security Hub gesammelt.

Datenquellentyp	Beschreibung	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 das angegebene 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

AWS-Config-Regeln unterstützt von AWS Audit Manager

Sie können Audit Manager verwenden, um AWS Config Bewertungen als Beweis für Audits zu erfassen. Wenn Sie eine benutzerdefinierte Kontrolle erstellen oder bearbeiten, können Sie eine oder mehrere AWS Config Regeln als Datenquellenzuordnung für die Beweissuche angeben. AWS Config führt Compliance-Prüfungen basierend auf diesen Regeln durch und Audit Manager meldet die Ergebnisse als Compliance-Prüfungsnachweise.

Neben verwalteten Regeln können Sie Ihre benutzerdefinierten Regeln auch einer Kontrolldatenquelle zuordnen.

Note

- Audit Manager sammelt keine Beweise aus serviceverknüpften AWS Config Regeln, mit Ausnahme von serviceverknüpften Regeln aus Conformance Packs und aus AWS Organizations. Weitere Informationen finden Sie im Abschnitt Fehlerbehebung dieses Handbuchs.
- Audit Manager verwaltet keine AWS Config Regeln 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 hat eine Kontrolle namens 1.9 – Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert. In hat die iam-password-policy Regel 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.

Themen

Verwenden von AWS Config verwalteten Regeln mit Audit Manager

326- AWS Config verwaltete Regeln werden derzeit 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_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- 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_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- 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_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED

Unterstützte Schlüsselwörter für AWS Config verwaltete Regeln

- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEYPAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_AN_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- 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
- ECSAWSVPC_NETWORKING_ENABLED
- 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_REQUIRED
- ELBV2_MULTIPLE_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_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Verwenden von AWS Config benutzerdefinierten Regeln mit Audit Manager

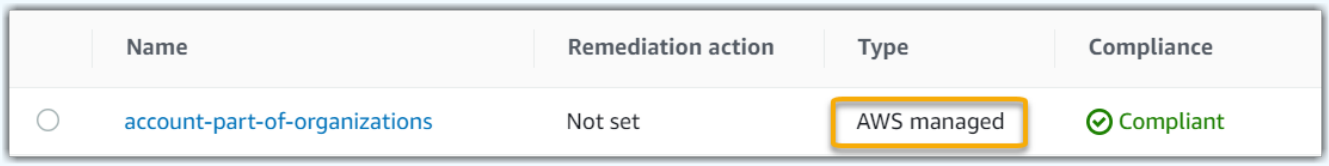
Sie können jetzt AWS Config benutzerdefinierte Regeln als Datenquelle für Audit-Berichte verwenden. Wenn eine Kontrolle über eine Datenquelle verfügt, die einer AWS Config Regel zugeordnet ist, fügt Audit Manager die Auswertung hinzu, die von der AWS Config Regel erstellt wurde.

Die benutzerdefinierten Regeln, die Sie verwenden können, hängen von der ab AWS-Konto , mit der Sie sich bei Audit Manager anmelden. Wenn Sie auf eine benutzerdefinierte Regel in 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

Anweisungen zum Erstellen einer Kontrolle, die benutzerdefinierte Regeln als Datenquelle verwendet, finden Sie unter Erstellen einer völlig neuen Kontrolle und Anpassen einer vorhandenen Kontrolle.

> **Tip**
>
> Beachten Sie, dass verwaltete Regeln nicht in der Dropdownliste der benutzerdefinierten Regeln in Audit Manager angezeigt werden.
> Wenn Sie überprüfen möchten, ob es sich bei einer AWS Config Regel um eine verwaltete Regel 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.
>
> 
>
>
> Um eine verwaltete Regel als Datenquelle zuzuordnen, können Sie in Audit Manager in der Dropdownliste der verwalteten Regeln nach dem Schlüsselwort für die verwaltete Regel suchen. Weitere Informationen finden Sie im Abschnitt Fehlerbehebung dieses Handbuchs.

Nachdem Sie Ihre benutzerdefinierten Regeln als Datenquelle für eine Kontrolle zugeordnet haben, können Sie diese Kontrolle einem benutzerdefinierten Framework in Audit Manager zuordnen. Anweisungen zum Erstellen eines benutzerdefinierten Frameworks, das Ihre benutzerdefinierte Kontrolle verwendet, finden Sie unter Erstellen eines völlig neuen Frameworks und Anpassen eines vorhandenen Frameworks. Anweisungen zum Hinzufügen Ihrer Kontrolle zu einem vorhandenen benutzerdefinierten Framework finden Sie unter Bearbeiten eines vorhandenen Frameworks.

Informationen zum Erstellen einer benutzerdefinierten Regel in AWS Configfinden Sie unter Entwickeln einer benutzerdefinierten Regel für AWS Config im AWS Config -Entwicklerhandbuch.

Fehlerbehebung bei der AWS Config Integration mit Audit Manager

Antworten auf häufig gestellte Fragen und Probleme finden Sie unter AWS Config Integration im Abschnitt Fehlerbehebung dieses Handbuchs.

AWS Security Hub -Steuerelemente, die von unterstützt werden AWS Audit Manager

Mit Audit Manager können Sie die Ergebnisse von Konformitätsprüfungen direkt vom Security Hub aus melden. Dazu geben Sie eine oder mehrere Kontrollen von Securit -Hub als Datenquellenzuordnung an, wenn Sie eine benutzerdefinierte Kontrolle in Audit Manager konfigurieren.

> **Note**
>
> - Audit Manager sammelt keine Beweise aus serviceverknüpften AWS Config Regeln, die von Security Hub erstellt wurden. Weitere Informationen finden Sie im Abschnitt Fehlerbehebung dieses Handbuchs.
> - Am 9. November 2022 führte Security Hub automatisierte Sicherheitsprüfungen ein, die auf die Anforderungen des Center for Internet Security (CIS) AWS Foundations Benchmark Version 1.4.0, Level 1 und 2 (CIS v1.4.0) abgestimmt sind. In Security Hub wird der CIS v1.4.0-Standard zusätzlich zum CIS v1.2.0-Standard unterstützt.

Themen

- Kontrollen in Security Hub mit Audit Manager verwenden
- Unterstützte Security Hub-Kontrollen

Kontrollen in Security Hub mit Audit Manager verwenden

> **Tip**
>
> Wir empfehlen, dass Sie die Einstellung für konsolidierte Kontrollergebnisse in Security Hub aktivieren, sofern sie nicht bereits aktiviert ist. Wenn Sie Security Hub am oder nach dem 23. Februar 2003 aktivieren, ist diese Einstellung standardmäßig aktiviert.

Wenn die Option „Konsolidierte Ergebnisse“ aktiviert ist, generiert Security Hub für jede Sicherheitsprüfung ein einziges Ergebnis (auch wenn dieselbe Prüfung für mehrere Standards gilt). Jede Erkenntnis aus Security Hub 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 von Security Hub 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-Einstellungen Beweise sammelt und präsentiert.

When consolidated findings is turned on

Angenommen, Sie haben die folgenden drei Sicherheitsstandards in Security Hub aktiviert: AWS FSBP, PCI DSS und CIS Benchmark v1.2.0.

- Alle drei dieser Standards verwenden dieselbe Kontrolle (IAM.4) mit derselben zugrunde liegenden AWS Config Regel (iam-root-access-key-Prüfung).
- Da die Einstellung „Konsolidierte Kontrollergebnisse“ aktiviert ist, generiert Security Hub ein einziges Ergebnis für diese Kontrolle.
- Security Hub sendet die konsolidierten Ergebnisse 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

Angenommen, Sie haben die folgenden drei Sicherheitsstandards in Security Hub aktiviert: AWS FSBP, PCI DSS und CIS Benchmark v1.2.0.

- Alle drei dieser Standards verwenden dieselbe Kontrolle (IAM.4) mit derselben zugrunde liegenden AWS Config Regel (iam-root-access-key-Prüfung).
- Da die Einstellung für konsolidierte Ergebnisse deaktiviert ist, generiert Security Hub für jeden aktivierten Standard ein separates Ergebnis pro Sicherheitsprüfung (in diesem Fall drei Ergebnisse).
- Security Hub 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 Beweise in Audit Manager (IAM.4) sammelt, drei separate Beweise, wenn die folgenden Ergebnisse von Security Hub 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-Kontrollen

Die folgenden Security Hub-Kontrollen 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 kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
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

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
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
CIS v1.2.0	2.1	CloudTrail.1
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	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6
CIS v1.2.0	3.7	CloudWatch.7
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	PCIAutoScaling.1	AutoScaling.1
PCI DSS	PCICloudTrail.1	CloudTrail.1
PCI DSS	PCICloudTrail.2	CloudTrail.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
PCI DSS	PCI.CloudTrail.3	CloudTrail.3
PCI DSS	PCICloudTrail..4	CloudTrail.4
PCI DSS	PCICodeBuild.1	CodeBuild.1
PCI DSS	PCI.CodeBuild2	CodeBuild.2
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch.1
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC 2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCIGuardDuty.1	GuardDuty.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
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
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.RedShift.1	Redshift.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
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	PCISageMaker.1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Bewährte Methoden für grundlegende Sicherheit	Account.1	Account.1
AWS Bewährte Methoden für grundlegende Sicherheit	Konto.2	Konto.2
AWS Bewährte Methoden für grundlegende Sicherheit	ACM.1	ACM.1
AWS Bewährte Methoden für grundlegende Sicherheit	ACM.2	ACM.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	APIGateway.1	APIGateway.1
AWS Bewährte Methoden für grundlegende Sicherheit	APIGateway.2	APIGateway.2
AWS Bewährte Methoden für grundlegende Sicherheit	APIGateway.3	APIGateway.3
AWS Bewährte Methoden für grundlegende Sicherheit	APIGateway.4	APIGateway.4
AWS Bewährte Methoden für grundlegende Sicherheit	APIGateway.5	APIGateway.5
AWS Bewährte Methoden für grundlegende Sicherheit	APIGateway.8	APIGateway.8
AWS Bewährte Methoden für grundlegende Sicherheit	APIGateway.9	APIGateway.9
AWS Bewährte Methoden für grundlegende Sicherheit	AppSync.2	AppSync.2
AWS Bewährte Methoden für grundlegende Sicherheit	AppSync.5	AppSync.5
AWS Bewährte Methoden für grundlegende Sicherheit	Athena.1	Athena.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	AutoScaling.1	AutoScaling.1
AWS Bewährte Methoden für grundlegende Sicherheit	AutoScaling.2	AutoScaling.2
AWS Bewährte Methoden für grundlegende Sicherheit	AutoScaling.3	AutoScaling.3
AWS Bewährte Methoden für grundlegende Sicherheit	AutoScaling.4	AutoScaling.4
AWS Bewährte Methoden für grundlegende Sicherheit	AutoScaling.5	AutoScaling.5
AWS Bewährte Methoden für grundlegende Sicherheit	AutoScaling.6	AutoScaling.6
AWS Bewährte Methoden für grundlegende Sicherheit	AutoScaling.9	AutoScaling.9
AWS Bewährte Methoden für grundlegende Sicherheit	Backup.1	Backup.1
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFormation.1	CloudFormation.1
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.1	CloudFront.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.2	CloudFront.2
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.3	CloudFront.3
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.4	CloudFront.4
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.5	CloudFront.5
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.6	CloudFront.6
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.7	CloudFront.7
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.8	CloudFront.8
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.9	CloudFront.9
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.10	CloudFront.10
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.12	CloudFront.12

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	CloudFront.13	CloudFront.13
AWS Bewährte Methoden für grundlegende Sicherheit	CloudTrail.1	CloudTrail.1
AWS Bewährte Methoden für grundlegende Sicherheit	CloudTrail.2	CloudTrail.2
AWS Bewährte Methoden für grundlegende Sicherheit	CloudTrail.3	CloudTrail.3
AWS Bewährte Methoden für grundlegende Sicherheit	CloudTrail.4	CloudTrail.4
AWS Bewährte Methoden für grundlegende Sicherheit	CloudTrail.5	CloudTrail.5
AWS Bewährte Methoden für grundlegende Sicherheit	CloudTrail.6	CloudTrail.6
AWS Bewährte Methoden für grundlegende Sicherheit	CloudTrail.7	CloudTrail.7
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.1	CloudWatch.1
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.2	CloudWatch.2

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.3	CloudWatch.3
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.4	CloudWatch.4
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.5	CloudWatch.5
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.6	CloudWatch.6
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.7	CloudWatch.7
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.8	CloudWatch.8
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.9	CloudWatch.9
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.10	CloudWatch.10
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.11	CloudWatch.11
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.12	CloudWatch.12

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.13	CloudWatch.13
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.14	CloudWatch.14
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.15	CloudWatch.15
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.16	CloudWatch.16
AWS Bewährte Methoden für grundlegende Sicherheit	CloudWatch.17	CloudWatch.17
AWS Bewährte Methoden für grundlegende Sicherheit	CodeBuild.1	CodeBuild.1
AWS Bewährte Methoden für grundlegende Sicherheit	CodeBuild.2	CodeBuild.2
AWS Bewährte Methoden für grundlegende Sicherheit	CodeBuild.3	CodeBuild.3
AWS Bewährte Methoden für grundlegende Sicherheit	CodeBuild.4	CodeBuild.4
AWS Bewährte Methoden für grundlegende Sicherheit	CodeBuild.5	CodeBuild.5

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	Config.1	Config.1
AWS Bewährte Methoden für grundlegende Sicherheit	DMS.1	DMS.1
AWS Bewährte Methoden für grundlegende Sicherheit	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.1	DocumentDB.1
AWS Bewährte Methoden für grundlegende Sicherheit	DocumentDB.2	DocumentDB.2
AWS Bewährte Methoden für grundlegende Sicherheit	DocumentDB.3	DocumentDB.3
AWS Bewährte Methoden für grundlegende Sicherheit	DocumentDB.4	DocumentDB.4

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	DocumentDB.5	DocumentDB.5
AWS Bewährte Methoden für grundlegende Sicherheit	DynamoDB.1	DynamoDB.1
AWS Bewährte Methoden für grundlegende Sicherheit	DynamoDB.2	DynamoDB.2
AWS Bewährte Methoden für grundlegende Sicherheit	DynamoDB.3	DynamoDB.3
AWS Bewährte Methoden für grundlegende Sicherheit	DynamoDB.4	DynamoDB.4
AWS Bewährte Methoden für grundlegende Sicherheit	DynamoDB.6	DynamoDB.6
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.1	EC2.1
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.2	EC2.2
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.3	EC2.3
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.4	EC2.4

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.6	EC2.6
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.7	EC2.7
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.8	EC2.8
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.9	EC2.9
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.10	EC2.10
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.12	EC2.12
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.13	EC2.13
AWS Bewährte Methoden für grundlegende Sicherheit	EC2,14	EC2,14
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.15	EC2.15
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.16	EC2.16

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.17	EC2.17
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.18	EC2.18
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.19	EC2.19
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.20	EC2.20
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.21	EC2.21
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.22	EC2.22
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.23	EC2.23
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.24	EC2.24
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.25	EC2.25
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.28	EC2.28

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	EC2.51	EC2.51
AWS Bewährte Methoden für grundlegende Sicherheit	ECR.1	ECR.1
AWS Bewährte Methoden für grundlegende Sicherheit	ECR.2	ECR.2
AWS Bewährte Methoden für grundlegende Sicherheit	ECR.3	ECR.3
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.1	ECS.1
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.2	ECS.2
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.3	ECS.3
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.4	ECS.4
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.5	ECS.5
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.8	ECS.8

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.9	ECS.9
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.10	ECS.10
AWS Bewährte Methoden für grundlegende Sicherheit	ECS.12	ECS.12
AWS Bewährte Methoden für grundlegende Sicherheit	EFS.1	EFS.1
AWS Bewährte Methoden für grundlegende Sicherheit	EFS.2	EFS.2
AWS Bewährte Methoden für grundlegende Sicherheit	EFS.3	EFS.3
AWS Bewährte Methoden für grundlegende Sicherheit	EFS.4	EFS.4
AWS Bewährte Methoden für grundlegende Sicherheit	EKS.1	EKS.1
AWS Bewährte Methoden für grundlegende Sicherheit	EKS.2	EKS.2
AWS Bewährte Methoden für grundlegende Sicherheit	EKS.8	EKS.8

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache.1	ElastiCache.1
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache.2	ElastiCache.2
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache.3	ElastiCache.3
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache.4	ElastiCache.4
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache.5	ElastiCache.5
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache.6	ElastiCache.6
AWS Bewährte Methoden für grundlegende Sicherheit	ElastiCache.7	ElastiCache.7
AWS Bewährte Methoden für grundlegende Sicherheit	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS Bewährte Methoden für grundlegende Sicherheit	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS Bewährte Methoden für grundlegende Sicherheit	ElasticBeanstalk.3	ElasticBeanstalk.3

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.1	ELB.1
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.2	ELB.2
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.3	ELB.3
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.4	ELB.4
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.5	ELB.5
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.6	ELB.6
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.7	ELB.7
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.8	ELB.8
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.9	ELB.9
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.10	ELB.10

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.12	ELB.12
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.13	ELB.13
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.14	ELB.14
AWS Bewährte Methoden für grundlegende Sicherheit	ELB.16	ELB.16
AWS Bewährte Methoden für grundlegende Sicherheit	ELBv2.1	ELB.1
AWS Bewährte Methoden für grundlegende Sicherheit	EMR.1	EMR.1
AWS Bewährte Methoden für grundlegende Sicherheit	EMR.2	EMR.2
AWS Bewährte Methoden für grundlegende Sicherheit	ES.1	ES.1
AWS Bewährte Methoden für grundlegende Sicherheit	ES.2	ES.2
AWS Bewährte Methoden für grundlegende Sicherheit	ES.3	ES.3

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	ES.4	ES.4
AWS Bewährte Methoden für grundlegende Sicherheit	ES.5	ES.5
AWS Bewährte Methoden für grundlegende Sicherheit	ES.6	ES.6
AWS Bewährte Methoden für grundlegende Sicherheit	ES.7	ES.7
AWS Bewährte Methoden für grundlegende Sicherheit	ES.8	ES.8
AWS Bewährte Methoden für grundlegende Sicherheit	EventBridge.3	EventBridge3.
AWS Bewährte Methoden für grundlegende Sicherheit	EventBridge.4	EventBridge.4
AWS Bewährte Methoden für grundlegende Sicherheit	FSx.1	FSx.1
AWS Bewährte Methoden für grundlegende Sicherheit	GuardDuty.1	GuardDuty.1
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.1	IAM.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.2	IAM.2
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.3	IAM.3
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.4	IAM.4
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.5	IAM.5
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.6	IAM.6
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.7	IAM.7
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.8	IAM.8
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.9	IAM.9
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.10	IAM.10
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.11	IAM.11

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.12	IAM.12
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.13	IAM.13
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.14	IAM.14
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.15	IAM.15
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.16	IAM.16
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.17	IAM.17
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.18	IAM.18
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.19	IAM.19
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.21	IAM.21
AWS Bewährte Methoden für grundlegende Sicherheit	IAM.22	IAM.22

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	Kinesis.1	Kinesis.1
AWS Bewährte Methoden für grundlegende Sicherheit	KMS.1	KMS.1
AWS Bewährte Methoden für grundlegende Sicherheit	KMS.2	KMS.2
AWS Bewährte Methoden für grundlegende Sicherheit	KMS.3	KMS.3
AWS Bewährte Methoden für grundlegende Sicherheit	KMS.4	KMS.4
AWS Bewährte Methoden für grundlegende Sicherheit	Lambda.1	Lambda.1
AWS Bewährte Methoden für grundlegende Sicherheit	Lambda.2	Lambda.2
AWS Bewährte Methoden für grundlegende Sicherheit	Lambda.3	Lambda.3
AWS Bewährte Methoden für grundlegende Sicherheit	Lambda.5	Lambda.5
AWS Bewährte Methoden für grundlegende Sicherheit	Macie.1	Macie.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	MQ.5	MQ.5
AWS Bewährte Methoden für grundlegende Sicherheit	MQ.6	MQ.6
AWS Bewährte Methoden für grundlegende Sicherheit	MSK.1	MSK.1
AWS Bewährte Methoden für grundlegende Sicherheit	MSK.2	MSK.2
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.1	Neptune.1
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.2	Neptune.2
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.3	Neptune.3
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.4	Neptune.4
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.5	Neptune.5
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.6	Neptune.6

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.7	Neptune.7
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.8	Neptune.8
AWS Bewährte Methoden für grundlegende Sicherheit	Neptune.9	Neptune.9
AWS Bewährte Methoden für grundlegende Sicherheit	NetworkFirewall.1	NetworkFirewall.1
AWS Bewährte Methoden für grundlegende Sicherheit	NetworkFirewall.2	NetworkFirewall.2
AWS Bewährte Methoden für grundlegende Sicherheit	NetworkFirewall.3	NetworkFirewall.3
AWS Bewährte Methoden für grundlegende Sicherheit	NetworkFirewall.4	NetworkFirewall.4
AWS Bewährte Methoden für grundlegende Sicherheit	NetworkFirewall.5	NetworkFirewall.5
AWS Bewährte Methoden für grundlegende Sicherheit	NetworkFirewall.6	NetworkFirewall.6
AWS Bewährte Methoden für grundlegende Sicherheit	NetworkFirewall.9	NetworkFirewall.9

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.1	OpenSearch.1
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.2	OpenSearch.2
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.3	OpenSearch.3
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.4	OpenSearch.4
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.5	OpenSearch.5
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.6	OpenSearch.6
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.7	OpenSearch.7
AWS Bewährte Methoden für grundlegende Sicherheit	OpenSearch.8	OpenSearch.8
AWS Bewährte Methoden für grundlegende Sicherheit	Opensearch.10	Opensearch.10
AWS Bewährte Methoden für grundlegende Sicherheit	PCA.1	PCA.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.1	RDS.1
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.2	RDS.2
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.3	RDS.3
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.4	RDS.4
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.5	RDS.5
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.6	RDS.6
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.7	RDS.7
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.8	RDS.8
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.9	RDS.9
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.10	RDS.10

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.11	RDS.11
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.12	RDS.12
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.13	RDS.13
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.14	RDS.14
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.15	RDS.15
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.16	RDS.16
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.17	RDS.17
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.18	RDS.18
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.19	RDS.19
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.20	RDS.20

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.21	RDS.21
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.22	RDS.22
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.23	RDS.23
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.24	RDS.24
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.25	RDS.25
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.26	RDS.26
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.27	RDS.27
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.34	RDS.34
AWS Bewährte Methoden für grundlegende Sicherheit	RDS.35	RDS.35
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.1	Redshift.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.2	Redshift.2
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.3	Redshift.3
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.4	Redshift.4
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.6	Redshift.6
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.7	Redshift.7
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.8	Redshift.8
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.9	Redshift.9
AWS Bewährte Methoden für grundlegende Sicherheit	Redshift.10	Redshift.10
AWS Bewährte Methoden für grundlegende Sicherheit	Route53.2	Route53.2
AWS Bewährte Methoden für grundlegende Sicherheit	S3.1	S3.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	S3.2	S3.2
AWS Bewährte Methoden für grundlegende Sicherheit	S3.3	S3.3
AWS Bewährte Methoden für grundlegende Sicherheit	S3.4	S3.4
AWS Bewährte Methoden für grundlegende Sicherheit	S3.5	S3.5
AWS Bewährte Methoden für grundlegende Sicherheit	S3.6	S3.6
AWS Bewährte Methoden für grundlegende Sicherheit	S3.7	S3.7
AWS Bewährte Methoden für grundlegende Sicherheit	S3.8	S3.8
AWS Bewährte Methoden für grundlegende Sicherheit	S3.9	S3.9
AWS Bewährte Methoden für grundlegende Sicherheit	S3.11	S3.11
AWS Bewährte Methoden für grundlegende Sicherheit	S3.12	S3.12

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	S3.13	S3.13
AWS Bewährte Methoden für grundlegende Sicherheit	S3.14	S3.14
AWS Bewährte Methoden für grundlegende Sicherheit	S3.15	S3.15
AWS Bewährte Methoden für grundlegende Sicherheit	S3.17	S3.17
AWS Bewährte Methoden für grundlegende Sicherheit	S3.19	S3.19
AWS Bewährte Methoden für grundlegende Sicherheit	S3.19	S3.20
AWS Bewährte Methoden für grundlegende Sicherheit	SageMaker.1	SageMaker.1
AWS Bewährte Methoden für grundlegende Sicherheit	SageMaker.2	SageMaker.2
AWS Bewährte Methoden für grundlegende Sicherheit	SageMaker.3	SageMaker.3
AWS Bewährte Methoden für grundlegende Sicherheit	SecretsManager.1	SecretsManager.1

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	SecretsManager.2	SecretsManager.2
AWS Bewährte Methoden für grundlegende Sicherheit	SecretsManager.3	SecretsManager.3
AWS Bewährte Methoden für grundlegende Sicherheit	SecretsManager.4	SecretsManager.4
AWS Bewährte Methoden für grundlegende Sicherheit	SNS.1	SNS.1
AWS Bewährte Methoden für grundlegende Sicherheit	SNS.2	SNS.2
AWS Bewährte Methoden für grundlegende Sicherheit	SQS.1	SQS.1
AWS Bewährte Methoden für grundlegende Sicherheit	SSM.1	SSM.1
AWS Bewährte Methoden für grundlegende Sicherheit	SSM.2	SSM.2
AWS Bewährte Methoden für grundlegende Sicherheit	SSM.3	SSM.3
AWS Bewährte Methoden für grundlegende Sicherheit	SSM.4	SSM.4

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	StepFunctions.1	StepFunctions.1
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.1	WAF.1
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.2	WAF.2
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.3	WAF.3
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.4	WAF.4
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.6	WAF.6
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.7	WAF.7
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.8	WAF.8
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.10	WAF.10
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.11	WAF.11

Sicherheitsstandard	Unterstütztes Schlüsselwort in Audit Manager (Standard kontroll-ID im Security Hub)	Dazugehörige Kontrolldokumentation (entsprechende Sicherheitskontroll-ID im Security Hub)
AWS Bewährte Methoden für grundlegende Sicherheit	WAF.12	WAF.12

Von unterstützte API-Aufrufe AWS Audit Manager

Audit Manager führt API-Aufrufe an durch, AWS-Services um einen Snapshot der Konfigurationsdetails für Ihre AWS Ressourcen zu erfassen. Sie können diese API-Aufrufe als Datenquellenzuordnung angeben, wenn Sie eine benutzerdefinierte Kontrolle in Audit Manager konfigurieren.

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.

Auf dieser Seite

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 Beweise 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-Kontoverknüpft sind.
acm_ListCertificates	Ruft eine Liste mit Zertifikat-ARNs und Domainnamen ab.
cloudtrail_DescribeTrails	Erfasst einen Snapshot der Einstellungen für einen oder mehrere Trails, die mit der aktuellen Region für Ihr AWS-Kontoverknüpft sind.
CloudWatch_DescribeAlarms	Erfasst einen Konfigurations-Snapshot der Alarme, die für Ihr AWS-Kontoverwendet werden.
config_DescribeConfigRules	Rufen Sie Details zu Ihren AWS Config Regeln ab.
config_DescribeDeliveryChannels	Erfasst einen Konfigurations-Snapshot für die Lieferkanäle in Ihrem AWS-Konto.
directconnect_DescribeDirectConnectGateways	Ruft eine Liste aller Ihrer AWS Direct Connect Gateways ab.
Directconnect_DescribeVirtualGateways	Ruft eine Liste der Virtual Private Gateways ab, die zum AWS-Kontogehören.
docdb_DescribeCertificates	Erfasst eine Liste von Zertifikaten für Ihr AWS-Konto.
docdb_DescribeDBClusterParameterGroups	Erfasst eine Liste mit `DBClusterParameterGroup` -Beschreibungen für Ihr AWS-Konto.
docdb_DescribeDBInstances	Erfasst Informationen über bereitgestellte Amazon-DynamoDB-Instances für Ihr 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

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
	`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-Kontoverknüpft sind.
DynamoDB_ListGlobalTables	Ruft eine Liste aller globalen Tabellen ab, die sich derzeit in Ihrem AWS-Kontobefinden.
DynamoDB_ListTables	Ruft eine Liste aller Tabellennamen ab, die mit Ihrem AWS-Konto und Ihrem aktuellen Endpunkt verknüpft sind.
ec2_DescribeAddresses	Erstellt einen Snapshot Ihrer Elastic-IP-Adressen.
ec2_DescribeCustomerGateways	Erfasst einen Snapshot Ihrer VPN-Kunden-Gateways.
ec2_DescribeEgressOnlyInternetGateways	Erfasst einen Snapshot Ihrer Internet-Gateways für ausgehenden Datenverkehr.
ec2_DescribeFlowLogs	Erfasst einen Snapshot Ihrer Flussprotokolle.
ec2_DescribeInstances	Erfasst einen Snapshot Ihrer Instances.
ec2_DescribeInternetGateways	Erfasst einen Snapshot Ihrer Internet-Gateways.
ec2_DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Erfasst eine Beschreibung der Zuordnungen zwischen den virtuellen Schnittstellengruppen und den Routing-Tabellen des lokalen Gateways in Ihrem AWS-Konto.
ec2_DescribeLocalGateways	Erfasst einen Snapshot Ihrer lokalen Gateways.
ec2_DescribeLocalGatewayVirtualInterfaces	Erfasst einen Snapshot der virtuellen Schnittstellen Ihres lokalen Gateways.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
ec2_DescribeNatGateways	Erfasst einen Snapshot Ihrer NAT-Gateways.
ec2_DescribeNetworkAcls	Erfasst einen Snapshot Ihrer Netzwerk-ACLs.
ec2_DescribeRouteTables	Erfasst einen Snapshot Ihrer Routing-Tabellen.
ec2_DescribeSecurityGroups	Erfasst einen Snapshot Ihrer Sicherheitsgruppen.
ec2_DescribeTransitGateways	Erfasst einen Snapshot Ihrer Transit-Gateways.
ec2_DescribeVolumes	Erfasst einen Snapshot Ihrer VPC-Endpunkte.
ec2_DescribeVpcs	Erfasst einen Snapshot Ihrer VPCs.
ec2_DescribeVpcEndpoints	Erfasst einen Snapshot Ihrer VPC-Endpunkte.
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	Erfasst einen Snapshot des Standard- AWS KMS key für die EBS-Verschlüsselung für Ihr AWS-Konto in der aktuellen Region.
ec2_GetEbsEncryptionByDefault	Beschreibt, ob die EBS-Verschlüsselung standardmäßig für Ihr AWS-Konto in der aktuellen Region aktiviert ist.
ecs_DescribeClusters	Erfasst einen Snapshot Ihrer ECS-Cluster.
eks_DescribeAddonVersions	Erfasst einen Snapshot Ihrer Add-on-Versionen.
Elasticache_DescribeCacheClusters	Erfasst einen Snapshot Ihrer bereitgestellten Cluster.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
Elasticache_DescribeServiceUpdates	Erfasst einen Snapshot von Service-Updates für Amazon ElastiCache.
Elasticfilesystem_DescribeAccessPoints	Erfasst einen Snapshot der Amazon-EFS-Zugriffspunkte in Ihrem AWS-Konto.
Elasticfilesystem_DescribeFileSystems	Erfasst einen Snapshot Ihrer Amazon EFS-Dateisysteme.
elasticloadbalancingv2_DescribeLoadBalancers	Erfasst einen Snapshot der Load Balancer in Ihrem AWS-Konto.
elasticloadbalancingv2_DescribeSSLPolicies	Erfasst einen Snapshot der Richtlinien, die Sie für die SSL-Aushandlung verwenden.
elasticloadbalancingv2_DescribeTargetGroups	Erfasst einen Snapshot Ihrer ELB-Zielgruppen.
ElasticmapReduce_ListSecurityConfigurations	Ruft eine Liste der Sicherheitskonfigurationen, die für Ihr AWS-Kontosichtbar sind, zusammen mit Datum und Uhrzeit der Erstellung sowie ihrer Namen ab.
events_ListConnections	Rufen Sie eine Liste der Amazon- EventBridge Verbindungen in Ihrem ab AWS-Konto.
events_ListEventBuses	Rufen Sie eine Liste der Amazon- EventBridge Ereignisbusse in Ihrem ab AWS-Konto, einschließlich des Standard-Ereignisbusses, benutzerdefinierter Ereignisbusse und Partner-Ereignisbusse.
events_ListEventSources	Ruft eine Liste der Partner-Ereignisquellen ab, die mit Ihrem AWS-Kontogeteilt wurden.
events_ListRules	Rufen Sie eine Liste Ihrer Amazon- EventBridge Regeln ab.
Firehose_ListDeliveryStreams	Ruft eine Liste Ihrer Bereitstellungsstreams ab.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
fsx_DescribeFileSystems	Erfasst einen Snapshot der Dateisysteme, die Ihrem AWS-Konto angehören.
Schutzvorkehrungen_ListDetectors	Rufen Sie eine Liste der `detectorIds` für Ihre Amazon-GuardDuty Detektorressourcen ab.
iam_GenerateCredentialReport	Generiert einen Bericht über Anmeldeinformationen für Ihr AWS-Konto.
iam_GetAccountPasswordPolicy	Erfasst einen Snapshot über die Passwortrichtlinie für Ihr AWS-Konto.
iam_GetAccountSummary	Erfasst einen Snapshot der IAM-Entity-Nutzung und der IAM-Kontingente in Ihrem AWS-Konto.
iam_ListGroupPolicies	Rufen Sie eine Liste der Inline-Richtlinien ab, die in eine IAM-Gruppe eingebettet sind, die in Ihrem verfügbar ist AWS-Konto.
iam_ListGroups	Rufen Sie eine Liste der IAM-Gruppen ab, die einem Pfadpräfix zugeordnet sind, das in Ihrem verfügbar ist AWS-Konto.
iam_ListOpenIDConnectProviders	Ruft eine Liste der Ressourcenobjekte des IAM OpenID Connect (OIDC)-Anbieters ab, die in Ihrem AWS-Kontodefiniert sind.
iam_ListPolicies	Ruft eine Liste aller verwalteten Richtlinien auf, die in Ihrem AWS-Kontoverfügbar sind, einschließlich der benutzerdefinierten verwalteten Richtlinien und aller von AWS-verwalteten Richtlinien.
iam_ListRoles	Rufen Sie eine Liste der IAM-Rollen ab, die einem Pfadpräfix zugeordnet sind, das in Ihrem verfügbar ist AWS-Konto.
iam_ListSAMLProviders	Ruft eine Liste der Ressourcenobjekte des SAML-Anbieters ab, die in IAM in Ihrem AWS-Kontodefiniert sind.
iam_ListUsers	Rufen Sie eine Liste der IAM-Benutzer in Ihrem ab AWS-Konto.

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
iam_ListVirtualMFADevices	Ruft eine Liste der virtuellen MFA-Geräte ab, die in Ihrem AWS-Kontodefiniert sind.
Kafka_ListClusters	Rufen Sie eine Liste der Amazon-MSK-Cluster in Ihrem ab AWS-Konto.
Kafka_ListKafkaVersions	Ruft eine Liste der Objekte der Apache Kafka-Version in Ihrem AWS-Kontoab.
Kinesis_ListStreams	Ruft eine Liste Ihrer Kinesis-Datenströme ab.
kms_GetKeyPolicy	Audit Manager verwendet diese API, um einen Snapshot über die Schlüsselrichtlinien für das AWS KMS keys in Ihrem AWS-Kontozu erfassen. Wenn Sie diese API als Datenquelle verwenden, müssen Sie den Namen eines bestimmten nicht 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 einen Snapshot darüber zu erfassen, ob die automatische Rotation für die AWS KMS keys in Ihrem aktiviert ist AWS-Konto. Wenn Sie diese API als Datenquelle verwenden, müssen Sie den Namen eines bestimmten nicht 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 .

Unterstützter API-Aufruf	Wie Audit Manager diese API verwendet, um Nachweise zu erfassen
Lambda_ListFunctions	Rufen Sie eine Liste der Lambda-Funktionen in Ihrem ab AWS-Konto, mit der jeweiligen versionsspezifischen Konfiguration.
rds_DescribeDBClusters	Erfasst einen Snapshot der vorhandenen Amazon 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.
Redshift_DescribeClusters	Erfasst einen Snapshot des bereitgestellten Amazon-Redshift-Cl usters in Ihrem AWS-Konto.
s3_GetBucketEncryption	Erfasst einen Snapshot, der die Standardverschlüsselungskon figuration 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 alle Ihre Buckets aufzulisten. Für jeden aufgelist eten Bucket führt Audit Manager dann den `GetBucket Encryption` -Vorgang aus, um Beweise für diese Ressource zu generieren. Audit Manager kann nur den Verschlüsselungsstatus für Buckets angeben, die in derselben AWS-Region wie Ihre Bewertung erstellt wurden. Wenn Sie den Verschlüsselungsstatus all Ihrer S3-Buckets über mehrere hinweg sehen müssen AWS-Regio nen, empfehlen wir Ihnen, in jedem , AWS-Region in 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.
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.

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 der API-Aufrufe, die Audit Manager unterstützt, sind paginiert. Das bedeutet, dass sie zunächst Teilergebnisse zurückgeben und nachfolgende Anfragen erfordern, um die gesamte Ergebnismenge zurückzugeben. Beispielsweise gibt der Amazon RDS-Vorgang DescribeDBInstances 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 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.

API-Aufrufe, die im AWS License Manager -Standard-Framework verwendet werden

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-APIs auf:

- 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). Zuerst ruft die `GetLicenseManagerSummary` Aktivität die ListLicenseConfigurations-API auf, die Details zu Lizenzkonfigurationen in Ihrem Konto bereitstellt. Als Nächstes werden zusätzliche Kontextdaten für jede Lizenzkonfiguration hinzugefügt, indem ListUsageForLicenseConfiguration und aufgerufen werdenListAssociationsForLicenseConfiguration. 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 CloudTrail -Ereignisnamen, die von unterstützt werden AWS Audit Manager

Sie können AWS CloudTrail Verwaltungsereignisse und globale Serviceereignisse als Beweis in Audit Manager erfassen. Dazu geben Sie den CloudTrail Ereignisnamen als Schlüsselwort für die Datenquellenzuweisung an, wenn Sie ein benutzerdefiniertes Steuerelement erstellen.

> **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 Arten von CloudTrail Ereignissen finden Sie unter -CloudTrail Konzepte im AWS CloudTrail -Benutzerhandbuch.

Als Ausnahme vom oben genannten werden die folgenden CloudTrail Ereignisse von Audit Manager nicht unterstützt:

- kms_GenerateDataKey
- kms_Decrypt

- sts_AssumeRole
- kinesisvideo_GetDataEndpoint
- Kinesisvideo_GetSignalingChannelEndpoint
- Kinesisvideo_DescribeSignalingChannel
- Kinesisvideo_DescribeStream

Ab dem 11. Mai 2023 unterstützt Audit Manager keine schreibgeschützten CloudTrail Ereignisse mehr als Schlüsselwörter für die Beweissuche. Wir haben insgesamt 3.135 schreibgeschützte Keywords entfernt. Da sowohl Kunden als auch AWS-Services APIs mit Lesevorgängen aufrufen, kommt es bei Nur-Lese-Events zu Störungen. Aus diesem Grund sammeln schreibgeschützte Stichwörter eine Menge Beweise, die für Audits weder zuverlässig noch relevant sind. Schreibgeschützte Schlüsselwörter umfassen `List-Describe`, - und -`Get`API-Aufrufe (z. B. GetObject und ListBuckets für 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.

AWS Audit Manager-Einstellungen

Sie können die Einstellungen für AWS Audit Manager jederzeit anzeigen und konfigurieren.

So greifen Sie auf Ihre Einstellungen zu

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.

Die folgenden Einstellungen sind verfügbar:

- Allgemeine Einstellungen
  - Berechtigungen
  - Datenverschlüsselung
  - Delegierter Administrator (optional)
  - AWS Config (optional)
  - Security Hub (optional)
  - Deaktivieren von AWS Audit Manager
- Bewertungseinstellungen
  - Standardmäßige Audit-Verantwortliche (optional)
  - Ziel des Bewertungsberichts (optional)
  - Benachrichtigungen (optional)
- Einstellungen für die Nachweissuche
  - Nachweissuche (optional)
  - Exportziel (optional)

Allgemeine Einstellungen

Die Registerkarte Allgemeine Einstellungen ist die Standardansicht der Einstellungsseite auf der Audit Manager-Konsole. Verwenden Sie diese Registerkarte, um Ihre allgemeinen Einstellungen für Audit Manager zu überprüfen und zu aktualisieren.

Themen

Berechtigungen

AWS Audit Manager verwendet eine serviceverknüpfte Rolle, um für sie eine Verbindung zu Datenquellen herzustellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Audit Manager.

Um die Details der serviceverknüpften Rolle zu überprüfen, die Audit Manager verwendet, wählen Sie Berechtigung für serviceverknüpfte IAM-Rollen anzeigen.

Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden serviceverknüpfter Rollen im IAM-Benutzerhandbuch.

Datenverschlüsselung

Audit Manager erstellt automatisch einen einzigartigen Von AWS verwalteter Schlüssel für die sichere Speicherung Ihrer Daten. Standardmäßig werden Ihre Audit Manager-Daten mit diesem KMS-Schlüssel verschlüsselt. Wenn Sie Ihre Datenverschlüsselungseinstellungen anpassen möchten, können Sie alternativ Ihren eigenen, vom Kunden verwalteten Schlüssel für symmetrische Verschlüsselung angeben. Die Verwendung eines eigenen Verschlüsselung gibt Ihnen mehr Flexibilität, einschließlich der Fähigkeit, Schlüssel zu erstellen, zu rotieren und zu deaktivieren.

> **Important**
>
> Damit Sie erfolgreich Bewertungsberichte erstellen und die Ergebnisse der Nachweissuche exportieren können, muss Ihr vom Kunde verwalteter Schlüssel (falls Sie einen angeben) denselben AWS-Region Ihrer Bewertung haben. Eine Liste der Regionen für Audit Manager finden Sie unter AWS Audit ManagerEndpunkte und Kontingente in Allgemeine Amazon Web Services-Referenz.

Sie können Ihre Verschlüsselungseinstellungen aktualisieren, indem Sie die Audit Manager-Konsole, AWS Command Line Interface(AWS CLI), oder die Audit Manager-API nutzen.

Audit Manager console

So aktualisieren Sie Ihre Datenverschlüsselungseinstellungen (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 (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 den *`Platzhaltertext`* 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

So aktualisieren Sie Ihre Datenverschlüsselungseinstellungen (API)

Rufen Sie den Befehl Einstellungen aktualisieren 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 des Befehls und der Parameter in einem der sprachspezifischen AWS-SDKs.

> **Note**
>
> Wenn Sie Ihre Audit Manager-Datenverschlüsselungseinstellungen ändern, gelten diese Änderungen für die neuen Bewertungen, die Sie erstellen. Dies schließt alle Bewertungsberichte und Nachweissuche-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. Eine Anleitung finden Sie unter Benutzern in anderen Konten die Verwendung eines KMS-Schlüssels erlauben im AWS Key Management Service Entwicklerhandbuch.

Anweisungen zum Erstellen von Schlüsseln finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service Benutzerhandbuch.

Delegierter Administrator (optional)

Wenn Sie AWS Organizations nutzen und die Unterstützung mehrerer Konten für Audit Manager aktivieren möchten, können Sie ein Mitgliedskonto in Ihrer Organisation als delegierten Administrator für Audit Manager festlegen.

Voraussetzungen

- Ihre Konten müssen Teil einer Organisation sein. Weitere Informationen finden Sie unter Erstellen und Verwalten einer Organisation im AWS Organizations-Benutzerhandbuch.
- Bevor Sie einen delegierten Administrator benennen, müssen Sie alle Featureen in Ihrer Organisation aktivieren. Sie müssen auch die Sicherheits-Hub-Einstellungen Ihrer Organisation konfigurieren. Auf diese Weise kann Audit Manager Sicherheits-Hub-Nachweise 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. Zur Überprüfung und Änderung Ihrer Verschlüsselungseinstellungen gehen Sie zu Datenverschlüsselung.

Wichtige Überlegungen für delegierte Administratoren in Audit Manager

Beachten Sie die folgenden Faktoren, die die Arbeitsweise des delegierten Administrators in Audit Manager definieren:

Nutzung des Verwaltungskontos

Sie können Ihr AWS Organizations-Verwaltungskonto nicht als delegierter Administrator in Audit Manager verwenden.

Verwendung delegierter Administratoren für mehrere AWS-Regionen

Wenn Sie Audit Manager in mehreren AWS-Region aktivieren möchten, müssen Sie in jeder Region separat ein delegiertes Administratorkonto einrichten. Sie sollten in Ihren Audit Manager-Einstellungen für alle Regionen dasselbe delegierte Administratorkonto angeben.

Bereinigungsaufgabe der Nachweissuche

Bevor Sie Ihr Verwaltungskonto verwenden, um einen delegierten Administrator zu entfernen oder zu ändern, stellen Sie sicher, dass sich das aktuelle delegierte Administratorkonto bei Audit Manager anmeldet und die Nachweissuche deaktiviert. Durch die Deaktivierung der Nachweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Nachweissuche 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.

Lösungen für häufig auftretende Probleme mit Organizations und delegierten Administratoren in Audit Manager finden Sie unter Behebung von Problemen mit delegierten AWS Organizations-Administratoren.

So verwalten Sie ein delegiertes Administratorkonto für Audit Manager

Sie können die Einstellungen Ihres delegierten Administratorkontos wie folgt überprüfen und ändern.

Einen delegierten Administrator hinzufügen

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 hinzu (Konsole)

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 Delegate (Delegieren).

AWS CLI

So fügen Sie einen delegierten Administrator (AWS CLI) hinzu

Führen Sie den Befehl register-organization-admin-account aus und geben Sie mit dem `--admin-account-id` Parameter die Konto-ID des delegierten Administrators an.

Ersetzen Sie im folgenden Beispiel den *`Platzhaltertext`* durch Ihre eigenen Informationen.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

So fügen Sie einen aktuellen delegierten Administrator hinzu (API)

Rufen Sie den Vorgang RegisterOrganizationAdminAccount auf und geben Sie mit dem Parameter adminAccountId die Konto-ID des delegierten Administrators an.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung des Befehls und der Parameter in einem der sprachspezifischen AWS-SDKs.

Einen delegierten Administrator ändern

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 (Konsole)

1. (Optional) Wenn der aktuelle delegierte Administrator (Konto A) die Nachweissuche 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 Nachweissuche deaktiviert.

  Durch die Deaktivierung der Nachweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als Konto A die Nachweissuche 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 Delegate (Delegieren).

AWS CLI

Bevor Sie beginnen

Wenn der aktuelle delegierte Administrator (Konto A) die Nachweissuche 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 Nachweissuche deaktiviert.

Durch die Deaktivierung der Nachweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als Konto A die Nachweissuche 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.

So ändern Sie den aktuellen delegierten Administrator (AWS CLI)

Führen Sie zunächst den Befehl deregister-organization-admin-account aus und geben Sie mit dem `--admin-account-id`-Parameter die Konto-ID des aktuellen delegierten Administrators an.

Ersetzen Sie im folgenden Beispiel den *Platzhaltertext* durch Ihre eigenen Informationen.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Führen Sie zunächst den Befehl deregister-organization-admin-account aus und geben Sie mit dem `--admin-account-id`-Parameter die Konto-ID des neuen delegierten Administrators an.

Ersetzen Sie im folgenden Beispiel den *Platzhaltertext* durch Ihre eigenen Informationen.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Bevor Sie beginnen

Wenn der aktuelle delegierte Administrator (Konto A) die Nachweissuche 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 Nachweissuche deaktiviert.

Durch die Deaktivierung der Nachweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als Konto A die Nachweissuche 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.

Um den aktuellen delegierten Administrator (API) zu ändern

Rufen Sie zunächst den Vorgang DeregisterOrganizationAdminAccount auf und geben Sie mit dem Parameter adminAccountId die Konto-ID des aktuellen delegierten Administrators an.

Rufen Sie dann den Vorgang RegisterOrganizationAdminAccount auf und geben Sie mit dem Parameter adminAccountId die Konto-ID des delegierten Administrators an.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung des Befehls und der Parameter in einem der sprachspezifischen AWS-SDKs.

Einen delegierten Administrator entfernen

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

So entfernen Sie den aktuellen delegierten Administrator (Konsole)

1. (Optional) Wenn der aktuelle delegierte Administrator die Nachweissuche 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 Nachweissuche deaktiviert.

     Durch die Deaktivierung der Nachweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Nachweissuche 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 deren 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

Bevor Sie beginnen

Wenn der aktuelle delegierte Administrator die Nachweissuche 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 Nachweissuche deaktiviert.

Durch die Deaktivierung der Nachweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Nachweissuche 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 deren Konto und es fallen weiterhin CloudTrail Lake-Speichergebühren an.

So entfernen Sie den aktuellen delegierten Administrator (AWS CLI)

Führen Sie den Befehl deregister-organization-admin-account aus und geben Sie mit dem `--admin-account-id`-Parameter die Konto-ID des delegierten Administrators an.

Ersetzen Sie im folgenden Beispiel den *`Platzhaltertext`* durch Ihre eigenen Informationen.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Bevor Sie beginnen

Wenn der aktuelle delegierte Administrator die Nachweissuche 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 Nachweissuche deaktiviert.

Durch die Deaktivierung der Nachweissuche wird automatisch der Ereignisdatenspeicher gelöscht, der im Konto erstellt wurde, als die Nachweissuche 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 deren Konto und es fallen weiterhin CloudTrail Lake-Speichergebühren an.

So entfernen Sie den aktuellen delegierten Administrator (API)

Rufen Sie den Vorgang DeregisterOrganizationAdminAccount auf und geben Sie mit dem Parameter adminAccountId die Konto-ID des aktuellen delegierten Administrators an.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung des Befehls und der Parameter in einem der sprachspezifischen AWS-SDKs.

AWS Config (optional)

Sie können Audit Manager erlauben, Ergebnisse von AWS Config zu sammeln. Wenn AWS Config aktiviert ist, kann Audit Manager Schnappschüsse Ihrer Ressourcensicherheit erfassen, indem die Ergebnisse von Regelprüfungen direkt von AWS Config gemeldet werden. Wir empfehlen die Aktivierung von AWS Config für eine optimale Benutzererfahrung in Audit Manager.

Zur Aktivierung von AWS Config, wählen Sie Aktivieren AWS Config, um zu diesem Service zu gelangen. Anweisungen zur Aktivierung von AWS Config finden Sie unter Einrichten AWS Config im AWS ConfigEntwicklerhandbuch.

Security Hub (optional)

Sie können Audit Manager erlauben, AWS Security Hub-Ergebnisse für unterstützte Compliance-Standards zu importieren. Wenn Security Hub aktiviert ist, kann Audit Manager Schnappschüsse Ihrer Ressourcensicherheit erfassen, indem die Ergebnisse der Sicherheitsprüfungen direkt von Security Hub gemeldet werden. Wir empfehlen die Aktivierung von Security Hub für eine optimale Benutzererfahrung in Audit Manager.

Um Security Hub zu aktivieren, wählen Sie Aktivieren des Security Hub, um zu diesem Service zu gelangen. Anleitung zur Aktivierung von Security Hub finden Sie unter Einrichten von Security HubAWS Security Hub im Security-Hub-Benutzerhandbuch.

Deaktivieren von 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.

> ⚠ 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.

Sie können Audit Manager über die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI) oder die Audit Manager-API deaktivieren.

Audit Manager console

Um Audit Manager (Konsole) zu deaktivieren

1. Gehen Sie auf der Registerkarte Allgemeine Einstellungen zum Abschnitt DeaktivierenAWS 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 (AWS CLI) zu deaktivieren

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 API-Vorgang UpdateSettings verwenden, um Ihre bevorzugte Datenaufbewahrungsrichtlinie festzulegen. Standardmäßig speichert Audit Manager Ihre Daten. Wenn Sie Ihre Daten löschen möchten, können Sie das Attribut DeregistrationPolicy verwenden, um die Löschung Ihrer Daten anzufordern.

Um Audit Manager (API) zu deaktivieren

Wenn Sie bereit sind, Audit Manager zu deaktivieren, rufen Sie den Vorgang deregister-account 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 Vorgänge und der Parameter in einem der sprachspezifischen AWS-SDKs.

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 Einrichten von AWS Audit Manager.

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.

Bewertungseinstellungen

Verwenden Sie diese Registerkarte, um Ihre Bewertungseinstellungen zu überprüfen und zu aktualisieren.

Themen

Standardmäßige Audit-Verantwortliche (optional)

Sie können die Standard-Audit-Verantwortlichen angeben, die primären Zugriff auf Ihre Bewertungen in Audit Manager haben.

Sie können diese Einstellungen aktualisieren, indem Sie die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI), oder die Audit Manager-API nutzen.

Audit Manager console

Sie können aus den AWS-Konten in der Tabelle wählen oder die Suchleiste verwenden, um nach anderen AWS-Konten zu suchen.

So aktualisieren Sie Ihre Standardeinstellungen für Audit-Verantwortliche (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 Ihre Standardeinstellungen für Audit-Verantwortliche (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 den *`Platzhaltertext`* 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

So aktualisieren Sie Ihre Standardeinstellungen für Audit-Verantwortliche (API)

Rufen Sie den Vorgang UpdateSettings auf und geben Sie mithilfe des Parameters DefaultProcessOwners die standardmäßigen Audit-Verantwortlichen an. Beachten Sie, dass `roleType` nur `PROCESS_OWNER` sein kann.

Weitere Informationen zu Audit-Verantwortlichen finden Sie im Abschnitt Konzepte und Terminologie dieses Handbuchs unter Audit-Verantwortliche.

Ziel des Bewertungsberichts (optional)

Wenn Sie einen Bewertungsbericht generieren, veröffentlicht Audit Manager den Bericht im S3-Bucket Ihrer Wahl. Dieser S3-Bucket wird als Ziel für Bewertungsberichte bezeichnet. Sie können den Amazon-S3-Bucket auswählen, in dem Audit Manager Ihre Bewertungsberichte speichert.

Sie können diese Einstellungen aktualisieren, indem Sie die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI), oder die Audit Manager-API nutzen.

Audit Manager console

So aktualisieren Sie die Zieleinstellungen für Ihren Bewertungsbericht (Konsole)

1. Gehen Sie auf der Registerkarte Bewertungseinstellungen zum Abschnitt Ziel des Bewertungsberichts.
2. Um einen vorhandenen Amazon S3-Bucket zu verwenden, wählen Sie einen Bucket-Namen aus dem Dropdown-Menü aus.
3. Um einen neuen Amazon S3-Bucket zu erstellen, wählen Sie Neuen Bucket erstellen.
4. Klicken Sie abschließend auf Speichern.

AWS CLI

So aktualisieren Sie die Zieleinstellungen für Ihren Bewertungsbericht (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 den *`Platzhaltertext`* durch Ihre eigenen Informationen:

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

So aktualisieren Sie die Zieleinstellungen für Ihren Bewertungsbericht (API)

Rufen Sie den Vorgang UpdateSettings auf und geben Sie den Parameter defaultAssessmentReportsDestination ein, um ein S3-Bucket anzugeben.

Weitere Anleitungen zum Erstellen eines S3-Buckets finden Sie unter Erstellen eines Buckets im Benutzerhandbuch für Amazon S3.

Konfigurationstipps für das Ziel Ihres Bewertungsberichts

Um die erfolgreiche Erstellung Ihres Bewertungsberichts sicherzustellen, empfehlen wir Ihnen, die folgenden Konfigurationen für das Ziel Ihres Bewertungsberichts zu überprüfen.

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 Ihres vom Kunden verwalteten 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 unter AWS Audit Manager-Einstellungen, Datenverschlüsselung. Anweisungen zum Ändern des S3-Buckets finden Sie unter AWS Audit Manager-Einstellungen, Ziel des Bewertungsberichts. Eine Liste der unterstützen Regionen für Audit Manager finden Sie unter AWS Audit ManagerEndpunkte 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 unter Datenverschlüsselungseinstellungen.

Kontoübergreifende S3-Buckets

Die Verwendung eines kontoübergreifenden S3-Buckets als Ziel für Ihren Bewertungsbericht wird in der Audit Manager-Konsole nicht unterstützt. Es ist möglich, mithilfe des AWS CLI oder

eines der AWS SDKs einen kontoübergreifenden Bucket als Ziel für Ihren Bewertungsbericht anzugeben. Der Einfachheit halber empfehlen wir jedoch, dies nicht zu tun. 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 den *`Platzhaltertext`* durch Ihre eigenen 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId: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/*"
            ]
        }
    ]
}
```

Benachrichtigungen (optional)

Audit Manager kann Benachrichtigungen zu dem Amazon SNS-Thema senden, das Sie in dieser Einstellung angeben. Wenn Sie dieses SNS-Thema abonniert haben, erhalten Sie Benachrichtigungen, wenn Sie sich bei Audit Manager anmelden.

Sie können diese Einstellungen aktualisieren, indem Sie die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI), oder die Audit Manager-API nutzen.

Audit Manager console

So aktualisieren Sie Ihre Benachrichtigungseinstellungen (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 (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 den *Platzhaltertext* durch Ihre eigenen Informationen:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

So aktualisieren Sie Benachrichtigungseinstellungen (API)

Rufen Sie den Vorgang UpdateSettings auf und benutzen Sie den Parameter snsTopic, um ein SNS-Thema anzugeben.

> **Note**
>
> Sie können entweder ein standardmäßiges SNS-Thema oder ein FIFO-SNS-Thema (First-In-First-Out) verwenden. Obwohl Audit Manager das Senden von Benachrichtigungen zu FIFO-Themen unterstützt, kann die Reihenfolge, in der Nachrichten gesendet werden, nicht garantiert werden.
> Wenn Sie ein Amazon-SNS-Thema verwenden möchten, für das Sie keine Rechte haben, konfigurieren Sie Ihre AWS Identity and Access Management-(IAM) Richtlinie dafür. Insbesondere müssen Sie sie so konfigurieren, dass das Veröffentlichen über den Amazon-Ressourcennamen (ARN) des Themas ermöglicht wird. Weitere Informationen über IAM finden Sie unter Identity and Access Management für AWS Audit Manager.

Weitere Informationen zur Liste der Handlungen, die Benachrichtigungen in Audit Manager auslösen, finden Sie unter Benachrichtigungen in AWS Audit Manager.

Anweisungen zum Erstellen eines Amazon-SNS-Themas finden Sie unter Erstellen eines Amazon SNS-Themas im Amazon SNS-Benutzerhandbuch.

Einstellungen für die Nachweissuche

Verwenden Sie diese Registerkarte, um Ihre Nachweissucheinstellungen zu überprüfen und zu aktualisieren.

Themen

- Nachweissuche (optional)

- Exportziel (optional)

Nachweissuche (optional)

Wir raten dringend dazu, die Nachweissuche zu aktivieren. Die Aktivierung dieser Feature ist erforderlich, wenn Sie Suchanfragen zu Ihren Nachweise ausführen möchten.

Gehen Sie wie folgt vor, um die Nachweissuche zu aktivieren, zu deaktivieren oder den Status zu überprüfen.

Nachweissuche aktivieren

Sie müssen die Nachweissuche in allen AWS-Region aktivieren, in denen Sie nach Nachweise suchen möchten. Wenn Sie ein delegierter Administrator für Audit Manager sind, aktivieren Sie die Nachweissuche, um nach Nachweisen für alle Mitgliedskonten in Ihrer Organisation zu suchen.

Erforderliche Berechtigungen zur Aktivierung der Nachweissuche

Um Evidence Finder zu aktivieren, benötigen Sie Berechtigungen zum Erstellen und Verwalten eines Ereignisdatenspeichers in CloudTrail Lake. Um die Feature nutzen zu können, benötigen Sie die Berechtigung zur Durchführung von CloudTrail Lake-Abfragen. Ein Beispiel für eine Berechtigungsrichtlinie, die Sie verwenden können, finden Sie unter Vollständigen Administratorzugriff zulassen.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung für Berechtigungen benötigen. Wenn Sie ein AWS-Administrator sind, können Sie die erforderliche Berechtigungserklärung kopieren und an eine IAM-Richtlinie anhängen.

Anforderung der Aktivierung der Nachweissuche

Sie können diese Aufgabe abschließen, indem Sie die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI), oder die Audit Manager-API nutzen.

Audit Manager console

Anforderung der Aktivierung der Nachweissuche (Konsole)

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Gehen Sie auf der Registerkarte Einstellungen für die Nachweissuche zum Abschnitt Nachweissuche.

3. Wählen Sie Erforderliche Berechtigungsrichtlinie und dann CloudTrail Lake-Berechtigungen anzeigen aus, um die erforderlichen Berechtigungen für die Nachweissuche anzuzeigen. 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

Anforderung der Aktivierung der Nachweissuche (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

Anforderung der Aktivierung der Nachweissuche (API)

Rufen Sie den Vorgang UpdateSettings auf und verwenden Sie den Parameter evidenceFinderEnabled.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieses Vorgangs und der Parameter in einem der sprachspezifischen AWS-SDKs.

Bestätigen Sie den Status der Nachweissuche

Nachdem Sie Ihre Anfrage eingereicht haben, dauert es bis zu 10 Minuten, bis die Nachweissuche 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.

Sie können den aktuellen Status der Nachweissuche mithilfe der Audit Manager-Konsole, der AWS CLI, oder der Audit Manager-API überprüfen.

Audit Manager console

So sehen Sie den aktuellen Status der Nachweissuche (Konsole)

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Überprüfen Sie unter Nachweissuche aktivieren – optional den aktuellen Status.

   Jeder Status ist wie folgt definiert:

   - Die Nachweissuche ist nicht aktiviert – Sie haben Evidence Finder noch nicht erfolgreich aktiviert.
   - Sie haben die Aktivierung der Nachweissuche beantragt – Ihre Anfrage steht noch aus, bis der Ereignisdatenspeicher erstellt wird.
   - Die Nachweissuche ist aktiviert – Der Ereignisdatenspeicher wurde erstellt. Sie können jetzt die Nachweissuche 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 Informationspanel 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 die Deaktivierung der Nachweissuche beantragt - Ihre Anfrage steht noch aus, bis der Ereignisdatenspeicher gelöscht ist.
   - Die Nachweissuche wurde deaktiviert - Die Nachweissuche wurde dauerhaft deaktiviert und der Ereignisdatenspeicher wurde gelöscht.

AWS CLI

So sehen Sie den aktuellen Status der Nachweissuche (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 Nachweissuche an.

- `ENABLE_IN_PROGRESS` - Sie haben die Aktivierung der Nachweissuche angefordert. Ein Ereignisdatenspeicher wird derzeit erstellt, um Abfragen zur Nachweismittelsuche zu unterstützen.
- `ENABLED` - Der Ereignisdatenspeicher wurde erstellt und die Nachweissuche ist aktiviert. Wir empfehlen, sieben Tage zu warten, bis der Ereignisdatenspeicher mit Ihren früheren Nachweisdaten aufgefüllt ist. In der Zwischenzeit können Sie die Nachweissuche verwenden, aber nicht alle Daten sind verfügbar, bis die Datenspeicherung abgeschlossen ist.
- `DISABLE_IN_PROGRESS` - Sie haben die Deaktivierung der Nachweissuche beantragt, Ihre Anfrage steht allerdings noch aus, bis der Ereignisdatenspeicher gelöscht ist.
- `DISABLED` - Sie haben die Nachweissuche dauerhaft deaktiviert und der Ereignisdatenspeicher wird gelöscht. Nach diesem Zeitpunkt können Sie die Nachweissuche 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

So sehen Sie den aktuellen Status der Nachweissuche (API)

Rufen Sie den Vorgang GetSettings auf, wobei der `attribute`-Parameter auf `EVIDENCE_FINDER_ENABLEMENT` gesetzt ist. Dieses Verfahren gibt die folgenden Informationen zurück:

enablementStatus

Dieses Attribut zeigt den aktuellen Status der Nachweissuche an.

- `ENABLE_IN_PROGRESS` - Sie haben die Aktivierung der Nachweissuche angefordert. Ein Ereignisdatenspeicher wird derzeit erstellt, um Abfragen zur Nachweismittelsuche zu unterstützen.
- `ENABLED` - Der Ereignisdatenspeicher wurde erstellt und die Nachweissuche ist aktiviert. Wir empfehlen, sieben Tage zu warten, bis der Ereignisdatenspeicher mit Ihren früheren Nachweisdaten aufgefüllt ist. In der Zwischenzeit können Sie die Nachweissuche verwenden, aber nicht alle Daten sind verfügbar, bis die Datenspeicherung abgeschlossen ist.
- `DISABLE_IN_PROGRESS` - Sie haben die Deaktivierung der Nachweissuche beantragt, Ihre Anfrage steht allerdings noch aus, bis der Ereignisdatenspeicher gelöscht wird.
- `DISABLED` - Sie haben die Nachweissuche dauerhaft deaktiviert und der Ereignisdatenspeicher wird gelöscht. Nach diesem Zeitpunkt können Sie die Nachweissuche 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 unter evidenceFinderEnablement in der API-Referenz von Audit Manager.

Nachweissuche deaktivieren

Wenn Sie die Nachweissuche nicht mehr verwenden möchten, können Sie diese Feature jederzeit deaktivieren.

> **Warning**
>
> Wenn Sie die Nachweissuche deaktivieren, wird der von Audit Manager erstellte CloudTrail Lake-Ereignisdatenspeicher gelöscht. Daher können Sie die Feature nicht erneut aktivieren.

Um die Nachweissuche nach der Deaktivierung erneut verwenden zu können, müssen Sie AWS Audit Manager deaktivieren und den Service anschließend vollständig wieder aktivieren.

Erforderliche Berechtigungen zur Deaktivierung der Nachweissuche

Um die Nachweissuche 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 Nachweissuche.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung für Berechtigungen benötigen. Wenn Sie ein AWS-Administrator sind, können Sie die erforderliche Berechtigungserklärung an eine IAM-Richtlinie anhängen.

Nachweissuche deaktivieren

Sie können diese Aufgabe abschließen, indem Sie die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI), oder die Audit Manager-API nutzen.

Audit Manager console

Um die Nachweissuche (Konsole) zu deaktivieren

1. Wählen Sie auf der Seite mit den Einstellungen von Audit Manager im Bereich Nachweissuche 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

Nachweissuche 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

Nachweissuche deaktivieren (API)

Rufen Sie den Vorgang UpdateSettings auf und verwenden Sie den Parameter evidenceFinderEnabled.

Für weitere Informationen klicken Sie auf einen der vorherigen Links, um mehr zu erfahren in Audit Manager API-Referenz. Dies beinhaltet Informationen zur Verwendung dieses Vorgangs und der Parameter in einem der sprachspezifischen AWS-SDKs.

Exportziel (optional)

Wenn Sie Abfragen in der Nachweissuche ausführen, können Sie Ihre Suchergebnisse in eine CSV-Datei exportieren. Verwenden Sie diese Einstellung, um den Standard-S3-Bucket auszuwählen, in dem Audit Manager Ihre exportierten Dateien speichert.

Sie können diese Einstellungen aktualisieren, indem Sie die Audit Manager-Konsole, AWS Command Line Interface (AWS CLI), oder die Audit Manager-API nutzen.

> **Important**
>
> Ihr S3-Bucket muss über die erforderlichen Berechtigungsrichtlinien verfügen, damit CloudTrail die Exportdateien darin schreiben kann. Insbesondere muss die Bucket-Richtlinie eine `s3:PutObject`-Aktion und den Bucket-ARN enthalten und CloudTrail als Dienstprinzipal auflisten. Wir stellen Ihnen eine Beispielberechtigungsrichtlinie 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 auf dieser Seite unter Konfigurationstipps für Ihr Exportziel.

Audit Manager console

So aktualisieren Sie Ihre Exportzieleinstellungen (Konsole)

1. Gehen Sie auf der Registerkarte Einstellungen für die Nachweissuche 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 (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 den *`Platzhaltertext`* durch Ihre eigenen Informationen:

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Anweisungen zum Erstellen eines S3-Buckets finden Sie unter create-bucket in der AWS CLIBefehlsreferenz.

Audit Manager API

So aktualisieren Sie Ihre Exportzieleinstellungen (API)

Rufen Sie den Vorgang UpdateSettings auf und geben Sie den Parameter defaultExportDestination ein, um ein S3-Bucket anzugeben.

Anweisungen zum Erstellen eines S3-Buckets finden Sie unter CreateBucket in der Referenz für Amazon S3 API.

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 Schlüssel (falls Sie einen angegeben haben) muss mit der Region Ihrer Bewertung übereinstimmen. 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, mithilfe des AWS CLI oder eines der AWS-SDKs einen kontoübergreifenden Bucket anzugeben. Der Einfachheit halber empfehlen wir jedoch, 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 z. B. CSV-Exporte – dem AWS-Konto, der das Objekt hochlädt. 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 den *`Platzhaltertext`* durch Ihre eigenen 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId: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/*"
          ]
      }
  ]
}
```

Benachrichtigungen in AWS Audit Manager

AWS Audit Manager kann Sie über Amazon Simple Notification Service (Amazon SNS) benachrichtigen.

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.

Voraussetzungen

Vergewissern Sie sich vor dem Einrichten von Amazon-SNS-Benachrichtigungen in Audit Manager, dass Sie die folgenden Schritte ausführen.

1. Erstellen Sie ein Thema in Amazon SNS, falls Sie noch keines haben. Eine Anleitung finden Sie unter Amazon SNS-Thema anlegen im Amazon Simple Notification Service-Entwicklerhandbuch.
2. Abonnieren Sie mindestens einen Endpunkt für das Thema. Wenn Sie beispielsweise Benachrichtigungen per Textnachricht erhalten möchten, abonnieren Sie einen SMS-Endpunkt für das Thema. Ein SMS-Endpunkt ist eine Mobiltelefonnummer. Um Benachrichtigungen per E-Mail zu erhalten, abonnieren Sie einen E-Mail-Endpunkt für das Thema. Ein E-Mail-Endpunkt ist eine E-Mail-Adresse.

   Weitere Informationen dazu erhalten Sie unter Erste Schritte im Amazon Simple Notification Service Entwicklerhandbuch.
3. (Optional) Wenn Ihr Thema AWS Key Management Service (AWS KMS) für die serverseitige Verschlüsselung (SSE) verwendet, müssen Sie der AWS KMS key-Richtlinie Berechtigungen hinzufügen. Ein Beispiel für eine Richtlinie, die Sie verwenden können, finden Sie unter Berechtigungen für einen KMS-Schlüssel, der an ein SNS-Thema angehängt ist.

Konfigurieren von Benachrichtigungen in AWS Audit Manager

Gehen Sie folgendermaßen vor, um Ihre Benachrichtigungen in AWS Audit Manager zu konfigurieren.

So konfigurieren Sie Benachrichtigungen in AWS Audit Manager

1. Öffnen Sie die Konsole von AWS Audit Manager unter https://console.aws.amazon.com/auditmanager/home.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Geben Sie unter Benachrichtigungen – optional das SNS-Thema ein, das Sie zum Empfang von Benachrichtigungen verwenden möchten.
   - Um ein vorhandenes Thema zu verwenden, wählen Sie den Namen des Themas im Dropdown-Menü aus.
   - Um ein neues Thema zu erstellen, wählen Sie Neues Thema erstellen. Dadurch gelangen Sie zur Amazon-SNS-Konsole, in der Sie ein Thema erstellen können.
4. Klicken Sie abschließend auf Save.

Hinweise

- Sie können entweder ein standardmäßiges SNS-Thema oder ein FIFO-SNS-Thema (First-In-First-Out) verwenden. Audi Manager unterstützt das Senden von Benachrichtigungen zu FIFO-Themen. Die Reihenfolge, in der Nachrichten gesendet werden, ist jedoch nicht garantiert.
- Wenn Sie ein Amazon-SNS-Thema verwenden möchten, für das Sie keine Rechte haben, müssen Sie Ihre AWS Identity and Access Management-(IAM) -Richtlinie konfigurieren. Genauer gesagt müssen Sie Ihre Richtlinie so konfigurieren, dass das Veröffentlichen des Amazon-Ressourcennamens (ARN) des Themas erlaubt wird. Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung für AWS Audit Manager.

Fehlerbehebung

Antworten auf häufig gestellte Fragen und Probleme finden Sie unter Behebung von Problemen mit Benachrichtigungen im Abschnitt Fehlerbehebung dieses Handbuchs.

Fehlerbehebung in AWS Audit Manager

Sie können die folgenden Informationen zur Behebung von Problemen verwenden, die bei der Arbeit mit AWS Audit Manager auftreten können.

Wenn die auftretenden Probleme den Rahmen der folgenden Informationen sprengen oder weiter auftreten, nachdem Sie versucht haben, sie zu beheben, wenden Sie sich an AWS Support.

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.

Themen

- In meiner Bewertung werden keine Beweise für Konfigurationsdaten für einen AWS-API-Aufruf gesammelt
- Bei meiner Bewertung werden keine Beweise von einem anderen AWS-Service gesammelt
- Meine Beweise werden in unterschiedlichen Intervallen generiert, und ich bin mir nicht sicher, wie oft sie gesammelt werden.
- Was passiert, wenn ich ein in den Bewertungsumfang fallendes Konto aus meiner Organisation entferne?
- Ich kann die Services, die für meine Bewertung gelten, nicht bearbeiten
- Was ist der Unterschied zwischen einem Service im Umfang und einem Datenquellentyp?
- Meine Bewertung konnte nicht erstellt werden
- Ich habe Audit Manager deaktiviert und dann wieder aktiviert, und jetzt sammeln meine bereits vorhandenen Bewertungen keine Beweise mehr

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. Vergewissern Sie sich, dass Sie den Audit Manager in demselben AWS-Region verwenden wie den AWS-Service, für den Sie Beweise erwarten.
3. Wenn Sie erwarten, dass von AWS Config und AWS Security Hub Beweise für Konformitätsprüfungen angezeigt werden, stellen Sie sicher, dass sowohl der AWS Config als auch die Security Hub-Konsole Ergebnisse für diese Prüfungen anzeigen. Die Ergebnisse von AWS Config und Security Hub sollten in derselben AWS-Region angezeigt werden, 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.

In meiner Bewertung werden keine Beweise für die Konformitätsprüfung von AWS Security Hub gesammelt.

Wenn Sie für eine AWS Security Hub-Kontrolle keine Beweise für die Einhaltung der Vorschriften sehen, könnte dies an einem der folgenden Probleme liegen.

Fehlende Konfiguration in AWS Security Hub

Dieses Problem kann auftreten, wenn Sie bei der Aktivierung von AWS Security Hub einige Konfigurationsschritte übersprungen haben.

Stellen Sie sicher, dass Sie Security Hub aktiviert und Ihre Einstellungen wie folgt konfiguriert haben.

Bestätigen Sie Ihre Security Hub-Einstellungen für jeden einzelnen AWS-Konto

Wenn Sie einen einzelnen AWS-Konto verwenden, überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass Sie AWS Config und die Ressourcenaufzeichnung für Ihr Konto aktiviert und konfiguriert haben.
- Bestätigen Sie, dass Sie den PCI DSS-Sicherheitsstandard für Ihr Konto aktiviert haben.
- Vergewissern Sie sich, dass Sie die Einstellung für konsolidierte Kontrollergebnisse in Security Hub aktiviert haben.

Bestätigung Ihrer Security Hub-Einstellungen für eine Organisation

Wenn Sie als Organisation handeln, überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass Sie AWS Config und die Ressourcenaufzeichnung für Ihre Organisation aktiviert und konfiguriert haben.
- Vergewissern Sie sich, dass Sie den PCI DSS-Sicherheitsstandard für jedes Mitgliedskonto der Organisation aktiviert haben.
- Vergewissern Sie sich, dass Sie die Einstellung für konsolidierte Kontrollergebnisse in Security Hub aktiviert haben.
- Vergewissern Sie sich, dass das delegierte Administratorkonto, das Sie in Security Hub verwenden, dasselbe ist, das Sie in Audit Manager verwenden.

- Vergewissern Sie sich, dass Sie Ihre Organisationskonten als Security Hub-Mitgliedskonten aktiviert haben.

Der Name eines Security Hub-Steuerelements wurde in Ihrem **`ControlMappingSource`** falsch eingegeben

Wenn Sie die Audit Manager-API verwenden, um ein benutzerdefiniertes Steuerelement zu erstellen, können Sie ein Security Hub-Steuerelement als Datenquellenzuordnung für die Beweiserhebung angeben. Dazu geben Sie eine Kontroll-ID als `keywordValue` ein.

Wenn Sie für eine Security Hub-Kontrolle keinen Beweis für die Einhaltung der Vorschriften sehen, kann es sein, dass die `keywordValue` falsch in Ihr `ControlMappingSource` hinterlegt wurde. 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-Schlüsselworts kann unterschiedlich sein. Genaueres finden Sie in der Liste der unterstützten Security Hub-Steuerschlüsselwörter.

`AuditManagerSecurityHubFindingsReceiver`Die Amazon EventBridge-Regel fehlt

Wenn Sie Audit Manager aktivieren, wird automatisch eine Regel mit dem Namen `AuditManagerSecurityHubFindingsReceiver` erstellt und in Amazon EventBridge aktiviert. Diese Regel ermöglicht es Audit Manager, Security Hub-Ergebnisse als Beweis zu sammeln.

Wenn diese Regel in der AWS-Region, in der Sie Security Hub verwenden, nicht aufgeführt bzw. aktiviert ist, kann Audit Manager keine Security Hub-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 AWS-Konto vorhanden ist. 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 AWS Support, um Unterstützung zu erhalten.

Von Security Hub erstellte servicebezogene AWS Config-Regeln

Denken Sie daran, dass Audit Manager keine Beweise anhand der servicebezogenen AWS Config-Regeln sammelt, die Security Hub erstellt. Dabei handelt es sich um eine bestimmte Art von verwalteter AWS Config-Regel, die vom Security Hub-Service aktiviert und gesteuert wird. Security Hub erstellt Instances dieser serviceverbundenen Regeln in Ihrer AWS-Umgebung, auch wenn bereits andere Instances derselben Regeln existieren. Um doppelte Beweise zu verhindern, unterstützt Audit Manager daher die Erfassung von Beweisen anhand der servicebezogenen Regeln nicht.

In meiner Bewertung werden keine Beweise für die Konformitätsprüfung von AWS Config gesammelt.

Wenn Sie für eine AWS Config-Regel keine Beweise für die Einhaltung der Vorschriften sehen, könnte dies an einem der folgenden Probleme liegen.

Die Regel-ID wurde falsch in Ihr **`ControlMappingSource`** eingegeben

Wenn Sie die Audit Manager API verwenden, um eine benutzerdefinierte Kontrolle zu erstellen, können Sie eine AWS Config-Regel als Datenquellenzuordnung für die Beweissammlung angeben. Der `keywordValue`, den Sie angeben, hängt vom Typ der Regel ab.

Wenn Sie keinen Beweis für die Einhaltung einer AWS Config-Regel sehen, könnte es sein, dass die `keywordValue` falsch in Ihr `ControlMappingSource` eingegeben wurde. 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. Zum 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
- Servicebezogene 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 servicebezogene Regel ist eine spezielle Art von verwalteter Regel, die es anderen AWS-Services ermöglicht, AWS Config-Regeln in Ihrem Konto zu erstellen. Beispielsweise verwenden einige Security Hub-Kontrollen eine servicebezogene AWS Config-Regel, um Sicherheitsprüfungen durchzuführen. Für jede Security Hub-Kontrolle, die eine servicebezogene AWS Config-Regel verwendet, erstellt Security Hub eine Instance der erforderlichen AWS Config-Regel in Ihrer AWS-Umgebung. 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 und nicht als Service im Leistungsumfang enthalten

AWS Config muss in Ihrer AWS-Konto aktiviert sein Sie muss auch als Service in den Umfang Ihrer Bewertung einbezogen werden. Nachdem Sie diese AWS Config eingerichtet haben, sammelt Audit Manager bei jeder Bewertung einer AWS Config-Regel Beweise.

Stellen Sie zunächst sicher, dass Sie Ihre AWS Config in Ihrem AWS-Konto aktiviert haben. Detaillierte Anweisungen hierzu finden Sie unter AWS Config aktivieren und einrichten..

Vergewissern Sie sich als nächstes, dass Sie AWS Config als Service in den Umfang Ihrer Bewertung aufgenommen haben. Eine Übersicht über die aktuellen Services, die für Ihre Bewertung in Frage kommen, finden Sie unter Bewertung überprüfen (Registerkarte „AWS-Services“). Um die Liste der Services zu bearbeiten, die für eine Bewertung in Frage kommen, lesen Sie In Frage kommende AWS-Services bearbeiten.

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 Beweise in Audit Manager nicht miteinander 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 zur betreffenden 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 API verwenden, um eine benutzerdefinierte Kontrolle zu erstellen, können Sie einen CloudTrail-Ereignisnamen als Datenquellenzuordnung für die Beweissammlung angeben. Geben Sie dazu den Namen des Ereignisses als den `keywordValue` ein.

Wenn Sie keine Benutzeraktivitätsbeweise für ein CloudTrail-Ereignis sehen, kann es sein, dass das `ControlMappingSource` in Ihrem `keywordValue` falsch eingegeben wurde. 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. Zum 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 API verwenden, um eine benutzerdefinierte Kontrolle zu erstellen, können Sie einen AWS API-Aufruf als Datenquellenzuordnung für die Beweissammlung angeben. Geben Sie dazu den API-Aufruf als den `keywordValue` ein.

Wenn Sie keine Hinweise auf Konfigurationsdaten für einen AWS API-Aufruf sehen, kann es sein, dass der `keywordValue` in Ihrem `ControlMappingSource` falsch eingegeben wurde. 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. Zum Beispiel `iam_ListGroups`. Informationen zur Genauigkeit finden Sie in der Liste der unterstützten API-Aufrufe.

Bei meiner Bewertung werden keine Beweise von einem anderen AWS-Service gesammelt

Wenn ein AWS-Service nicht als Umfang für Ihre Bewertung ausgewählt wurde, sammelt Audit Manager keine Beweise von Ressourcen, die sich auf diesen Service beziehen. Dies ist auch der Fall, wenn ein AWS-Service ausgewählt ist, Sie es aber in Ihrer Umgebung nicht aktiviert haben.

Wenn Sie Ihre Bewertung anhand eines benutzerdefinierten Frameworks erstellt haben, können Sie die Services im Bewertungsumfang bearbeiten. Anschließend können Sie weitere AWS-Services angeben, zu denen Sie Beweise sammeln möchten. Nachdem Sie diese Services hinzugefügt haben, sind die Beweise nach 24 Stunden verfügbar.

> **Note**
>
> Wenn Sie Ihre Bewertung anhand eines Standard-Frameworks erstellt haben, ist die Liste der im Bewertungsumfang enthaltenen AWS-Services bereits erstellt und kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager automatisch die relevanten Datenquellen und Services für Sie zuordnet und auswählt, wenn Sie eine Bewertung anhand eines Standard-Frameworks erstellen. Die Auswahl erfolgt auf der Grundlage der Anforderungen des Standard-Frameworks. Beachten Sie, dass bei Standard-Frameworks, die nur manuelle Kontrollen enthalten, im Bewertungsumfang keine AWS-Services enthalten sind.
> Die Abhilfe für die Bearbeitung des AWS-Services bei gleichzeitiger Erstellung einer Bewertung auf der Grundlage eines Standard-Frameworks besteht darin, das Standard-Framework anzupassen. Mithilfe dieser Problemumgehung können Sie das Framework verwenden, das Sie angepasst haben, um eine neue Bewertung zu erstellen. In dieser Bewertung können Sie dann angeben, welche AWS-Services in den Bewertungsumfang fallen.

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 allgemeingültige 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	Beschreibung	Häufigkeit der Beweiserhebung	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 Protokoll

Datenquellentyp	Beschreibung	Häufigkeit der Beweiserhebung	Wenn diese Kontrolle in einer Bewertung aktiv ist
			e werden als Beweis für Benutzeraktivitäten importiert.
AWS Security Hub	Erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem Ergebnisse aus dem Security Hub gemeldet werden.	Basierend auf dem Zeitplan der Security Hub-Überprüfung (in der Regel etwa alle 12 Stunden)	Audit Manager ruft das Sicherheitsergebnis direkt aus Security Hub ab. Das Ergebnis wird als Beweis für die Konformitätsprüfung importiert.
AWS Config	Erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem die Ergebnisse von AWS Configgemeldet werden.	Basierend auf den Einstellungen, die in der AWS Config-Regel definiert sind	Audit Manager ruft die Regelauswertung direkt von AWS Config ab. Die Bewertung wird als Beweis für die Konformitätsprüfung importiert.
AWSAPI-Aufrufe	Nimmt einen Schnappschuss Ihrer Ressourcenkonfiguration auf, der direkt über einen API-Aufruf an die angegebene AWS-Service gesendet wird.	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.

Unabhängig von der Häufigkeit der Beweiserhebung werden neue Beweise automatisch gesammelt, solange die Bewertung aktiv ist. Weitere Informationen finden Sie unter Häufigkeit der Beweiserhebung.

Weitere Informationen finden Sie unter Unterstützte Kontrolldatenquellen für automatisierte Beweise und Ändern der Häufigkeit der Beweiserhebung für eine Kontrolle.

Was passiert, wenn ich ein in den Bewertungsumfang fallendes Konto aus meiner Organisation entferne?

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.

Ich kann die Services, die für meine Bewertung gelten, nicht bearbeiten

Wenn Sie die Audit-Manager-Konsole verwenden, um eine Bewertung anhand eines Standard-Frameworks zu erstellen, ist die Liste der AWS-Services im Geltungsbereich standardmäßig ausgewählt. Diese Liste kann nicht bearbeitet werden. Dies liegt daran, dass Audit Manager die Datenquellen und Services automatisch für Sie zuordnet und auswählt. Diese Auswahl erfolgt gemäß den Anforderungen des Standard-Frameworks. Wenn das von Ihnen gewählte Standard-Framework nur manuelle Kontrollen enthält, fallen keine AWS-Services in den Geltungsbereich Ihrer Bewertung, und Sie können Ihrer Bewertung keine Services hinzufügen.

Wenn Sie die Liste der Services im Bewertungsumfang bearbeiten müssen, verwenden Sie den API-Vorgang UpdateAssessment (Bewertung aktualisieren), der von Audit Manager bereitgestellt wird. Alternativ können Sie das Standard-Framework anpassen und dann eine Bewertung anhand des benutzerdefinierten Frameworks erstellen.

Was ist der Unterschied zwischen einem Service im Umfang und einem Datenquellentyp?

Ein Service, der zum Bewertungsumfang gehört, ist ein AWS-Service, der als Teil Ihrer Bewertung angegeben wird. Wenn ein Service in den Bewertungsumfang fällt, sammelt Audit Manager Beweise über Ihre Nutzung dieses Dienstes und seiner Ressourcen.

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 – erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem Ergebnisse aus dem Security Hub gemeldet werden.
2. AWS Config – erfasst eine Momentaufnahme Ihrer Ressourcensicherheit, indem die Ergebnisse von gemeldet AWS Config werden.
3. AWS CloudTrail – verfolgt eine bestimmte Benutzeraktivität für eine Ressource.
4. AWS API-Aufrufe – nimmt einen Schnappschuss Ihrer Ressourcenkonfiguration auf, der direkt über einen API-Aufruf an die angegebene AWS-Service gesendet wird.

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 Auswertung Ihrer S3-Buckets zu suchen. In diesem Beispiel gilt Folgendes:

- Der Service im Bewertungsumfang ist Amazon S3
- Bei den Ressourcen, die bewertet werden, handelt es sich um Ihre S3-Buckets
- Der Typ der Datenquelle 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 Kontrolle verwendet Audit Manager CloudTrail-Protokolle, um nach allen Anmeldeereignissen der AWS-Managementkonsole zu suchen. In diesem Beispiel gilt Folgendes:

- Der Service im Bewertungsumfang 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`)

Meine Bewertung konnte nicht erstellt werden

Wenn die Erstellung Ihrer Bewertung fehlschlägt, kann dies daran liegen, dass Sie zu viele AWS-Konten in Ihrem Bewertungsumfang ausgewählt haben. Wenn Sie AWS Organizations verwenden, kann Audit Manager bis zu etwa 150 Mitgliedskonten im Rahmen einer einzigen Bewertung unterstützen. Wenn Sie diese Zahl überschreiten, schlägt die Bewertungserstellung möglicherweise fehl. Um dieses Problem zu umgehen, können Sie mehrere Bewertungen mit unterschiedlichen Konten für jede einzelne Bewertung durchführen.

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.

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
- Ich habe die obige Checkliste befolgt, und mein Bewertungsbericht konnte immer noch nicht erstellt werden

- Ich erhalte die Fehlermeldung Zugriff verweigert, wenn ich versuche, einen Bericht zu erstellen
- Ich kann den Bewertungsbericht nicht entpacken
- Wenn ich in einem Bericht einen Beweisnamen auswähle, werde ich nicht zu den Beweisdetails weitergeleitet
- Die Erstellung meines Bewertungsberichts befindet sich im Status In Bearbeitung und ich bin mir nicht sicher, wie sich das auf meine Abrechnung auswirkt
- Weitere Informationen finden Sie auch unter

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 erst, ob Ihre AWS-Region-Informationen möglicherweise nicht übereinstimmen:
   a. Stimmt der AWS-Region des vom Ihrem Kunden verwalteten Schlüssels mit dem AWS-Region Ihrer Bewertung überein?

      Wenn Sie Ihren eigenen KMS-Schlüssel für die Audit Manager-Datenverschlüsselung angegeben haben, muss sich der Schlüssel in derselben AWS-Region befinden wie Ihre Bewertung. 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 unter AWS Audit Manager-Einstellungen, Datenverschlüsselung.
   b. Stimmt der AWS-Region des vom Ihrem Kunden verwalteten Schlüssels mit dem AWS-Region Ihres S3-Buckets überein?

      Wenn Sie Ihren eigenen KMS-Schlüssel für die Audit Manager-Datenverschlüsselung angegeben haben, muss sich der Schlüssel in derselben AWS-Region befinden wie der S3-Bucket, 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 unter AWS Audit Manager-Einstellungen, Datenverschlüsselung. Anweisungen zum Ändern des S3-Buckets finden Sie unter AWS Audit Manager-Einstellungen, Ziel des Bewertungsberichts.
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. Anweisungen zur Angabe eines anderen S3-Buckets finden Sie unter AWS Audit Manager-Einstellungen, Ziel des Bewertungsberichts.

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 unter AWS Audit Manager-Einstellungen, Datenverschlüsselung. Anweisungen zum Ändern des S3-Buckets finden Sie unter AWS Audit Manager-Einstellungen, Ziel des Bewertungsberichts.

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 dem AWS-Region Ihrer Bewertung, der Region des S3-Buckets, der als Ziel für Ihren Bewertungsbericht verwendet wird, und darauf, ob für Ihre Bewertung ein vom Kunden verwaltetes AWS KMS key verwendet wird.

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 unter Datenverschlüsselung.
- 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 unter Beispiele für identitätsbasierte Richtlinien für AWS Audit Manager.

> **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 Featureieren 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 Featureiert 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 Informationen finden Sie auch unter

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 einem Bewertungsbericht keine einzelnen Suchergebnisse 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

AWS Config-Integrationsprobleme

- Ich muss mehrere AWS Config-Regeln als Datenquelle für eine einzelne Kontrolle 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 Kontrollen, 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 Audit-Verantwortlichen, die AWSAuditManagerAdministratorAccess-Richtlinie 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. Weitere Informationen finden Sie unter Kontrollstatus aktualisieren.

> **Important**
>
> Jeder AWS-Konto kann täglich nur 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 Nachweise auf eine einzelne Kontrolle hochladen müssen, laden Sie Ihre Nachweise stapelweise über mehrere Tage hinweg hoch.

Ich muss mehrere AWS Config-Regeln als Datenquelle für eine einzelne Kontrolle verwenden

Sie können für eine einzelne Kontrolle eine Kombination aus verwalteten und benutzerdefinierten Regeln verwenden. Richten Sie dazu mehrere Datenquellen für die Kontrolle ein und wählen Sie für jede einzelne Ihren bevorzugten Regeltyp aus. Sie können bis zu zehn Datenquellen für eine einzelne benutzerdefinierte Kontrolle 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 Vorgang DescribeConfigRules in der Audit Manager-Konsole auszuführen.

Um dieses Problem zu lösen, wenden Sie sich an Ihren AWS-Administrator, um Hilfe zu erhalten. 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 in AWS Config eingerichtet haben, 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.

Um dieses Problem zu lösen, wenden Sie sich an Ihren AWS Config-Administrator, um Hilfe zu erhalten. Wenn Sie ein AWS Config-Administrator sind, können Sie die Liste der ausgeschlossenen Konten aktualisieren, indem Sie den Befehl put-organization-config-rule ausführen.

Die Regel wurde nicht erfolgreich erstellt und in AWS Config aktiviert

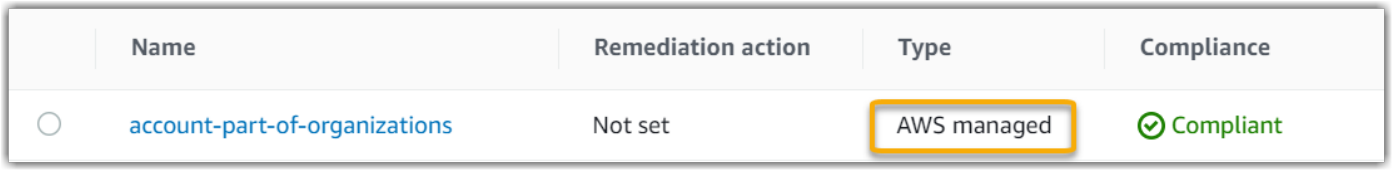
Es ist auch möglich, dass die benutzerdefinierte Regel nicht erfolgreich erstellt und aktiviert wurde. Wenn beim Erstellen der Regel ein Fehler aufgetreten ist oder die Regel nicht aktiviert ist, wird sie nicht in der Liste der verfügbaren Regeln in Audit Manager angezeigt.

Wir empfehlen, sich an Ihren AWS Config-Administrator zu wenden, um Hilfe bei diesem Problem zu erhalten.

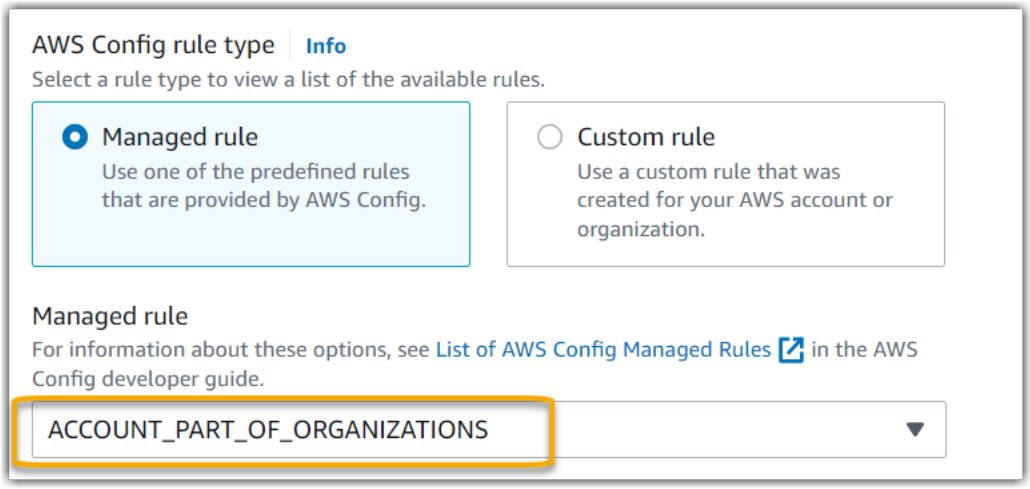
Die Regel ist eine verwaltete Regel

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.

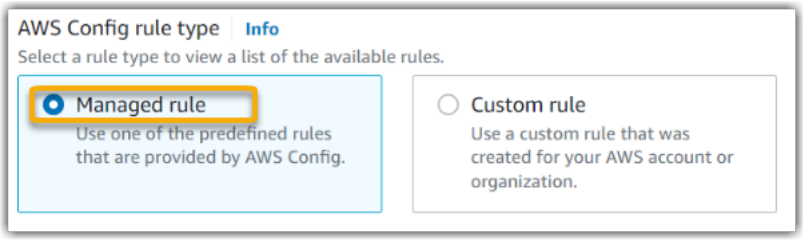


Nachdem Sie bestätigt haben, dass es sich um eine verwaltete Regel handelt, kehren Sie zu Audit Manager zurück und wählen als Regeltyp Verwaltete Regel aus. Suchen Sie dann in der Dropdownliste der verwalteten Regeln nach dem Schlüsselwort für die verwaltete Regel-ID.



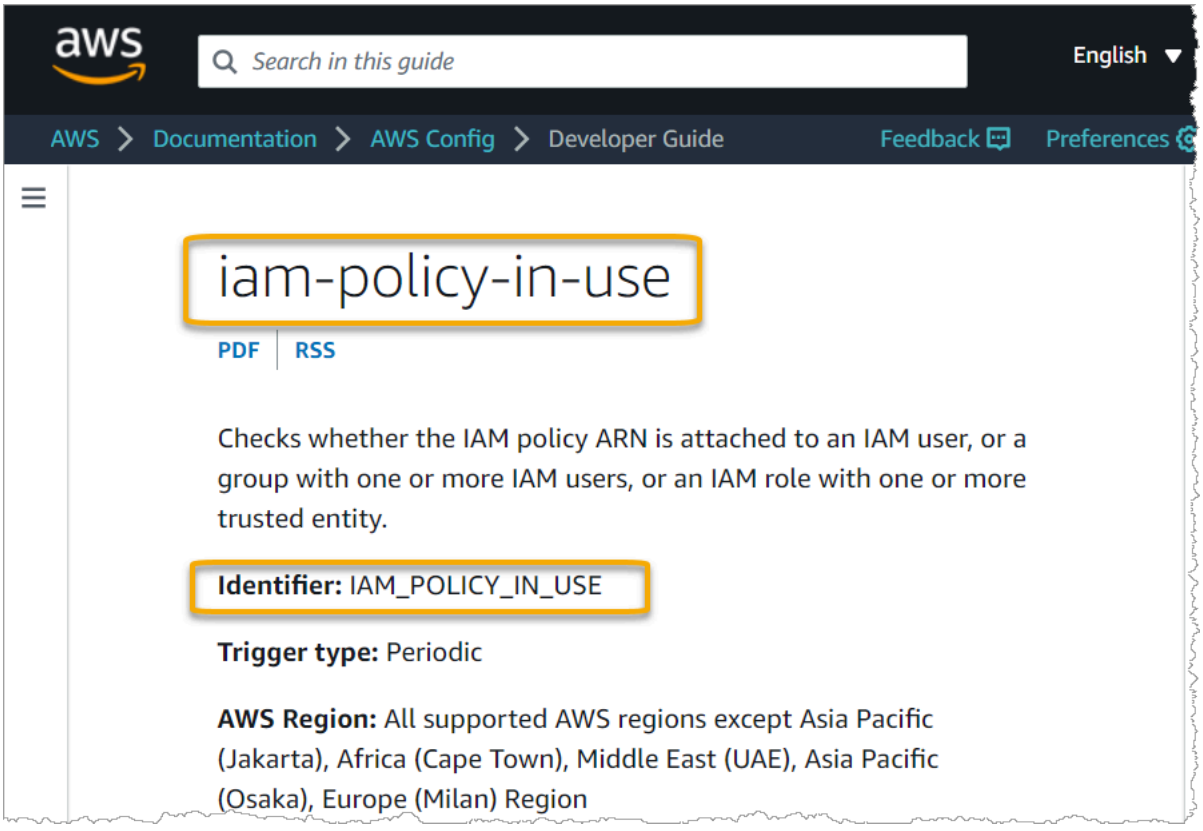
Ich kann die verwaltete Regel, die ich verwenden möchte, nicht sehen

Bevor Sie eine Regel aus der Dropdownliste in der Audit Manager-Konsole auswählen, stellen Sie sicher, dass Sie Verwaltete Regel als Regeltyp ausgewählt haben.



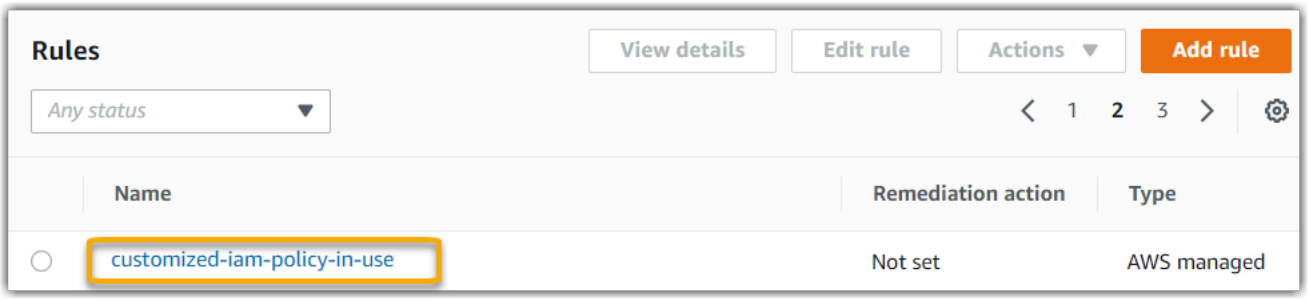
Wenn Sie die erwartete verwaltete Regel immer noch nicht sehen können, suchen Sie vielleicht nach dem Regelnamen. Stattdessen müssen Sie nach der Regel-ID suchen.

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 die ID für eine verwaltete Standardregel zu finden, überprüfen Sie die Liste der unterstützten Schlüsselwörter für in 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.

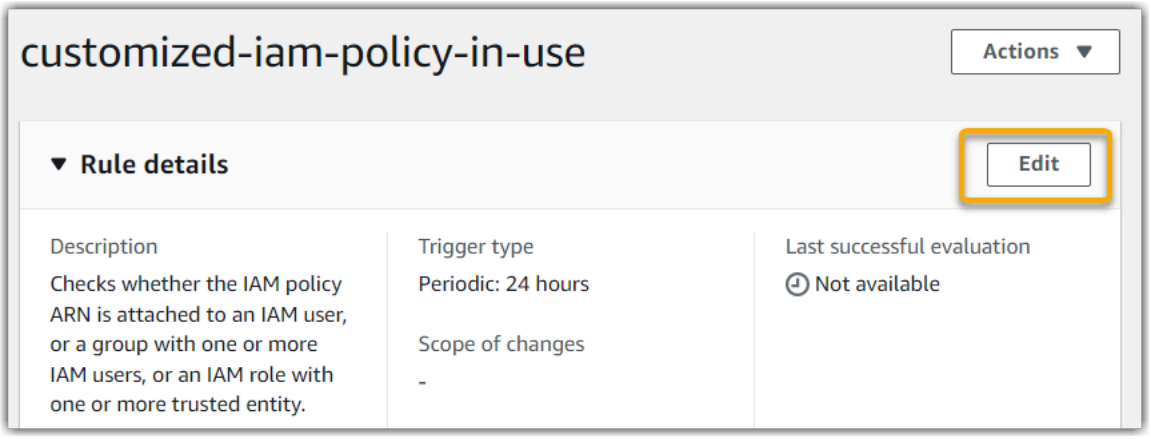


Wenn Sie eine benutzerdefinierte verwaltete Regel verwenden, können Sie die Regel-ID mithilfe der AWS Config-Konsole suchen. Angenommen, Sie möchten die verwaltete Regel mit dem Namen

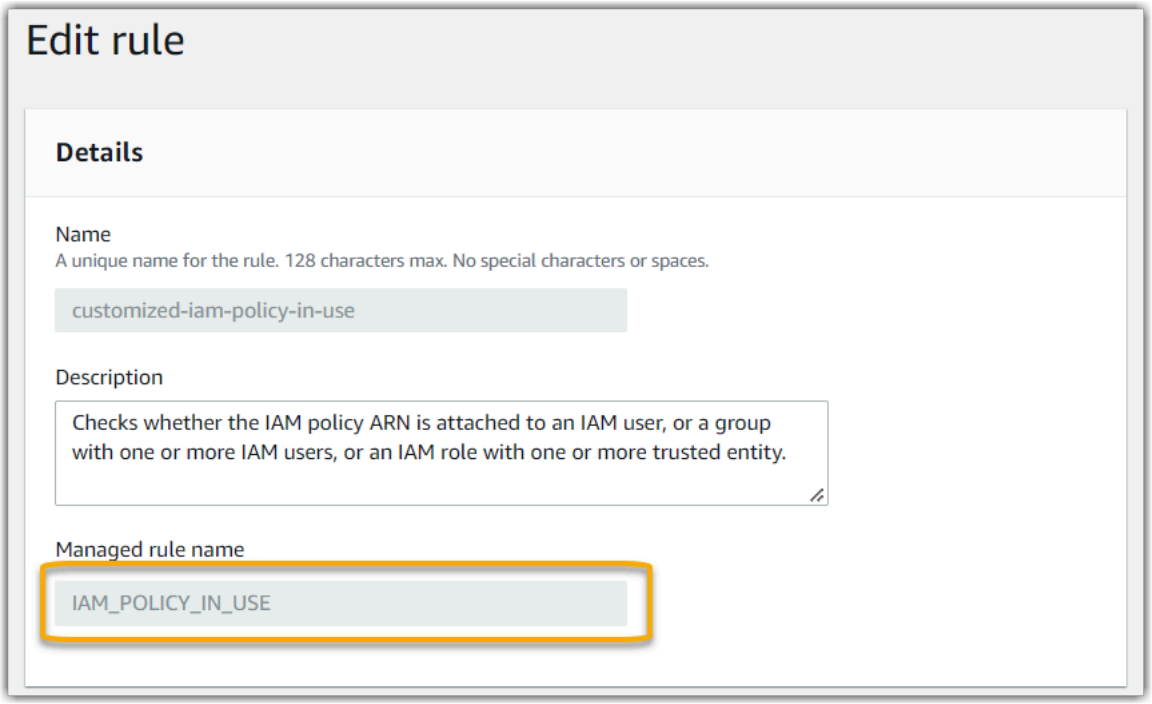
`customized-iam-policy-in-use` verwenden. Um die ID für diese Regel zu finden, rufen Sie die AWS Config-Konsole auf, wählen Sie im linken Navigationsmenü Regeln und dann die Regel in der Tabelle aus.



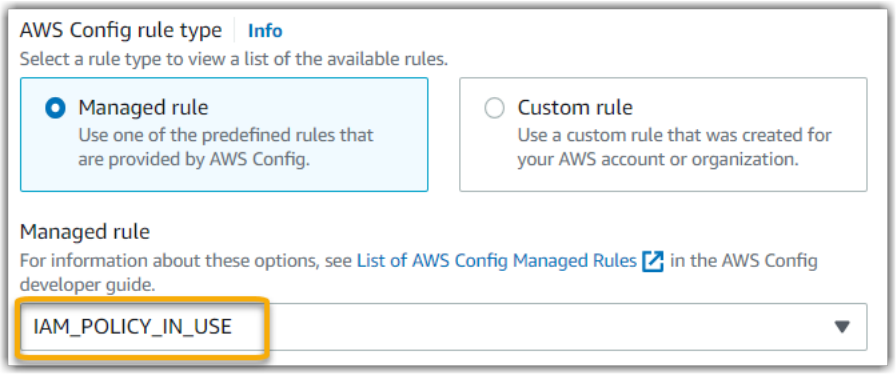
Wählen Sie Bearbeiten, um Details zur verwalteten Regel zu öffnen.



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 Kontrollen, 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 noch nicht 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 Instance von AWS Config erstellen. 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 Instance von AWS Config aktualisiert.	Audit Manager berichtet weiterhin anhand der aktualisierten Regeldefinition über Ergebnisse für diese Regel.	Keine Aktion erforderlich.
Eine benutzerdefinierte Regel wird in Ihrer Instance von AWS Config gelöscht.	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

Szenario	Was Audit Manager macht	Wichtige Informationen
		Datenquellenzuordnung verwendet haben. Auf diese Weise, d. h. indem Sie die gelöschte Regel entfernen, können Sie Ihre Datenquel leneinstellungen bereinige n. Andernfalls bleibt der Name der gelöschten Regel als unbenutzte Datenquel lenzuordnung 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. Dies 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
Sender	• Sie haben ein Framework geteilt, das benutzerdefinierte Regeln als Datenquel lenzuordnung verwendet. • Nachdem Sie das Framework geteilt haben, haben Sie eine dieser Regeln in AWS Config aktualisiert oder gelöscht.	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 Instance von AWS Config	Führen Sie die entsprechende Regelaktualisierung in Ihrer eigenen Instance von AWS Config durch.

Ihre Rolle	Szenario	Empfohlene Aktion
	neu erstellt haben, hat der Absender eine dieser Regeln aktualisiert oder gelöscht.	

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

Auf meinem Dashboard befinden sich keine Daten

Wenn die Zahlen im täglichen Snapshot-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 the section called “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 Featureiert 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.

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 zur Häufigkeit der Beweiserhebung finden Sie unter So sammelt AWS Audit Manager Beweise.

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 in AWS Organizations mehrere delegierte Administratoren unterstützt werden, 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. Anweisungen finden Sie unter Einstellungen, Delegierter Administrator.

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 mehreren AWS-Region aktivieren möchten, 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 Datenverschlüsselung.

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 unter Datenverschlüsselung.
- 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 unter Beispiele für identitätsbasierte Richtlinien für AWS Audit Manager.

> **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 AWS-Konto angezeigt, wenn Sie die Konten im Bewertungsumfang angeben.

- Bei bestehenden Bewertungen können Sie den Bewertungsbereich manuell bearbeiten, um das erneut verknüpfte Mitgliedskonto hinzuzufügen. Eine Anleitung dazu finden Sie unter AWS-Konten-Bewertungsumfang bearbeiten.
- Für neue Bewertungen können Sie das erneut verknüpfte Konto bei der Einrichtung des Tests hinzufügen. Eine Anleitung finden Sie unter AWS-Konten-Bewertungsumfang angeben.

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

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 Informationsquellen

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, die Beweiserhebung zu aktivieren, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Diese Berechtigungen ermöglichen es Ihnen, einen Ereignisdatenspeicher in CloudTrail Lake zu erstellen und zu verwalten, der für die Unterstützung von Beweiserhebungsanfragen erforderlich ist. Mit den Berechtigungen können Sie dann Beweiserhebungsanfragen durchführen.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung für Berechtigungen benötigen. 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 der Datenauffüllung überprüfen können, finden Sie unter Bestätigen des Beweiserhebungs-Status.

Ich kann die Beweiserhebung nicht deaktivieren

Dies kann durch einen der folgenden Gründe bedingt sein.

Ihnen fehlen Berechtigungen

Wenn Sie zum ersten Mal versuchen, die Beweiserhebung zu deaktivieren, stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Mit diesen Berechtigungen können Sie einen Ereignisdatenspeicher in CloudTrail Lake aktualisieren und löschen, der zum Deaktivieren der Beweiserhebung erforderlich ist.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung für Berechtigungen benötigen. 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 Beweiserhebungs-Status.

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 Beweiserhebungs-Status.

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
- DescribeQueries
- CancelQuery
- GetQueryResults

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung für Berechtigungen benötigen. 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 Lake StartQuery-Vorgang auszuführen, stellen Sie sicher, dass Ihre `queryStatement` gültig 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 StartQuery-API kann aus verschiedenen anderen Gründen fehlschlagen. Eine vollständige Liste möglicher Fehler und Beschreibungen finden Sie unter StartAnfrage-Fehler in der AWS CloudTrail-API-Referenz.

Ich kann aus meinen Suchergebnissen nicht mehrere Bewertungsberichte erstellen

Dieser Fehler wird dadurch verursacht, dass zu viele CloudTrail Lake-Anfragen 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 dem AWS-Region Ihrer Bewertung, der Region des S3-Buckets,

der als Ziel für Ihren Bewertungsbericht verwendet wird, und darauf, ob für Ihre Bewertung ein vom Kunden verwaltetes AWS KMS key verwendet wird.

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 CreateAssessmentReport-API verwenden und Ihre Anfrageanweisung eine Validierungsausnahme zurückgibt, finden Sie in der folgenden Tabelle Anleitungen zur Behebung des Problems.

> **Note**
>
> Selbst wenn eine Anfrageanweisung in CloudTrail Featureiert, ist dieselbe Anfrage 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 AWS KMS key verwendet wird, 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 AggregatFeatureen oder Aliase, die in der `SELECT`-Klausel nicht enthalten sind	Stellen Sie sicher, dass die `ORDER BY`-Klausel keine Bedingungen enthält, die AggregatFeatureen oder Aliase verwenden.	Diese Validierung wird von der CloudTrail Startanfrage-API durchgeführt.

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 Startanfrage-API durchgeführt.

Beispiele

In den folgenden Beispielen wird gezeigt, wie Sie den `queryStatement`-Parameter beim Aufrufen des CreateAssessmentReport-Vorgangs verwenden. Bevor Sie diese Anfragen verwenden, ersetzen Sie den *`Platzhaltertext`* durch Ihren eigenen `edsId` und `assessmentId`-Werte.

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 Informationsquellen

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-ExportFeature 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 Status der Beweisauffüllung finden Sie unter Beweiserhebungs-Status bestätigen.

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 Sie Ihre Suchanfrage bearbeiten und 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. Anweisungen zur Verwendung eines anderen S3-Buckets finden Sie unter Zieleinstellungen exportieren.

4. Prüfen Sie erst, ob Ihre AWS-Region-Informationen möglicherweise nicht übereinstimmen:
   a. Stimmt der AWS-Region des vom Ihrem Kunden verwalteten Schlüssels mit dem AWS-Region 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 unter 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 unter 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-Anfragen 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 Problemen beim Teilen von Frameworks

Sie können die Informationen auf dieser Seite verwenden, um häufig auftretende Probleme bei der gemeinsamen Nutzung von Frameworks in Audit Manager zu lösen.

Themen

- Mein freigegebenes Framework verfügt über Kontrollen, 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?

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 AWS-Konto des Empfängers 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 Allgemeinen Amazon Web Services-Referenz.
2. Stellen Sie sicher, 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.

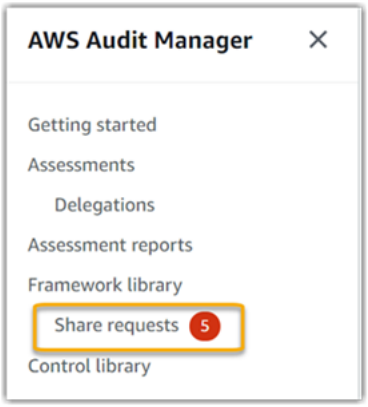
Sie können das folgende Verfahren verwenden, um nach ablaufenden Freigabeanfragen zu suchen und dem Empfänger eine optionale Erinnerung zu senden, damit er Maßnahmen ergreifen kann.

Um Benachrichtigungen für gesendete Anfragen einzusehen

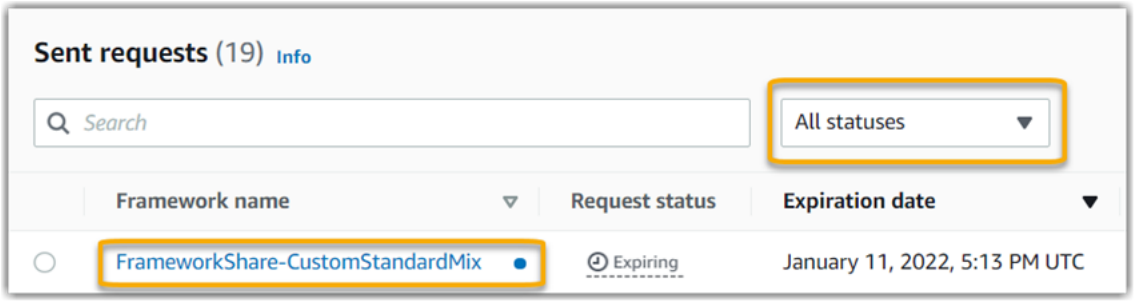
1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
2. Wenn Sie eine Benachrichtigung über eine Freigabeanfrage haben, sehen Sie in Audit Manager einen roten Punkt neben dem Navigationssymbol.

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

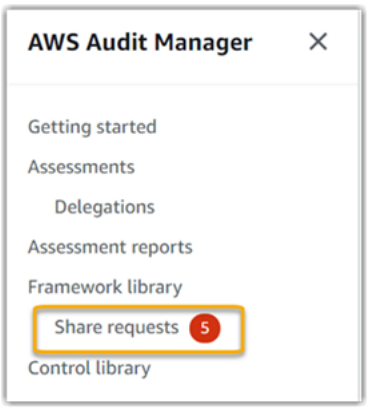
Neben eingegangenen Freigabeanfragen mit dem Status Aktiv oder Läuft ab wird ein blauer Benachrichtigungspunkt angezeigt. Audit Manager zeigt die Benachrichtigung mit dem blauen Punkt an, um Sie daran zu erinnern, Maßnahmen zur Freigabeanfrage zu ergreifen, bevor sie abläuft. Damit der blaue Benachrichtigungspunkt 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.

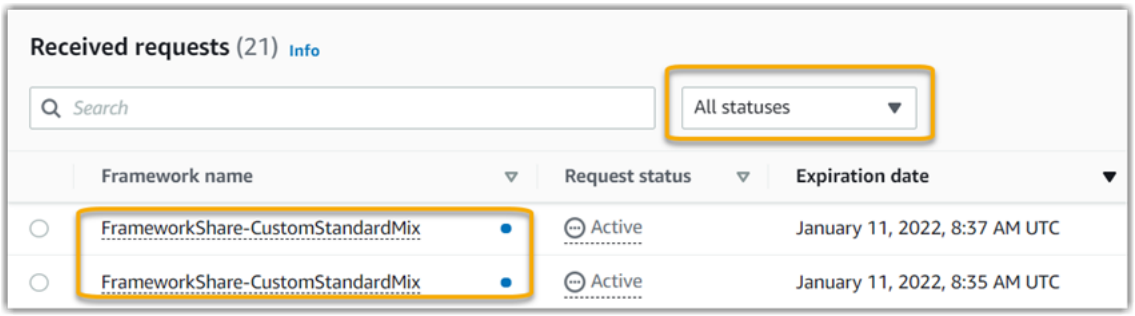
Um Benachrichtigungen für eingegangene Anfragen einzusehen

1. Öffnen Sie die AWS Audit Manager-Konsole unter https://console.aws.amazon.com/auditmanager/home.
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 freigegebenes Framework verfügt über Kontrollen, 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 noch nicht 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 Instance von AWS Config erstellen. Nachdem der Empfänger die Regeln erstellt und anschließend aktiviert hatAWS 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 Instance von AWS Config benutzerdefinierte AWS Config-Regeln erstellt werden müssen.

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, ist in Audit Manager keine Aktion 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 Instance von AWS Config aktualisiert.	Audit Manager berichtet weiterhin anhand der aktualisierten Regeldefinition über Ergebnisse für diese Regel.	Keine Aktion erforderlich.
Eine benutzerdefinierte Regel wird in Ihrer Instance von AWS Config gelöscht.	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

Szenario	Was Audit Manager macht	Wichtige Informationen
		Regel entfernen, um die Datenquelleneinstellungen Ihrer Kontrolle zu bereinige n. Andernfalls bleibt der Name der gelöschten Regel als unbenutzte Datenquel lenzuordnung erhalten.

Für Regelaktualisierungen außerhalb Ihrer AWS-Umgebung

In der AWS-Umgebung des Empfängers erkennt Audit Manager die Regelaktualisierung 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
Sender	• Sie haben ein Framework geteilt, das benutzerdefinierte Regeln als Datenquel lenzuordnung verwendet. • Nachdem Sie das Framework geteilt haben, haben Sie eine dieser Regeln in AWS Config aktualisiert oder gelöscht.	Wenden Sie sich an den Empfänger, um ihn über das Update zu informieren. Auf diese Weise können sie dasselbe Update durchführen 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 Instance von AWS Config neu erstellt haben, 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-Thema AWS KMS für die 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. Eine Beispielrichtlinie ist auf der Seite Benachrichtigungen dieses Handbuchs verfügbar.
- 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 Featureiert die Konsole nicht wie vorgesehen. Das Einrichtungsverfahren in diesem Handbuch enthält eine Richtlinie, die die Mindestberechtigungen gewährt, die für die Einrichtung 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 Audit-Verantwortliche lautet die empfohlene Richtlinie AWSAuditManagerAdministratorAccess. Für Delegierte können Sie dieses Beispiel verwenden, das 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 Audit-Verantwortliche empfehlen wir, die Richtlinie AWSAuditManagerAdministratorAccess verwenden. Weitere Informationen finden Sie unter Empfohlene Richtlinien für Benutzerrollen in 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 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 meiner AWS-Konto Zugriff auf meine Audit Manager-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien

oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Audit Manager diese Featureen unterstützt, finden Sie unter Funktionsweise AWS Audit Manager von mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Weitere Informationen finden Sie auch unter

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 Bewertungsbericht 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 in der Beweiserhebung fehl

- Ich habe in Audit Manager ein Amazon SNS-Thema angegeben, erhalte aber keine Benachrichtigungen

Kontingente und Einschränkungen für AWS Audit Manager

Ihr AWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden 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-Kontingente (aber nicht alle) sind unter dem AWS Audit Manager-Namespace in der Service Quotas-Konsole für Dienstkontingente aufgeführt. Informationen zum Anfordern einer Kontingenterhöhung finden Sie unter Verwaltung Ihrer Audit Manager-Kontingente.

Audit Manager-Standardkontingente

Die folgenden AWS-Konto-Kontingente gelten pro AWS Audit Manager pro Region

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
  - Für Berichte, bei denen für die zugehörige Bewertung ein vom Kunden verwalteter AWS KMS key verwendet wird: 3.500

Kontrollen

- Anzahl von benutzerdefinierten Kontrollen pro Konto: 500

Beweis

- 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

- Anzahl der Transaktionen pro Sekunde (TPS) über alle APIs: 20 TPS

Verwaltung Ihrer Audit Manager-Kontingente

AWS Audit Manager ist in Service Quotas, integriert, ein AWS-Service, mit dem Sie Ihre Kontingente von einem zentralen Ort aus anzeigen und verwalten können. Weitere Informationen zu Service Quotas finden Sie unter Was sind Service Quotas im Benutzerhandbuch für Service Quotas. 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 Service Quotas wird der Name der Service Quota, das angewendete Kontingent (falls verfügbar) und das AWS-Standardkontingent angezeigt. Zudem wird angezeigt, ob der Kontingentwert 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 Informationen finden Sie unter Beantragen einer Quota-Erhöhung im Service-Quotas-Benutzerhandbuch.

Sicherheit in AWS Audit Manager

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

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

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS Services in der AWS Cloud ausführt. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Externe Prüfer testen und überprüfen im Rahmen der AWS Compliance-Programme regelmäßig die Wirksamkeit unserer Sicherheit. Informationen zu den Compliance-Programmen, die für gelten AWS Audit Manager, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -ServicesIm.
- Sicherheit in der Cloud – Ihre Verantwortung wird durch den - AWS Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von einsetzen können AWS Audit Manager. Die folgenden Themen veranschaulichen, wie Sie Audit Manager zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren auch, wie Sie andere - AWS Services verwenden, die Sie bei der Überwachung und Sicherung Ihrer Audit Manager-Ressourcen unterstützen.

Themen

Datenschutz in AWS Audit Manager

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

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

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit - AWS Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API- und Benutzeraktivitätsprotokollierung mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder eine API FIPS-140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Audit Manager oder anderen AWS-Services über die Konsole, API AWS CLIoder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

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

  - Siehe auch: DeleteAssessment in der AWS Audit Manager API-Referenz zu
- Löschen eines benutzerdefinierten Frameworks
  - Siehe auch: DeleteAssessmentFramework in der AWS Audit Manager API-Referenz zu
- Löschen einer Freigabeanfrage
  - Siehe auch: DeleteAssessmentFrameworkShare in der AWS Audit Manager API-Referenz zu
- Löschen eines Bewertungsberichts
  - Siehe auch: DeleteAssessmentReport in der AWS Audit Manager API-Referenz zu
- Löschen eines benutzerdefinierten Steuerelements
  - Siehe auch: DeleteControl in der AWS Audit Manager API-Referenz zu

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 die serverseitige Verschlüsselung mit Von AWS verwaltete Schlüssel für alle seine Datenspeicher und Protokolle.

Ihre Daten werden je nach Ihren ausgewählten Einstellungen mit einem vom Kunden AWS-eigener Schlüsselverwalteten Schlüssel oder einem verschlüsselt. Wenn Sie keinen vom Kunden verwalteten Schlüssel angeben, 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 Schlüsselverschlüsselt.

Audit Manager verschlüsselt Daten wie folgt:

- In Amazon S3 gespeicherte Service-Metadaten werden AWS-eigener Schlüssel mit einem mit SSE-KMS verschlüsselt.
- In DynamoDB gespeicherte Dienst-Metadaten werden serverseitig mit KMS und einem AWS-eigener Schlüsselverschlüsselt.

- Ihre in DynamoDB gespeicherten Inhalte werden clientseitig entweder mit einem vom Kunden verwalteten Schlüssel oder einem AWS-eigener Schlüsselverschlüsselt. 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 Schlüsselsein.
- 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 die 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-Anforderungen 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 sowohl AWS-eigene Schlüssel als auch vom Kunden verwaltete Schlüssel für die Verschlüsselung aller Audit Manager-Ressourcen (Bewertungen, Kontrollen, Frameworks, Beweise 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 ein endgültiger und potenziell gefährlicher Vorgang. 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 über die AWS Management Console, die Audit Manager-API oder die AWS Command Line Interface () aktivierenAWS CLI. Anweisungen finden Sie unter Aktivieren von AWS Audit Manager.

Sie können Ihre Verschlüsselungseinstellungen jederzeit überprüfen und ändern. Anweisungen finden Sie unter Datenverschlüsselung.

Weitere Informationen zur Einrichtung von kundenverwalteten Schlüsseln finden Sie im AWS Key Management Service -Benutzerhandbuch unter Schlüssel erstellen.

Identity and Access Management für AWS Audit Manager

AWS Identity and Access Management (IAM) ist ein AWS-Service , mit dem ein Administrator den Zugriff auf - AWS Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer für die Nutzung von Audit Manager-Ressourcen authentifiziert (angemeldet) und autorisiert (über Berechtigungen verfügen) werden kann. IAM ist ein AWS-Service , den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Serviceübergreifende Confused-Deputy-Prävention
- AWS Von verwaltete Richtlinien für AWS Audit Manager
- Fehlerbehebung für AWS Audit Manager Identität und Zugriff
- Verwenden von serviceverknüpften Rollen für AWS Audit Manager

Zielgruppe

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

Service-Nutzer – Wenn Sie den Audit Manager-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Audit Manager-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf eine Features in Audit Manager nicht zugreifen können, siehe Fehlerbehebung für AWS Audit Manager Identität und Zugriff.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für Audit Manager-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Audit Manager. Es ist Ihre Aufgabe, zu bestimmen, auf welche Audit Manager-Funktionen und Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Audit Manager verwenden kann, finden Sie unter Funktionsweise AWS Audit Manager von mit IAM.

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

Authentifizierung mit Identitäten

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

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

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

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

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

AWS-Konto Root-Benutzer

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

Verbundidentität

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

Eine Verbundidentität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, ein Web-Identitätsanbieter, die AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit AWS-Services Anmeldeinformationen auf zugreift, die über eine Identitätsquelle bereitgestellt werden. Wenn Verbundidentitäten auf zugreifen AWS-Konten, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

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

IAM-Benutzer und -Gruppen

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

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI - oder AWS -API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können AWS-ServicesSie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen in auszuführen AWS, gelten Sie als Prinzipal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung AWS-Service , Anfragen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Service eine Anfrage erhält, die Interaktionen mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

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

- Anwendungen, die auf Amazon EC2 ausgeführt werden – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und - AWS CLI oder AWS -API-Anforderungen stellen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine - AWS Rolle zuzuweisen und sie für alle ihre Anwendungen verfügbar zu machen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff in , AWS indem Sie Richtlinien erstellen und sie an AWS Identitäten oder Ressourcen anfügen. Eine Richtlinie ist ein Objekt in , AWS das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen

in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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

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

Identitätsbasierte Richtlinien

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

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

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

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

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

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services AWS WAF, die ACLs unterstützen. Weitere Informationen zu ACLs finden Sie unter Zugriffssteuerungsliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs)– SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in angeben AWS Organizations. AWS Organizations ist ein Service zum Gruppieren und zentralen Verwalten mehrerer AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation

alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Die SCP beschränkt Berechtigungen für Entitäten in Mitgliedskonten, einschließlich jeder Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS bestimmt, ob eine Anforderung zugelassen werden soll, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik zur Richtlinienbewertung im IAM-Benutzerhandbuch.

Funktionsweise AWS Audit Manager von 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

IAM-Feature	Audit Manager – Support
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen Überblick über das Zusammenwirken von AWS Audit Manager und anderen - AWS Services mit den meisten IAM-Funktionen finden Sie unter -AWS Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

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 Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

AWS Audit Manager erstellt eine verwaltete Richtlinie mit dem Namen `AWSAuditManagerAdministratorAccess` für Audit Manager-Administratoren. 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 Benutzern den vollständigen Administratorzugriff auf AWS Audit Managerer lauben 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 in 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder umfassen AWS-Services.

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

Richtlinienaktionen für AWS Audit Manager

Unterstützt Richtlinienaktionen	Ja

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

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

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

Eine Liste der AWS Audit Manager Aktionen finden Sie unter Von AWS Audit Manager definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in AWS Audit Manager verwenden das folgende Präfix vor der Aktion.

```
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.

Richtlinienressourcen für AWS Audit Manager

Unterstützt Richtlinienressourcen	Ja

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS Audit Manager Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Audit Manager definierte Ressourcen in der Service-Autorisierungs-Referenz. 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-Ressourcennamen (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. gibt beispielsweise eine Liste der Bewertungsmetadaten `ListAssessments` zurück, auf die das aktuell angemeldete zugreifen kann AWS-Konto. Ein Benutzer muss daher über Berechtigungen zum Anzeigen der Bewertungen verfügen. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [
      "resource1",
      "resource2"
```

Eine Liste der Audit Manager-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Audit Managerdefinierte Ressourcen im IAM-Benutzerhandbuch. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Audit Managerdefinierte 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 die ARNs durch Kommata voneinander.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Richtlinienbedingungsschlüssel für AWS Audit Manager

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Teilweise

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

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

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

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 auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. 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. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Zugriffssteuerungslisten (ACLs) in AWS Audit Manager

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

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

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

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

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

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

Weitere Informationen zum Markieren von AWS Audit Manager Ressourcen finden Sie unter Markieren von AWS Audit Manager-Ressourcen.

Verwenden temporärer Anmeldeinformationen mit AWS Audit Manager

Unterstützt temporäre Anmeldeinformationen	Ja

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

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

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

Weiterleiten von Zugriffssitzungen für AWS Audit Manager

Unterstützt Forward Access Sessions (FAS)	Ja

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

Servicerollen für 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 Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service 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.

Serviceverknüpfte Rollen für AWS Audit Manager

Unterstützt serviceverknüpfte Rollen	Ja

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

Weitere Informationen zu serviceverknüpften Rollen für AWS Audit Managerfinden Sie 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. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

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

Einzelheiten zu den von AWS Audit Manager definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für in der Service-Autorisierungs-Referenz.

Themen

Bewährte Methoden 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. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit - AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu erteilen, verwenden Sie die -AWS verwalteten Richtlinien, die Berechtigungen für viele häufige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar AWS-Konto. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die für Ihre Anwendungsfälle spezifisch sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten:Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte

Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

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

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

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 Managerzulassen 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.

```
{
    "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"
                }
            }
        }
    ]
}
```

Für Benutzer, die nur Aufrufe an die AWS CLI oder die AWS API durchführen, müssen Sie keine Mindestberechtigungen für die Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die Sie ausführen möchten.

Benutzern den vollständigen Administratorzugriff auf AWS Audit Managererlauben

Die folgenden Beispielrichtlinien gewähren vollständigen Administratorzugriff auf AWS Audit Manager.

- Beispiel 1 (Verwaltete Richtlinie, `AWSAuditManagerAdministratorAccess`)
- Beispiel 2 (Zielberechtigungen für den Bewertungsbericht)
- Beispiel 3 (Zielberechtigungen exportieren)
- Beispiel 4 (Berechtigungen zur Aktivierung der Beweissuche)
- Beispiel 5 (Berechtigungen zum Deaktivieren der Beweissuche)

Beispiel 1 (Verwaltete Richtlinie, **`AWSAuditManagerAdministratorAccess`**)

Die Richtlinie in diesem Beispiel ist die verwaltete Richtlinie `AWSAuditManagerAdministratorAccess`. Diese Richtlinie umfasst die Möglichkeit, Audit Manager zu aktivieren und zu deaktivieren, die Audit Manager-Einstellungen zu ändern und alle Audit Manager-Ressourcen wie Bewertungen, Frameworks, Kontrollen und Bewertungsberichte zu verwalten.

```
{
    "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": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "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": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

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 den *Platzhaltertext* durch Ihre eigenen 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Beispiel 3 (Zielberechtigungen exportieren)

Die folgende Richtlinie ermöglicht es CloudTrail , Abfrageergebnisse für die Beweissuche an den angegebenen S3-Bucket zu übermitteln. Als bewährte Sicherheitsmethode trägt der globale IAM-

Bedingungsschlüssel dazu `aws:SourceArn` bei, dass nur für den Ereignisdatenspeicher in den S3-Bucket CloudTrail schreibt.

Ersetzen Sie den *`Platzhaltertext`* mit Ihren eigenen Informationen wie folgt:

- Ersetzen Sie *`DOK-ZIEL-BUCKET-BEISPIEL`* durch den S3-Bucket, den Sie als Exportziel verwenden.
- Ersetzen Sie *`myQueryRunningRegion`* durch die AWS-Region für Ihre Konfiguration geeignete .
- Ersetzen Sie *`myAccountID`* durch die AWS-Konto ID, die für verwendet wird CloudTrail. Diese ist möglicherweise nicht identisch mit der AWS-Konto -ID des S3-Buckets. Wenn es sich um einen Ereignisdatenspeicher einer Organisation handelt, müssen Sie die AWS-Konto für das Verwaltungskonto verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-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:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "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": "*"
        }
    ]
}
```

Beispiel 4 (Berechtigungen zur Aktivierung der Beweissuche)

Die folgende Berechtigungsrichtlinie ist erforderlich, wenn Sie die Beweissuch-Funktion aktivieren und verwenden möchten. Diese Richtlinienanweisung ermöglicht es Audit Manager, einen CloudTrail Lake-Ereignisdatenspeicher zu erstellen und Suchabfragen auszuführen.

```
{
    "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 5 (Berechtigungen zum Deaktivieren der Beweissuche)

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 den *Platzhaltertext* durch Ihre eigenen Informationen. 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
```

```
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Erlauben Sie der Benutzerverwaltung Zugriff auf AWS Audit Manager

In diesem Beispiel wird gezeigt, wie Sie Verwaltungszugriff auf AWS Audit Managergewähren 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
```

```
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "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": "*"
        }
    ]
}
```

Benutzern schreibgeschützten Zugriff auf gewähren AWS Audit Manager

Diese Richtlinie gewährt schreibgeschützten Zugriff auf AWS Audit Manager Ressourcen wie Bewertungen, Frameworks und Kontrollen.

```
{
    "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 enthält Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder AWS API.

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

Zulassen AWS Audit Manager des Sendens von Benachrichtigungen an Amazon SNS-Themen

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-Themen-Zugriffsrichtlinie Berechtigungen hinzuzufügen.
- Beispiel 2 – Wenn Ihr SNS-Thema AWS Key Management Service (AWS KMS) für die 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 den *`Platzhaltertext`* 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.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

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 den *Platzhaltertext* 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 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.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
```

```
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
             }
             "ArnLike": {
                  "aws:SourceArn": "arn:aws:sns:region:accountID: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 Ausführen von Abfragen für einen CloudTrail Lake-Ereignisdatenspeicher. Diese Berechtigungsrichtlinie ist erforderlich, wenn Sie die Beweissuch-Funktion verwenden möchten.

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

```
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In kann ein AWSserviceübergreifender Identitätswechsel zu einem Confused-Deputy-Problem 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 `aws:SourceAccount` globalen Bedingungskontextschlüssel `aws:SourceArn` und in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die einem anderen Service für den Zugriff auf Ihre Ressourcen AWS Audit Manager gewährt.

- 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 Datenverschlüsselung-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.

AWS Von verwaltete Richtlinien für AWS Audit Manager

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

Beachten Sie, dass von AWS verwaltete Richtlinien möglicherweise keine Berechtigungen mit den geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle - AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in verwalteten AWS Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS von verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie angefügt ist. aktualisiert am AWS wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer gestartet AWS-Service wird oder neue API-Operationen für vorhandene Services verfügbar werden.

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

Themen

- AWS Von verwaltete Richtlinie: AWSAuditManagerAdministratorAccess
- AWS Von verwaltete Richtlinie: AWSAuditManagerServiceRolePolicy
- AWS Audit Manager -Aktualisierungen für - AWS verwaltete Richtlinien

AWS Von verwaltete Richtlinie: AWSAuditManagerAdministratorAccess

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

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Verwaltungszugriff auf ermöglichen AWS Audit Manager. Dieser Zugriff umfasst die Möglichkeit, zu aktivieren und zu deaktivieren AWS Audit Manager, Einstellungen in zu ändern AWS Audit Managerund alle Audit Manager-Ressourcen wie Bewertungen, Frameworks, Kontrollen und Bewertungsberichte zu verwalten.

AWS Audit Manager erfordert umfassende Berechtigungen für mehrere - AWS Services. Dies liegt daran, dass in mehrere - AWS Services AWS Audit Manager integriert wird, um automatisch Beweise aus den - AWS-Konto und -Services 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 die Durchführung von Bewertungen über mehrere Konten und AWS Audit Manager die Konsolidierung von Beweisen in einem delegierten Administratorkonto ermöglichen können.
- `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 Ressourcen bereinigen und die serviceverknüpfte Rolle für Sie löschen AWS Audit Manager kann, wenn Sie den Service in der deaktivieren AWS Management Console.
- `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 es Prinzipalen, Prüfungen von aufzulisten und zu verwalten AWS Security Hub. Dies ist erforderlich, damit automatisch AWS Security Hub Ergebnisse für die AWS Services sammeln AWS Audit Manager kann, die von überwacht werden AWS Security Hub. 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 Managerdurchsuchen.

```
{
    "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": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "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": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Von verwaltete Richtlinie: AWSAuditManagerServiceRolePolicy

Sie können `AWSAuditManagerServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer serviceverknüpften Rolle, , verbunden`AWSServiceRoleForAuditManager`, die AWS Audit Manager es ermöglicht, Aktionen in Ihrem Namen durchzuführen. 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
  - Compliance-Prüfungen von AWS-Config-Regeln
  - Compliance-Prüfungen von AWS Security Hub
- Verwenden Sie API-Aufrufe, um Ihre Ressourcenkonfigurationen für die folgende AWS-Serviceszu 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.

- AWS Certificate Manager
- AWS Backup
- Amazon Bedrock
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch -Protokolle
- Amazon-Cognito-Benutzerpools
- AWS Config
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon Data Firehose
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS

- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming für Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Details zu Berechtigungen

`AWSAuditManagerServiceRolePolicy` ermöglicht AWS Audit Manager die Durchführung der folgenden Aktionen für die angegebenen Ressourcen:

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`
- `cloudwatch:DescribeAlarms`
- `cloudwatch:DescribeAlarmsForMetric`

- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections

- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- 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:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- 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`
- `organizations:DescribeOrganization`
- `organizations:DescribePolicy`
- `rds:DescribeCertificates`
- `rds:DescribeDbClusterEndpoints`
- `rds:DescribeDbClusterParameterGroups`
- `rds:DescribeDbClusters`
- `rds:DescribeDBInstances`
- `rds:DescribeDbSecurityGroups`
- `redshift:DescribeClusters`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketPolicy`
  - Diese API-Aktion wird innerhalb des Bereichs des ausgeführt AWS-Konto , in dem verfügbar service-linked-role ist. Sie kann nicht auf kontoübergreifende Bucket-Richtlinien zugreifen.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `securityhub:DescribeStandards`
- `sns:ListTopics`
- `sqs:ListQueues`
- `waf-regional:GetLoggingConfiguration`
- `waf-regional:ListRuleGroups`

- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
```

```
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
```

```
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "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",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
```

```
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
      "aws.securityhub"
     ]
    }
```

```
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit Manager -Aktualisierungen für - AWS verwaltete Richtlinien

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

Änderung	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die serviceverknüpfte Rolle erlaubt jetzt AWS Audit Manager , die `s3:GetBucketPolicy` Aktion auszuführen. Diese API-Aktion ist erforderlich, um das AWS - Best-Practices-Framework v1 für generative KI zu unterstützen. Es ermöglicht Audit Manager, automatisierte Nachweise über die Richtlini eneinschränkungen zu erfassen, die für Ihre Trainingsdatensätze mit generativen KI-Modell daten gelten.	12/06/2023

Änderung	Beschreibung	Datum
	Die `GetBucketPolicy` Aktion wird innerhalb des Bereichs des ausgeführt AWS-Konto , in dem verfügbar service-linked-role ist. Sie kann nicht auf kontoübergreifende Bucket-Richtlinien zugreifen.	

Änderung	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Wir haben die folgenden Berechtigungen zu 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

Änderung	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	

Änderung	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	

Änderung	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

Änderung	Beschreibung	Datum
AWSAuditManagerServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die serviceverknüpfte Rolle erlaubt jetzt AWS Audit Manager , die `organizations:DescribeOrganization` Aktion auszuführen. 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.	05/20/2022
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.	04/29/2022
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.	03/16/2022
AWS Audit Manager hat mit der Verfolgung von Änderungen begonnen	AWS Audit Manager hat mit der Verfolgung von Änderungen für seine AWS -verwalteten Richtlinien begonnen.	05/06/2021

Fehlerbehebung für 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 autorisiert, eine Aktion in auszuführen AWS Audit Manager

Der `AccessDeniedException` Fehler wird angezeigt, wenn ein Benutzer nicht über die Berechtigung zur Verwendung von AWS Audit Manager oder der Audit Manager-API-Operationen verfügt.

In diesem Fall muss Ihr Administrator die Richtlinie aktualisieren, um Ihnen den Zugriff zu ermöglichen.

Ich bin nicht autorisiert, iam durchzuführen: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 vorhandene Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder serviceverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in 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 meines AWS-Konto Zugriff auf meine - AWS Audit Manager Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Services, die ressourcenbasierte Richtlinien oder Zugriffssteuerungslisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob Audit Manager diese Funktionen unterstützt, finden Sie unter Funktionsweise AWS Audit Manager von mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen in Ihrem Besitz finden AWS-Konten Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , das Sie besitzen im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre -Ressourcen gewähren AWS-Konten, finden Sie unter Gewähren von Zugriff auf im AWS-Konten Besitz von Dritten im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

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. Serviceverknüpfte Rollen werden von Audit Manager vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer - AWS Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle AWS Audit Manager vereinfacht die Einrichtung von , 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.

Berechtigungen von serviceverknüpften Rollen für AWS Audit Manager

Audit Manager verwendet die serviceverknüpfte Rolle namens **`AWSServiceRoleForAuditManager`**, die den Zugriff auf AWS-Services und -Ressourcen ermöglicht, die von verwendet oder verwaltet werden AWS Audit Manager.

Die serviceverknüpfte Rolle `AWSServiceRoleForAuditManager` vertraut dem Service `auditmanager.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Rollenberechtigungsrichtlinie ermöglicht es Audit Manager`AWSAuditManagerServiceRolePolicy`, automatisierte Beweise über Ihre AWS Nutzung zu sammeln. Genauer gesagt, kann er die folgenden Aktionen in Ihrem Namen ergreifen.

- Audit Manager kann verwenden AWS Security Hub , um Beweise für Compliance-Prüfungen zu sammeln. In diesem Fall verwendet Audit Manager die folgende Berechtigung, um die Ergebnisse von Sicherheitsprüfungen direkt von zu melden AWS Security Hub. Anschließend fügt er die Ergebnisse als Beweise Ihren jeweiligen Bewertungskontrollen bei.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Weitere Informationen darüber, welche spezifischen Security Hub-Steuerelemente Audit Manager beschreiben kann, finden Sie unter AWS Security Hub -Kontrollen, die von AWS Audit Managerunterstützt werden.

- Audit Manager kann verwenden AWS Config , um Beweise für Compliance-Prüfungen zu 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 Von AWS Config unterstützte Regeln AWS Audit Manager.

- Audit Manager kann verwenden AWS CloudTrail , um Beweise für 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 Von AWS CloudTrail unterstützte Ereignisnamen AWS Audit Manager.

- Audit Manager kann AWS API-Aufrufe verwenden, um Beweise für die Ressourcenkonfiguration zu sammeln. In diesem Fall verwendet Audit Manager die folgenden Berechtigungen, um schreibgeschützte APIs aufzurufen, die Ihre Ressourcenkonfigurationen für den folgenden AWS-Servicesbeschreiben. Anschließend fügt er die API-Antworten als Beweis Ihren jeweiligen Bewertungskontrollen bei.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`

- bedrock:ListModelCustomizationJobs
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections

- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- 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:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- 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
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - Diese API-Aktion wird innerhalb des Bereichs des ausgeführt AWS-Konto , in dem verfügbar service-linked-role ist. Sie kann nicht auf kontoübergreifende Bucket-Richtlinien zugreifen.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs

- `waf:ListActivatedRulesInRuleGroup`

> **Note**
>
> Weitere Informationen zu den spezifischen API-Aufrufen, die Audit Manager beschreiben kann, finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen.

Die vollständigen Berechtigungsdetails der serviceverknüpften Rolle finden Sie unter AWSAuditManagerServiceRolePolicy im Referenzhandbuch zu -`AWSServiceRoleForAuditManager`verwalteten Richtlinien. AWS

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.

Erstellen der AWS Audit Manager serviceverknüpften Rolle

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie aktivieren AWS Audit Manager, erstellt der Service automatisch die serviceverknüpfte Rolle für Sie. Sie können Audit Manager auf der Onboarding-Seite der AWS Management Consoleoder über die API oder aktivieren AWS CLI. Weitere Informationen finden Sie unter Aktivieren von 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.

Bearbeiten der AWS Audit Manager serviceverknüpften Rolle

AWS Audit Manager erlaubt Ihnen nicht, die `AWSServiceRoleForAuditManager` serviceverknüpfte 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 AWS Audit Manager serviceverknüpften 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 in allen abgemeldet wird 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:

- Deaktivieren von AWS Audit Manager in dieser Anleitung
- DeregisterAccount in der AWS Audit Manager -API-Referenz
- deregister-account in der -AWS CLI Referenz für 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 Management Console 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 aus der verwenden AWS CLI , um eine serviceverknüpfte 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 aufGetRole, 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.

   Um eine Löschanfrage für eine serviceverknüpfte Rolle zu übermitteln, rufen Sie DeleteServiceLinkedRole auf. 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.

> **Tip**
>
> Das Löschen schlägt fehl, wenn der Audit Manager-Service die Rolle verwendet oder über zugeordnete Ressourcen verfügt. Dies passiert nur, wenn Sie in einem oder mehreren AWS-Regionennoch bei Audit Manager registriert sind. Nach der Abmeldung verwendet Audit Manager die serviceverknüpfte Rolle nicht mehr.
> Um ein Problem mit fehlgeschlagenem Löschen zu beheben, stellen Sie zunächst sicher, dass Sie Audit Manager in allen abgemeldet haben, AWS-Regionen in denen Sie den Service verwendet haben. Versuchen Sie dann erneut, die Schritte des zuvor angegebenen Verfahrens auszuführen.

Unterstützte Regionen für AWS Audit Manager serviceverknüpfte Rollen

AWS Audit Manager unterstützt die Verwendung von serviceverknüpften Rollen in allen , in AWS-Regionen denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS -Service-Endpunkte.

Compliance-Validierung für AWS Audit Manager

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

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

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

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

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

- AWS Compliance-Ressourcen – Diese Sammlung von Arbeitsmappen und Leitfäden könnte für Ihre Branche und Ihren Standort gelten.
- AWS Kunden-Compliance-Leitfäden – Verstehen Sie das Modell der geteilten Verantwortung anhand der Compliance. Die Leitfäden fassen die bewährten Methoden zur Sicherung zusammen AWS-Services und ordnen die Leitlinien den Sicherheitskontrollen in mehreren Frameworks zu (einschließlich National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Officer (PCI) und International Organization for Standardization (ISO)).
- Bewertung von Ressourcen mit Regeln im -AWS Config Entwicklerhandbuch – Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub – Dies AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager – Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um den Umgang mit Risiken und die Einhaltung von Branchenstandards zu vereinfachen.

Ausfallsicherheit in AWS Audit Manager

Die AWS globale -Infrastruktur ist um - AWS Regionen und Availability Zones herum aufgebaut. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit hoch redundanten Netzwerken mit niedriger Latenz und hohem Durchsatz verbunden sind.

Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

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

Infrastruktursicherheit in AWS Audit Manager

Als verwalteter Service ist AWS Audit Manager durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS Sicherheitsservices und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung mit den bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz in Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf 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.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Sie können diese API-Operationen von jedem Netzwerkstandort aus aufrufen, unterstützt jedoch AWS Audit Manager ressourcenbasierte Zugriffsrichtlinien, die Einschränkungen auf der Grundlage der Quell-IP-Adresse enthalten können. Sie können auch Audit Manager-Richtlinien verwenden, um den Zugriff über bestimmte Amazon Virtual Private Cloud (Amazon VPC)-Endpunkte oder bestimmte VPCs zu steuern. Dadurch wird der Netzwerkzugriff auf eine bestimmte Audit 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 herstellen, AWS Audit Manager indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Die Schnittstellen-Endpunkte werden mit AWS PrivateLink bereitgestellt, einer Technologie, die es Ihnen ermöglicht, ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder AWS Direct-Connect-Verbindung privat auf Audit Manager-APIs zuzugreifen. Die Instances in Ihrer VPC benötigen für die Kommunikation mit Audit Manager-APIs keine öffentlichen IP-Adressen. Der Datenverkehr zwischen Ihrer VPC und verlässt das AWS Netzwerk AWS Audit Manager 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 AWS Audit Manager, lesen Sie die Eigenschaften und Einschränkungen von Schnittstellenendpunkten im Amazon-VPC-Benutzerhandbuch.

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 über die Amazon-VPC-Konsole oder die 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 AWS Audit Manager unter Verwendung des folgenden Servicenamens:

- `com.amazonaws.region.auditmanager`

Wenn Sie ein privates DNS für den Endpunkt aktivieren, können Sie API-Anforderungen an AWS Audit Manager unter Verwendung seines standardmäßigen DNS-Namens für die Region senden, z. B. `auditmanager.us-east-1.amazonaws.com`.

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 Managersteuert. 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 - AWS Audit Manager Aktionen

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:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Protokollierung und Überwachung in AWS Audit Manager

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Audit Manager und Ihren anderen - AWS Lösungen aufrechtzuerhalten. AWS bietet die folgenden

Überwachungstools, um Audit Manager zu überwachen, Missstände zu melden und ggf. 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 AWSaufgerufen 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 Serverless-Event-Bus-Service, mit dem Sie Ihre Anwendungen einfach mit Daten aus einer Vielzahl von Quellen verbinden können. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, S-Service-(SaaS)oftware-as-a-Anwendungen und - AWS Services bereit und leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können Sie Ereignisse überwachen, die in Services auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im Amazon- EventBridge Benutzerhandbuch.

Überwachung AWS Audit Manager mit Amazon EventBridge

Amazon EventBridge hilft Ihnen, Ihr zu automatisieren AWS-Services und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren.

Sie können Regeln verwenden EventBridge, um Audit Manager-Ereignisse zu erkennen und darauf zu reagieren. Basierend auf den von Ihnen erstellten Regeln EventBridge ruft eine oder mehrere Zielaktionen auf, wenn ein Ereignis mit den Werten übereinstimmt, 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:

- Verwenden Sie eine - AWS Lambda Funktion, um eine Benachrichtigung an einen Slack-Kanal zu übergeben.
- 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 Amazon- CloudWatch Alarmaktion benachrichtigen.

> **Note**
>
> Audit Manager liefert Ereignisse auf dauerhafter Basis. Das bedeutet, dass Audit Manager erfolgreich versucht, Ereignisse EventBridge mindestens einmal an zu übermitteln. In Fällen, in denen Ereignisse aufgrund einer - EventBridge Serviceunterbrechung nicht zugestellt werden können, werden sie später von Audit Manager bis zu 24 Stunden lang 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 das Erstellen 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 Amazon- EventBridge 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 Ziele.

Erstellen einer - EventBridge Regel für Audit Manager

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.

So erstellen Sie eine - EventBridge Regel für Audit Manager

1. Öffnen Sie die Amazon- EventBridge Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules 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 für 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"]
   }
   ```

   Ersetzen Sie *Event* (Ereignis) 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 Amazon- EventBridge 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 EventBridge benötigt Berechtigungen zum Senden von Ereignissen an das Ziel. In diesen Fällen EventBridge kann die IAM-Rolle erstellen, die für die Ausführung Ihrer Regel erforderlich ist.

    a. Um automatisch eine IAM-Rolle zu erstellen, wählen Sie Create a new role for this specific resource (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.

Protokollieren von AWS Audit Manager API-Aufrufen mit CloudTrail

Audit Manager ist in integriert, einem Service CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in Audit Manager protokolliert. 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 Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für Audit Manager.

Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen.

Anhand der von CloudTrailgesammelten Informationen können Sie die an Audit Manager gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

Audit Manager-Informationen in CloudTrail

CloudTrail wird beim Erstellen des Kontos AWS-Konto auf Ihrem aktiviert. Wenn eine Aktivität in Audit Manager auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen AWS-Service Ereignissen im Ereignisverlauf aufgezeichnet.

Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -API-Ereignisverlauf.

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Audit Manager, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der - AWS Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3-Bucket bereit.

Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen CloudTrail von Protokolldateien aus mehreren Konten

Alle Audit Manager-Aktionen werden von protokolliert CloudTrail und sind in der AWS Audit Manager API-Referenz dokumentiert. Aufrufe der `UpdateAssessmentTemplate` API-Operationen `CreateCustomControl`, `DeleteControl` und erzeugen beispielsweise 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-Servicegesendet 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 Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

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"
    }
```

Konfigurations- und Schwachstellenanalyse in AWS Audit Manager

Konfigurations- und IT-Kontrollen sind eine übergreifende Verantwortung zwischen AWS und Ihnen, unserem Kunden. Weitere Informationen finden Sie im AWS Modell der geteilten Verantwortung.

Markieren von AWS Audit Manager-Ressourcen

Ein Tag ist ein Metadaten-Etikett, das von Ihnen oder von AWS einer AWS-Ressource 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 das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services das gleiche Tag zuweisen, um anzugeben, dass die Ressourcen zusammengehören.
- Überwachen von AWS-Kosten. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. Weitere Informationen finden Sie unter Use cost allocation tags (Verwendung von Kostenzuordnungs-Tags) im AWS Billing and Cost Management-Benutzerhandbuch.

In den folgenden Abschnitten erhalten Sie weitere Informationen zu Tags für AWS Audit Manager.

In Audit Manager unterstützte Ressourcen

Die folgenden Ressourcen in Audit Manager unterstützen das Tagging:

- Bewertungen
- Kontrollen
- Frameworks

Tag (Markierung)-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 nicht `aws:` als Präfix für Schlüssel. Dieses Präfix ist für AWS reserviert.

Verwalten von Tags

Sie können Tags als Eigenschaften festlegen, wenn Sie eine Bewertung, ein Framework oder ein Kontrollelement erstellen. Sie können Tags hinzufügen, bearbeiten und löschen, indem Sie die Audit Manager-Konsole, die AWS Command Line Interface (AWS CLI)-Konsole und die Audit Manager-API verwenden. Weitere Informationen finden Sie unter den folgenden Links:

- Für Bewertungen:
  - Erstellen einer Bewertung und Bearbeiten einer Bewertung im Abschnitt Assessments dieses Handbuchs
  - Registerkarte „Tags“ im Abschnitt Eine Bewertung überprüfen dieses Handbuchs
  - BewertungErstellen und BewertungAktualisieren in der AWS Audit Manager API-Referenz
  - TaggenRessource und EnttaggenRessource in der AWS Audit Manager API-Referenz
- Für Frameworks:
  - Erstellen eines benutzerdefinierten Frameworks und Bearbeiten eines benutzerdefinierten Frameworks im Abschnitt Framework-Bibliothek dieses Handbuchs
  - Registerkarte Tags im Abschnitt Framework-Details anzeigen dieses Handbuchs
  - ErstellenBewertungsFramework und AktualisierenBewertungsFramework in der AWS Audit Manager API-Referenz
  - TaggenRessource und EnttaggenRessource in der AWS Audit Manager API-Referenz
- Für Kontrollen:
  - Erstellen einer benutzerdefinierten Kontrolle und Bearbeiten einer benutzerdefinierten Kontrolle im Abschnitt Kontrollen-Bibliothek dieses Handbuchs
  - Registerkarte Tags im Abschnitt Kontrolldetails anzeigen dieses Handbuchs
  - ErstellenKontrolle und AktualisierenKontrolle in der AWS Audit Manager API-Referenz

- TaggenRessource und EnttaggenRessource in der AWS Audit Manager API-Referenz

AWS Audit Manager Ressourcen erstellen mit AWS CloudFormation

AWS Audit Manager ist in AWS CloudFormation integriert, ein Service, der Ihnen hilft, Ihre AWS-Ressourcen zu modellieren und einzurichten, damit Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen können. Sie erstellen eine Vorlage, in der alle gewünschten AWS-Ressourcen beschrieben werden (wie z. B. Bewertungen) und AWS CloudFormation übernimmt dann die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

Wenn Sie AWS CloudFormation verwenden, können Sie Ihre Vorlage wiederverwenden, um Ihre Audit Manager-Ressourcen einheitlich und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und können die gleichen Ressourcen dann in mehreren AWS-Konten und -Regionen immer wieder bereitstellen.

Audit Manager und AWS CloudFormation-Vorlagen

Um Ressourcen für und verwandte Dienstleistungen für Audit Manager bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen kennen und verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

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

Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen.

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

Dokumentverlauf für das AWS Audit Manager-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
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 weitere AWS-API-Aufrufe als Datenquelle für Ihre benutzerdefinierten Steuerelemente in Audit Manager verwenden. Weitere Informationen finden Sie unter Unterstützte API-Aufrufe für benutzerdefinierte Kontrolldatenquellen.	07. Dezember 2023
Von AWS verwaltete Richtlinie aktualisiert	AWS Audit Manager hat die AWSAuditManagerServiceRolePolicy aktualisiert. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien für AWS Audit Manager.	6. Dezember 2023
Support für AWS Security Hub konsolidierte Kontrollergebnisse	Audit Manager unterstützt jetzt konsolidierte Kontrollen in AWS Security Hub. Weitere Informationen finden Sie unter	16. November 2023

	AWS Security Hub von AWS Audit Manager unterstützte Kontrollen.	
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: AWS Bewährte Verfahren für generative KI	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter AWSFramework v1: Bewährte Verfahren für generative KI .	8. November 2023
Von AWS verwaltete Richtlinie aktualisiert	AWS Audit Manager hat die AWSAuditManagerSer viceRolePolicy aktualisiert. 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 AWS Audit Manager passieren und diese Ereignisse als Teil Ihrer ereignisgesteuerte n Architektur verwenden. Weitere Informationen finden Sie unter Überwachen von AWS Audit Managermit 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 AWS Audit Manager verfügbar. 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	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	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
Von AWS verwaltete Richtlinie aktualisiert	AWS Audit Manager hat die AWSAuditManagerServiceRolePolicy aktualisiert. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien für AWS Audit Manager.	7. Juli 2022
Von AWS verwaltete Richtlinie aktualisiert	AWS Audit Manager hat die AWSAuditManagerServiceRolePolicy aktualisiert. 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

Von AWS verwaltete Richtlinie aktualisiert	AWS Audit Managerhat die AWSAuditManagerAdministratorAccess-Richtlinie 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 Steuerelemente in Audit Manager verwenden. Weitere Informationen finden Sie unter Verwenden AWS Config von verwalteten Regeln 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 AWS Config von 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 AWS Audit Manager verfügbar. Weitere Informationen finden Sie in Anhang A zu ISO/IEC 27001:2013.	7. April 2022

Von AWS verwaltete Richtlinie aktualisiert	AWS Audit Manager hat die AWSAuditManagerServiceRolePolicy aktualisiert. 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 inAWS 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 Ihre benutzerdefinierten Frameworks mit einem anderen AWS-Konto teilen oder Ihre Frameworks in einen anderen AWS-Region unter Ihrem eigenen Konto replizieren. Weitere Informationen finden Sie unter Freigeben eines benutzerdefinierten Frameworks.	22. Oktober 2021
Neue Beispiele für AWS Audit Manager Kontrollen	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 AWS Audit Manager verfügbar. Weitere Informationen finden Sie im 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 Fehlerbehebung in 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 ManagerBewertungsberichte verbessert. Weitere Informationen zur Navigation und zum Verständnis der neuen Bewertungsberichte finden Sie unter Bewertungsberichte.	8. Juni 2021
Neue Seite über von AWS verwaltete Richtlinien	AWS Audit Manager hat mit der Verfolgung von Änderungen für seine verwalteten Richtlinien begonnen. 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 AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter AWSWell-Architected.	5. Mai 2021

Neues unterstütztes Framework: AWS Bewährte grundlegende Sicherheitsmethoden	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie unter AWSBewährte Methoden der grundlegenden Sicherheit.	5. Mai 2021
Neues unterstütztes Framework: GxP EU Annex 11	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar. Weitere Informationen finden Sie in GxP EU Annex 11.	28. April 2021
Neues unterstütztes Framework: NIST 800-53 (Rev. 5) Niedrig-Moderat-Hoch	Ein neues vorgefertigtes Framework ist jetzt in AWS Audit Manager verfügbar . Weitere Informationen finden Sie unter NIST 800-53 (Rev. 5) Niedrig-Moderat-Hoch.	25. März 2021

Neues unterstütztes Framework: CIS Benchmark for CIS AWS Audit ManagerFoundations 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

AWS-Glossar

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

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.