aws

ユーザーガイド

AWS Audit Manager

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Audit Manager: ユーザーガイド

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有しない他の商標はすべてそれぞれの所有者に帰属します。所有者は必ずしも Amazon との提携や関連があるわけではありません。また、Amazon の支援を受けているとはかぎりません。

Table of Contents

とは AWS Audit Manager

AWS Audit Manager ユーザーガイドへようこそ。

AWS Audit Manager は、 AWS 使用状況を継続的に監査して、リスクの管理方法と規制や業界標準への準拠を簡素化するのに役立ちます。Audit Manager は証拠収集を自動化するため、ポリシー、手順、およびアクティビティ (コントロールとも呼びます) が効果的に機能しているかどうかをより簡単に評価できます。監査の時期において、Audit Manager は、コントロールのステークホルダーのレビューを管理するのに役立ちます。これは、労力を大幅に抑えながら、監査対応のレポートを作成できることを意味します。

Audit Manager は、特定のコンプライアンス標準または規制の評価を構造化および自動化する、事前に構築されたフレームワークを提供します。フレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、指定されたコンプライアンス標準または規制の要件に従ってグループ化されています。フレームワークとコントロールをカスタマイズして、特定の要件に従って内部監査をサポートすることもできます。

フレームワークから評価を作成できます。評価を作成すると、Audit Manager はリソース評価を自動的に実行します。これらの評価では、 AWS アカウント 監査の範囲内で定義した のデータを収集します。収集されたデータは、監査に適した証拠となるように自動的に変換されます。その後、それらの証拠は関連するコントロールにアタッチされます。これは、セキュリティ、変更管理、ビジネス継続性、およびソフトウェアライセンスのコンプライアンスを実証するのに役立ちます。この証拠収集プロセスは継続的なものであり、評価を作成したときに開始されます。監査が完了し、Audit Manager を使用して証拠を収集する必要がなくなったら、証拠の収集を停止できます。これを行うには、評価のステータスを [inactive] (非アクティブ) に変更します。

Audit Manager の機能 Manager の機能

では AWS Audit Manager、次のタスクを実行できます。

- すぐに開始する - さまざまなコンプライアンス標準と規制をサポートする構築済みのフレームワークのギャラリーから選択して、最初の評価を作成します。次に、自動証拠収集を開始して AWS のサービス 使用状況を監査します。
- ハイブリッド環境またはマルチクラウド環境からの証拠のアップロードと管理 — Audit Manager がお客様の AWS 環境から収集する証拠に加えて、オンプレミスまたはマルチクラウド環境から証拠をアップロードして一元管理することもできます。

- 一般的なコンプライアンス標準および規制をサポートする - AWS Audit Manager 標準フレームワークのいずれかを選択します。これらのフレームワークは、一般的なコンプライアンス標準および規制のための構築済みコントロールマッピングを提供します。これには、CIS Foundation Benchmark、PCI DSS、GDPR、HIPAA、SOC2、GxP、および AWS 運用上のベストプラクティスが含まれます。
- アクティブな評価をモニタリングする - Audit Manager ダッシュボードを使用して、アクティブな評価の分析データを表示し、是正が必要な非準拠の証拠を迅速に特定します。
- 証拠の検索 — 証拠ファインダーこの機能を使用すると、検索クエリに関連する証拠をすばやく見つけることができます。検索結果から評価レポートを生成したり、検索結果を CSV 形式でエクスポートしたりできます。
- カスタムコントロールの作成 — 独自のコントロールを最初から作成するか、既存の標準コントロールまたはカスタムコントロールの編集可能なコピーを作成します。また、カスタム統制機能を使用してリスク評価用の質問を作成し、それらの質問への回答を手作業による証拠として保存することもできます。
- エンタープライズコントロールをデータソースの AWS 事前定義されたグループにマッピングする — 目標を表す一般的なコントロールを選択し、それらを使用してコンプライアンスニーズのポートフォリオの証拠を収集するカスタムコントロールを作成します。
- カスタムフレームワークの作成 — 内部監査の特定の要件に基づいて、標準またはカスタムコントロールを使用して独自のフレームワークを作成します。
- カスタムフレームワークの共有 — カスタム Audit Manager フレームワークを別の と共有するか AWS アカウント、自分のアカウント AWS リージョン で別の にレプリケートします。
- チーム間のコラボレーションをサポートする - 関連する証拠をレビューし、コメントを追加し、各コントロールのステータスを更新できる内容領域専門家にコントロールセットを委任します。
- 監査人用にレポートを作成する - 監査のために収集された関連する証拠を要約し、詳細な証拠を含むフォルダにリンクする評価レポートを生成します。
- 証拠の完全性を確保する - 変更されることのない、安全な場所に証拠を保管します。

> **Note**
>
> AWS Audit Manager は、特定のコンプライアンス標準および規制への準拠の検証に関連する証拠の収集を支援します。ただし、コンプライアンス自体を評価するものではありません。AWS Audit Manager したがって、 によって収集された証拠には、監査に必要な AWS 使用状況に関するすべての情報が含まれていない場合があります。 AWS Audit Manager は、法律顧問やコンプライアンスの専門家に代わるものではありません。

Audit Manager の価格

料金の詳細については、「AWS Audit Manager 料金」を参照してください。

Audit Manager を初めてお使いになる方向けの情報

Audit Manager を初めて使用する場合は、次のページから開始することをお勧めします。

1. AWS Audit Manager 概念と用語を理解する – 評価、フレームワーク、コントロールなど、Audit Manager で使用される主要な概念と用語について説明します。
2. が証拠を AWS Audit Manager 収集する方法を理解する – Audit Manager がリソース評価の証拠を収集する方法について説明します。
3. 推奨設定 AWS Audit Manager を使用した のセットアップ – Audit Manager のセットアップ要件について説明します。
4. の開始方法 AWS Audit Manager – チュートリアルに従って、最初の Audit Manager 評価を作成します。
5. AWS Audit Manager API リファレンス — Audit Manager API アクションとデータ型について理解します。

Audit Manager のその他のリソース

Audit Manager の詳細については、以下のリソースを参照してください。

- を使用して証拠を収集し、監査データを管理する AWS Audit Manager
- 3 行モデル全体での統合 (パート 2): 管理とガバナンスブログの AWS Config 「コンフォーマンスパックを AWS Audit Manager 評価に変換するAWS 」

AWS Audit Manager 概念と用語を理解する

使用を開始するのに役立つように、このページでは用語を定義し、 AWS Audit Managerの主要な概念のいくつかを説明します。

A

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

評価

Audit Manager の評価を使用して、監査に関連する証拠を自動的に収集できます。

評価は、監査に関連するコントロールのグループであるフレームワークに基づいています。標準またはカスタムのフレームワークから評価を作成できます。標準フレームワークには、特定のコンプライアンス標準または規制をサポートする構築済みのコントロールセットが含まれています。対照的に、カスタムフレームワークには、特定の監査要件に応じてカスタマイズおよびグループ化できるコントロールが含まれています。フレームワークを開始点として使用 AWS アカウント して、監査の範囲に含める を指定する評価を作成できます。

評価を作成すると、Audit Manager はフレームワークで定義されているコントロール AWS アカウント に基づいて、 内のリソースの評価を自動的に開始します。次に、関連する証拠を収集し、監査人が確認しやすい形式に変換します。これを行った後、評価のコントロールに証拠をアタッチします。監査の時間になると、ユーザー (または任意の受任者) は収集された証拠をレビューし、それらの証拠を評価レポートに追加できます。この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

証拠の収集は、評価を作成したときに開始される継続的なプロセスです。評価ステータスを [inactive] (非アクティブ) に変更することで、証拠の収集を停止できます。または、コントロールレベルで証拠の収集を停止することもできます。これを実行するには、評価内の特定のコントロールのステータスを [inactive] (非アクティブ) に変更します。

評価を作成および管理する方法については、「での評価の管理 AWS Audit Manager」を参照してください。

評価レポート

評価レポートは、 Audit Manager の評価から生成された確定ドキュメントです。これらのレポートは、監査のために収集された関連する証拠を要約したものです。それらのレポートは、関連する証拠のフォルダにリンクしています。フォルダは、評価で指定されたコントロールに従って名前が付けられ、編成されています。各評価について、Audit Manager が収集した証拠をレビューし、評価レポートに含める証拠を決定できます。

評価レポートの詳細については、「評価レポート」を参照してください。評価レポートを生成する方法については、「での評価レポートの準備 AWS Audit Manager」を参照してください。

評価レポートの宛先

評価レポートの送信先は、Audit Manager が評価レポートを保存するデフォルトの S3 バケットです。詳細については、「デフォルトの評価レポートの送信先の設定」を参照してください。

監査

監査とは、組織の資産、オペレーション、または事業上の誠実さを独立して調べることをいいます。情報技術 (IT) 監査は、組織の情報システム内のコントロールを集中的に調べるものです。IT 監査の目的は、情報システムがアセットを保護し、効果的に運用されており、データの完全性を維持しているかどうかを確認することにあります。これらはすべて、コンプライアンス標準または規制によって義務付けられている規制要件を満たすために重要です。

監査所有者

監査所有者という用語には、文脈に応じて 2 つの異なる意味があります。

Audit Manager において、監査所有者とは、評価とその関連リソースを管理する IAM ユーザーまたはロールです。この Audit Manager のペルソナの責任には、評価の作成、証拠のレビュー、および評価レポートの生成が含まれます。Audit Manager はコラボレーションが可能なサービスであり、監査所有者は、他のステークホルダーが評価に参加する際にそのメリットを享受できます。例えば、他の監査所有者を評価に追加して、管理タスクを共有できます。または、ユーザーが監査所有者であり、コントロールのために収集された証拠の解釈についてサポートが必要な場合は、その分野における内容領域専門家であるステークホルダーにそのコントロールセットを委任できます。このような担当者は、受任者ペルソナとして知られています。

ビジネス用語では、監査所有者は、会社の監査準備に向けた取り組みを調整および監督し、監査人に証拠を提示する担当者をいいます。通常、これは、コンプライアンスオフィサーや GDPR データ保護オフィサーなどのガバナンス、リスク、およびコンプライアンス (GRC) の専門家です。GRC の専門家は、監査に向けた準備を管理するための専門知識と権限を有しています。より具体的には、これらの専門家はコンプライアンス要件を理解しており、レポートデータを分析、解釈、および準備できます。ただし、GRC の専門家だけがこの役割を担うのではなく、ビジネスにおける他の役割も監査所有者の Audit Manager のペルソナを引き受けることができます。例えば、次のいずれかのチームの技術エキスパートに Audit Manager の評価を設定および管理させることもできます。

- SecOps
- IT/DevOps
- セキュリティオペレーションセンター/インシデント対応
- クラウドアセットを所有、開発、修復、およびデプロイし、組織のクラウドインフラストラクチャを理解している同様のチーム

Audit Manager の評価で監査所有者として誰を割り当てるかは、組織によって大きく異なります。また、セキュリティオペレーションをどのように構成するか、および監査の詳細によっても

異なります。Audit Manager では、同じ個人がある評価で監査所有者のペルソナを引き受け、別の評価で委任ペルソナを引き受けることができます。

Audit Manager の使用方法にかかわらず、監査所有者/委任ペルソナを使用し、各ユーザーに特定の IAM ポリシーを付与することで、組織全体の職務の分離を管理できます。この 2 段階のアプローチにより、Audit Manager は、個々の評価のあらゆる詳細を完全にコントロールできるようにします。詳細については、「 のユーザーペルソナに推奨されるポリシー AWS Audit Manager」を参照してください。

AWS マネージドソース

AWS マネージドソースは、 が AWS 管理する証拠ソースです。

各 AWS マネージドソースは、特定の共通コントロールまたはコアコントロールにマッピングされるデータソースの事前定義されたグループです。証拠ソースとして共通コントロールを使用すると、その共通コントロールをサポートするすべてのコアコントロールの証拠が自動的に収集されます。個々のコアコントロールを証拠ソースとして使用することもできます。

AWS マネージドソースが更新されるたびに、その AWS マネージドソースを使用するすべてのカスタムコントロールに同じ更新が自動的に適用されます。つまり、カスタムコントロールは、その証拠ソースの最新の定義に照らして証拠を収集します。これにより、クラウドコンプライアンス環境の変化に応じて継続的なコンプライアンスを確保できます。

「」、customer managed source「」も参照してくださいevidence source。

C

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

変更ログ

Audit Manager は、評価内のコントロールごとに、そのコントロールのユーザーアクティビティを追跡します。その後、特定のコントロールに関連するアクティビティの監査証跡を確認できます。変更ログにキャプチャされるユーザーアクティビティの詳細については、「」を参照してくださいChangelog タブ。

クラウドコンプライアンス

クラウドコンプライアンスは、クラウドをご利用のお客様が従わなければならない標準に、クラウドで提供されるシステムが準拠している必要があるという一般原則です。

共通コントロール

control を参照してください。

コンプライアンス規制

コンプライアンス規制は、通常は行動を規制するために、当局によって規定される法令、規則、または他の命令です。1 つの例は GDPR です。

コンプライアンス標準

コンプライアンス標準は、組織のプロセスを詳述する一連の構造化されたガイドラインであり、確立された規制、仕様、または法律に従って維持することを目的としています。PCI DSS、HIPAA はその一例です。

コントロール

統制とは、情報システムまたは組織に規定されている保護手段または対策です。コントロールは、情報の機密性、完全性、可用性を保護し、定義された一連の要件を満たすように設計されています。リソースが意図したとおりに動作していること、データが信頼できること、組織が適用可能な法律や規制に準拠していることを保証します。

Audit Manager では、統制はベンダーリスク評価アンケート内の質問を表すこともできます。この場合、統制とは、組織のセキュリティとコンプライアンス体制に関する情報を尋ねる具体的な質問です。

統制部門は、Audit Manager の評価で有効になっているときに、継続的に証拠を収集します。任意のコントロールに証拠を手動で追加することもできます。各証拠は、コントロールの要件への準拠を示すのに役立つレコードです。

Audit Manager には、次のタイプのコントロールが用意されています。

コントロールタイプ	説明
共通コントロール	共通のコントロールは、コントロールの目的を達成するのに役立つアクションと考えることができます。一般的なコントロールはコンプライアンス標準に固有のものではないため、重複するコンプライアンス義務の範囲をサポートできる証拠を収集するのに役立ちます。 例えば、データ分類と処理というコントロール目標があるとします。この目標を達成するために、アクセスコントロールと呼ばれる共通のコントロールを実装して、 リソースへの不正アクセスをモニタリングおよび検出できます。

コントロールタイプ	説明
	• 自動共通コントロールは証拠を収集します。これらは、1 つ以上の関連するコアコントロールのグループ化で構成されます。次に、これらの各コアコントロールは、事前定義された AWS データソースグループから関連する証拠を自動的に収集します。 AWS は、これらの基盤となるデータソースを管理し、規制や標準が変更され、新しいデータソースが特定されるたびにそれらを更新します。 • 手動の一般的なコントロールでは、独自の証拠をアップロードする必要があります。これは、通常、物理レコードのプロビジョニング、または AWS 環境外で発生するイベントの詳細が必要なためです。このため、手動の共通コントロールの要件をサポートする証拠を生成できる AWS データソースは存在しないことがよくあります。 共通コントロールを編集することはできません。ただし、カスタムコントロール を作成するときに、証拠ソースとして任意の共通コントロールを使用できます。
コアコントロール	これは、 AWS 環境の規範的なガイドラインです。コアコントロールは、共通のコントロールの要件を満たすのに役立つアクションと考えることができます。 例えば、アクセスコントロールと呼ばれる共通のコントロールを使用して、リソースへの不正アクセスをモニタリングするとします。この共通コントロールをサポートするには、S3 バケットのパブリック読み取りアクセスのブロックと呼ばれるコアコントロールを使用できます。 コアコントロールはコンプライアンス標準に固有ではないため、重複するコンプライアンス義務の範囲をサポートできる証拠を収集します。各コアコントロールは、1 つ以上のデータソースを使用して、特定の に関する証拠を収集します AWS のサービス。 は、これらの基盤となるデータソース AWS を管理し、規制や標準が変更され、新しいデータソースが特定されるたびにそれらを更新します。 コアコントロールを編集することはできません。ただし、カスタムコントロール を作成するときに、任意のコアコントロールを証拠ソースとして使用できます。

コントロールタイプ	説明
標準コントロール	これは、Audit Manager が提供する構築済みのコントロールです。 標準コントロールを使用して、特定のコンプライアンス標準に対する監査の準備を支援できます。各標準コントロールは Audit Manager framework の特定の標準に関連しており、そのフレームワークへの準拠を示すために使用できる証拠を収集します。標準コントロールは、 が AWS 管理する基盤となるデータソースから証拠を収集します。これらのデータソースは、規制や標準が変更され、新しいデータソースが特定されるたびに自動的に更新されます。 標準コントロールは編集できません。ただし、標準コントロールの編集可能なコピーを作成できます。
カスタムコントロール	これは、特定のコンプライアンス要件を満たすために Audit Manager で作成するコントロールです。 カスタムコントロールを最初から作成することも、既存の標準コントロールの編集可能なコピーを作成することもできます。カスタムコントロールを作成するときに、evidence sourceAudit Manager が証拠を収集する場所を決定する特定の を定義できます。カスタムコントロールを作成したら、そのコントロールを編集したり、カスタムフレームワークに追加したりできます。カスタムコントロールの編集可能なコピーを作成することもできます。

コントロールドメイン

コントロールドメインは、コンプライアンス標準に固有ではないコントロールのカテゴリと考えることができます。コントロールドメインの例は、データ保護 です。

コントロールは、多くの場合、単純な組織上の目的でドメインごとにグループ化されます。各ドメインには複数の目標があります。

コントロールドメインのグループ化は、Audit Manager のダッシュボードの最も強力な機能の 1 つです。Audit Manager は、非準拠の証拠がある評価のコントロールを強調表示し、コントロールドメインごとにグループ化します。これにより、監査に向けて準備する際に、特定の対象ドメインの是正に集中的に取り組むことができます。

コントロールの目標

コントロールの目標には、その下にある一般的なコントロールの目標が記述されます。各目標には、複数の共通コントロールを含めることができます。これらの一般的なコントロールが正常に実装されれば、目的を達成するのに役立ちます。

各コントロール目標はコントロールドメインに分類されます。例えば、データ保護コントロールドメインには、データ分類と処理という名前のコントロール目標がある場合があります。このコントロールの目的をサポートするために、アクセスコントロールと呼ばれる共通のコントロールを使用して、 リソースへの不正アクセスをモニタリングおよび検出できます。

コアコントロール

control を参照してください。

カスタムコントロール

control を参照してください。

カスタマーマネージドソース

カスタマーマネージドソースは、ユーザーが定義する証拠ソースです。

Audit Manager でカスタムコントロールを作成する場合、このオプションを使用して独自の個々のデータソースを作成できます。これにより、カスタム AWS Config ルールなどのビジネス固有のリソースから自動証拠を柔軟に収集できます。カスタムコントロールに手動証拠を追加する場合は、このオプションを使用することもできます。

カスタマーマネージドソースを使用する場合は、作成するすべてのデータソースを維持する責任があります。

「」、AWS managed source「」も参照してくださいevidence source。

D

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

データソース

Audit Manager はデータソースを使用してコントロールの証拠を収集します。データソースには次のプロパティがあります。

- データソースタイプは、Audit Manager が証拠を収集するデータソースのタイプを定義します。

  - 自動証拠の場合、タイプは AWS Security Hub、、、または API AWS Config AWS CloudTrailコールです。 AWS
  - 独自の証拠をアップロードする場合、タイプは手動 です。
  - Audit Manager API は、データソースタイプを sourceTypeと呼びます。
- データソースマッピングは、特定のデータソースタイプについて証拠が収集される場所を特定するキーワードです。
  - 例えば、これは CloudTrail イベントの名前や AWS Config ルールの名前などです。
  - Audit Manager API は、データソースマッピングを sourceKeywordと呼びます。
- データソース名は、データソースタイプとマッピングのペアにラベルを付けます。
  - 標準コントロールの場合、Audit Manager はデフォルト名を提供します。
  - カスタムコントロールの場合は、独自の名前を指定できます。
  - Audit Manager API は、データソース名を sourceName 名と呼びます。

1 つのコントロールに複数のデータソースタイプと複数のマッピングを含めることができます。例えば、1 つのコントロールが、データソースタイプ (AWS Config や Security Hub など) の混在から証拠を収集する場合があります。別のコントロールは、マッピング AWS Config として複数の AWS Config ルールを使用して、唯一のデータソースタイプとして を持つ場合があります。

次の表は、自動化されたデータソースタイプの一覧と、対応するマッピングの例を示しています。

[Data source type]	説明	マッピングの例
AWS Security Hub	このデータソースタイプを使用して、リソースのセキュリティ体制のスナップショットをキャプチャします。 Audit Manager は、Security Hub コントロールの名前をマッピングキーワードとして使用し、セキュリティチェックの結果を Security Hub から直接報告します。	`EC2.1`

[Data source type]	説明	マッピングの例
AWS Config	このデータソースタイプを使用して、リソースのセキュリティ体制のスナップショットをキャプチャします。 Audit Manager は、マッピングキーワードとして AWS Config ルールの名前を使用し、そのルールチェックの結果を から直接レポートします AWS Config。	`SNS_ENCRYPTED_KMS`
AWS CloudTrail	このデータソースタイプを使用して、Audit で必要な特定のユーザーアクティビティを追跡します。 Audit Manager は、CloudTrail イベントの名前をマッピングキーワードとして使用し、 CloudTrail ログから関連するユーザーアクティビティを収集します。	`CreateAccessKey`
AWS API コール	このデータソースタイプを使用して、特定の への API コールを通じてリソース設定のスナップショットを作成します AWS のサービス。 Audit Manager は API 呼び出しの名前をマッピングキーワードとして使用し、API レスポンスを収集します。	`kms_ListKeys`

受任者

代理人は、アクセス許可が制限された AWS Audit Manager ユーザーです。受任者は通常、専門的なレベルでビジネスまたは技術に関する知識を有しています。例えば、これらの専門知識は、データ保持ポリシー、トレーニングプラン、ネットワークインフラストラクチャ、または ID 管理に関するものである可能性があります。受任者は、監査所有者が自らの専門分野に属するコントロールに関して収集された証拠をレビューするのをサポートします。受任者は、コントロールセットとそれに関連する証拠のレビュー、コメントの追加、追加の証拠のアップロード、レビュー用に割り当てられた各コントロールのステータスの更新を行うことができます。

監査所有者は、評価全体ではなく、特定のコントロールセットを委任者に割り当てます。その結果、代表者による評価へのアクセスが制限されます。コントロールセットを委任する方法については、「での委任 AWS Audit Manager」を参照してください。

E

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

証拠

証拠とは、統制の要件への準拠を証明するために必要な情報を含む記録です。証拠の一例として、ユーザーによって呼び出された変更アクティビティとシステム設定スナップショットを挙げることができます。

Audit Manager の証拠には、主に自動と手動の証拠の 2 つのタイプがあります。

証拠タイプ	説明
自動証拠	これは、Audit Manager が自動的に収集する証拠です。これには、次の 3 つのカテゴリの自動証拠が含まれます。 1. コンプライアンスチェック — コンプライアンスチェックの結果は AWS Security Hub、、 AWS Config、またはその両方から取得されます。 コンプライアンスチェックの例には、PCI DSS コントロールの Security Hub からのセキュリティチェック結果や、HIPAA コントロールの AWS Config ルール評価などがあります。

証拠タイプ	説明
	詳細については、「AWS Config ルール でサポートされる AWS Audit Manager」および「AWS Security Hub でサポートされている コントロール AWS Audit Manager」を参照してください。 2. ユーザーアクティビティ — リソース設定を変更するユーザーアクティビティは、そのアクティビティが発生すると CloudTrail ログからキャプチャされます。 ユーザーアクティビティの例には、ルートテーブルの更新、Amazon RDS インスタンスのバックアップ設定の変更、S3 バケット暗号化ポリシーの変更が含まれます。 詳細については、「AWS CloudTrail でサポートされているイベント名 AWS Audit Manager」を参照してください。 3. 設定データ — リソース設定のスナップショットは、日次、週次、または月次ベースで AWS のサービス のサービスから直接キャプチャされます。 設定スナップショットの例には、VPC ルートテーブルのルートのリスト、Amazon RDS インスタンスのバックアップ設定、および S3 バケット暗号化ポリシーが含まれます。 詳細については、「AWS でサポートされている API コール AWS Audit Manager」を参照してください。
手動証拠	これは、Audit Manager に自分で追加した証拠です。独自の証拠を追加する方法は 3 つあります。 1. Amazon S3 からファイルをインポートする 2. ブラウザからファイルをアップロードする 3. リスクアセスメントの質問に対する回答をテキストで入力する 詳細については、「での手動証拠の追加 AWS Audit Manager」を参照してください。

評価を作成すると、自動証拠収集が開始されます。これは継続的なプロセスであり、Audit Manager は、証拠タイプと基盤となるデータソースに応じてさまざまな頻度で証拠を収集しま

す。詳細については、「が証拠を AWS Audit Manager 収集する方法を理解する」を参照してください。

評価で証拠をレビューする方法については、「での証拠の確認 AWS Audit Manager」を参照してください。

証拠ソース

証拠ソースは、コントロールが証拠を収集する場所を定義します。個々のデータソースでも、共通のコントロールまたはコアコントロールにマッピングされるデータソースの事前定義されたグループでもかまいません。

カスタムコントロールを作成すると、マネージドソース、カスタマーマネージドソース、またはその両方から AWS 証拠を収集できます。

> **Tip**
>
> AWS マネージドソースを使用することをお勧めします。 AWS マネージドソースが更新されるたびに、これらのソースを使用するすべてのカスタムコントロールに同じ更新が自動的に適用されます。つまり、カスタムコントロールは常に、その証拠ソースの最新の定義に照らして証拠を収集します。これにより、クラウドコンプライアンス環境の変化に応じて継続的なコンプライアンスを確保できます。

「」、AWS managed source「」も参照してくださいcustomer managed source。

証拠収集方法

コントロールがエビデンスを収集する方法は 2 つあります。

証拠収集方法	説明
自動	自動コントロールは、 AWS データソースから証拠を自動的に収集します。この自動エビデンスは、統制の完全または部分的な遵守を証明するのに役立ちます。
手動	手動コントロールでは、コントロールへの準拠を実証するために独自の証拠をアップロードする必要があります。

> **Note**
>
> 手動による証拠はどの自動統制にも添付できます。多くの場合、統制への完全な準拠を証明するには、自動化された証拠と手動の証拠を組み合わせる必要があります。Audit Manager は有用で関連性のある自動エビデンスを提供できますが、一部の自動エビデンスは部分的なコンプライアンスしか証明できない場合があります。この場合、Audit Manager が提供する自動エビデンスを独自のエビデンスで補足できます。
> 例:
>
> - には、 というコントロールAWS 生成 AI ベストプラクティスフレームワーク v2が含まれていますError analysis。このコントロールでは、モデルの使用状況に誤りが検出された場合にそれを特定する必要があります。また、根本原因を理解して是正措置を講じるために、徹底的なエラー分析を行う必要があります。
> - このコントロールをサポートするために、Audit Manager は、評価が実行されているでアラームが有効になっているかどうか CloudWatchを示す自動証拠を収集 AWS アカウント します。この証拠を利用して、アラームとチェックが正しく設定されていることを証明することで、統制に部分的に準拠していることを証明できます。
> - 完全なコンプライアンスを証明するには、自動エビデンスを手作業によるエビデンスで補足できます。例えば、エラー分析プロセス、エスカレーションや報告の基準値、根本原因分析の結果を示すポリシーや手順をアップロードできます。この手作業によるエビデンスを使用して、確立されたポリシーが実施されていること、および求められたときに是正措置が講じられたことを証明できます。
>
> より詳細な例については、「データソースが混在する場合の管理」を参照してください。

エクスポート先

エクスポート先は、エビデンスファインダーからエクスポートしたファイルを Audit Manager が保存するデフォルトの S3 バケットです。詳細については、「エビデンスファインダーのデフォルトのエクスポート先の設定」を参照してください。

F

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

フレームワーク

Audit Manager フレームワークは、特定の標準またはリスクガバナンス原則の評価を構造化および自動化します。これらのフレームワークには、構築済みコントロールまたはユーザー定義コントロールのコレクションが含まれており、 AWS リソースをこれらのコントロールの要件にマッピングするのに役立ちます。

Audit Manager には 2 種類のフレームワークがあります。

フレームワークタイプ	説明
標準フレームワーク	これは、さまざまなコンプライアンス標準および規制の AWS ベストプラクティスに基づく構築済みのフレームワークです。 標準フレームワークを使用して、PCI DSS や HIPAA などの特定のコンプライアンス標準または規制の監査準備を支援できます。
カスタムフレームワーク	これは、Audit Manager ユーザーとして定義するカスタマイズされたフレームワークです。 カスタムフレームワークを使用して、特定の GRC 要件に従って監査の準備を支援できます。

フレームワークを作成および管理する方法については、「フレームワークライブラリを使用してでフレームワークを管理する AWS Audit Manager」を参照してください。

> **Note**
>
> AWS Audit Manager は、特定のコンプライアンス標準および規制への準拠の検証に関連する証拠の収集を支援します。ただし、コンプライアンス自体を評価するものではありません。 AWS Audit Manager そのため、 を通じて収集された証拠には、監査に必要な AWS 使用状況に関するすべての情報が含まれていない場合があります。 AWS Audit Manager は、法律顧問やコンプライアンスの専門家に代わるものではありません。

フレームワークの共有

でのカスタムフレームワークの共有 AWS Audit Manager この機能を使用すると、カスタムフレームワークを AWS アカウント およびリージョン間ですばやく共有できます。カスタムフレームワークを共有するには、[共有リクエスト] を作成します。その後、受信者はリクエストを承諾または拒否するまでに 120 日かかります。承諾されると、Audit Manager は、フレームワークライブラリに共有されたカスタムフレームワークをレプリケートします。カスタムフレームワークをレプリケートすることに加えて、Audit Manager は、そのフレームワーク内に含まれているカスタムコントロールセットおよびコントロールもレプリケートします。これらのカスタムコントロールは、受信者のコントロールライブラリに追加されます。Audit Manager は、標準のフレームワークまたはコントロールをレプリケートしません。これは、これらのリソースが各アカウントとリージョンでデフォルトで既に利用可能であるためです。

R

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

リソース

リソースは、監査で評価される物理的な資産または情報アセットです。 AWS リソースの例としては、Amazon EC2 インスタンス、Amazon RDS インスタンス、Amazon S3 バケット、Amazon VPC サブネットなどがあります。

リソース評価

リソース評価は、個々のリソースを評価するプロセスです。この評価は、コントロールの要件に基づきます。評価がアクティブである間、は、評価の範囲内の個々のリソースごとにリソース評価を実行します。リソース評価では、次の一連のタスクが実行されます。

1. リソース設定、イベントログ、検出結果などの証拠を収集する
2. 証拠を変換してコントロールにマッピングする
3. 完全性を保つために証拠の系統を保存および追跡する

リソースコンプライアンス

資源コンプライアンスとは、コンプライアンスチェックの証拠を収集する際に評価された資源の評価状況を指します。

Audit Manager は、 AWS Config と Security Hub をデータソースタイプとして使用するコントロールのコンプライアンスチェックの証拠を収集します。このエビデンス収集では、複数のリ

ソースが評価される場合があります。その結果、1 つのコンプライアンスチェックエビデンスに 1 つ以上のリソースが含まれる可能性があります。

エビデンスファインダーのリソースコンプライアンスフィルターを使用して、リソースレベルでのコンプライアンスステータスを調べることができます。検索が完了すると、検索クエリに一致したリソースをプレビューできます。

エビデンスファインダーでは、リソースのコンプライアンス値として 3 つの値が指定できます。

値	説明
非準拠	これは、コンプライアンスチェックの問題があるリソースを指します。 これは、Security Hub がリソースの失敗結果を報告した場合、または が非準拠結果を AWS Config 報告した場合に発生します。
準拠	これは、コンプライアンスチェックの問題がないリソースを指します。 これは、Security Hub がリソースのパス結果を報告した場合、または が準拠結果を AWS Config 報告した場合に発生します。
未決定	これは、コンプライアンスチェックが利用できない、または適用できないリソースを指します。 これは、 AWS Config または Security Hub が基盤となるデータソースタイプであるが、それらのサービスが有効になっていない場合に発生します。 これは、基盤となるデータソースタイプがコンプライアンスチェック (手動証拠、 AWS API コール、 など) をサポートしていない場合にも発生します CloudTrail。

S

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

対象サービス

Audit Manager AWS のサービス は、評価の対象となる を管理します。古い評価がある場合は、過去にスコープ内のサービスを手動で指定していた可能性があります。2024 年 6 月 4 日以降は、対象範囲内のサービスを手動で指定または編集することはできません。

対象範囲内のサービスとは、評価によって証拠 AWS のサービス が収集される です。サービスが評価の範囲に含まれると、Audit Manager はそのサービスのリソースを評価します。リソースの例は下記のとおりです。

- Amazon EC2 インスタンス
- S3 バケット
- IAM ユーザーまたはロール
- DynamoDB テーブル。
- Amazon 仮想プライベートクラウド (VPC)、セキュリティグループ、ネットワークアクセスコントロールリスト (ACL) の表などのネットワークコンポーネント

例えば、Amazon S3 が範囲内のサービスである場合、Audit Manager は S3 バケットに関する証拠を収集できます。収集される正確な証拠は、コントロールの によって決まりますdata source。例えば、データソースタイプが で AWS Config、データソースマッピングが AWS Config ルール (など`s3-bucket-public-write-prohibited`) の場合、Audit Manager はそのルール評価の結果を証拠として収集します。

> **Note**
>
> 対象範囲内のサービスは、データソースタイプ とは異なることに注意してください。データソースタイプは、 AWS のサービス または別のものでもかまいません。詳細については、このガイドのサービスの対象範囲とデータソースタイプにはどのような違いがありますか?「トラブルシューティング」セクションの「」を参照してください。

標準コントロール

control を参照してください。

が証拠を AWS Audit Manager 収集する方法を理解する

の各アクティブな評価は、さまざまなデータソースから証拠 AWS Audit Manager を自動的に収集します。各評価では、証拠を収集する AWS アカウント Audit Manager を定義し、Audit Manager AWS のサービス はどの対象が対象であるかを管理します。これらのサービスおよびアカウントには、所有および使用する複数のリソースが含まれています。Audit Manager における証拠収集では、範囲内の各リソースが評価されます。これをリソース評価と呼びます。

次の手順は、Audit Manager が各リソース評価の証拠を収集する方法を説明するものです。

1. データソースからのリソース評価

証拠収集を開始するために、Audit Manager はデータソースから範囲内のリソースを評価します。これは、設定スナップショット、関連するコンプライアンスチェック結果、またはユーザーアクティビティをキャプチャすることによって行われます。その後、分析を実行して、このデータがサポートするコントロールを判別します。その後、リソース評価の結果が保存され、証拠に変換されます。さまざまな証拠タイプの詳細については、このガイドevidenceのAWS Audit Manager 概念と用語セクションの「」を参照してください。

2. 評価結果を証拠に変換する

リソース評価の結果には、そのリソースからキャプチャされた元のデータと、データがサポートするコントロールを示すメタデータの両方が含まれます。Audit Manager は、元のデータを監査人にわかりやすい形式に変換します。変換されたデータとメタデータは、コントロールにアタッチされる前に Audit Manager の証拠として保存されます。

3. 関連するコントロールに証拠をアタッチする

Audit Manager は証拠のメタデータを読み取ります。その後、保存された証拠を評価内の関連するコントロールにアタッチします。アタッチされた証拠は、Audit Manager に表示されます。これで、リソース評価のサイクルが完了します。

> **Note**
>
> コントロールの設定によっては、同じ証拠を、複数の Audit Manager の評価からの複数のコントロールにアタッチできる場合があります。同じ証拠が複数のコントロールにアタッチされている場合、Audit Manager はリソース評価を 1 回だけ実行します。これは、同じ証拠が収集されるのが 1 回のみであることによります。ただし、Audit Manager の評価における 1 つのコントロールには、複数のデータソースからの複数の証拠が含まれている場合があります。

証拠収集の頻度

証拠の収集は、評価を作成したときに開始される継続的なプロセスです。Audit Manager は、さまざまな頻度で複数のデータソースから証拠を収集します。その結果、証拠が収集される頻度に対する one-size-fits-all 回答はありません。証拠収集の頻度は、以下で説明するように、証拠タイプとそのデータソースに基づいています。

- コンプライアンスチェック — Audit Manager はこの証拠タイプを AWS Security Hub および から収集します AWS Config。
  - Security Hub の場合、証拠収集は Security Hub チェックのスケジュールに従います。Security Hub チェックのスケジュールの詳細については、AWS Security Hub ユーザーガイドの「セキュリティチェックの実行スケジュール」を参照してください。Audit Manager でサポートされている Security Hub チェックの詳細については、「AWS Security Hub でサポートされている コントロール AWS Audit Manager」を参照してください。
  - の場合 AWS Config、証拠収集は AWS Config ルールで定義されているトリガーに従います。AWS Config ルールのトリガーの詳細については、AWS Config ユーザーガイドの「トリガータイプ」を参照してください。Audit Manager でサポートされている の詳細については AWS Config ルール 、「」を参照してくださいAWS Config ルール でサポートされる AWS Audit Manager。
- ユーザーアクティビティ — Audit Manager は、この証拠タイプ AWS CloudTrail を継続的に から収集します。この頻度は継続的です。これは、ユーザーアクティビティが 1 日のうち、いつでも発生する可能性があるためです。詳細については、「AWS CloudTrail でサポートされているイベント名 AWS Audit Manager」を参照してください。
- 設定データ — Audit Manager は、Amazon EC2、Amazon S3、IAM AWS のサービス などの別の への describe API コールを使用してこの証拠タイプを収集します。 Amazon S3 どの API アクションを呼び出すかを選択できます。また、Audit Manager で頻度を日次、週次、または月次として設定します。コントロールライブラリでコントロールを作成または編集するときに、この頻度を指定できます。コントロールを編集または作成する手順については、「コントロールライブラリを使用して でコントロールを管理する AWS Audit Manager」を参照してください。Audit Manager でサポートされている API コールの詳細については、「」を参照してくださいAWS でサポートされている API コール AWS Audit Manager。

データソースの証拠収集の頻度にかかわらず、コントロールと評価がアクティブである限り、新しい証拠は自動的に収集されます。

AWS Audit Manager コントロールの例

このページの例を確認して、 AWS Audit Managerでコントロールがどのように機能するかを確認できます。

Audit Manager では、コントロールは 4 つのデータソースタイプから証拠を自動的に収集できます。

1. AWS CloudTrail – CloudTrail ログからユーザーアクティビティをキャプチャし、ユーザーアクティビティの証拠としてインポートします。
2. AWS Security Hub – Security Hub から検出結果を収集し、コンプライアンスチェックの証拠としてインポートします。
3. AWS Config – からルール評価を収集 AWS Config し、コンプライアンスチェックの証拠としてインポートする
4. AWS API コール – API コールからリソーススナップショットをキャプチャし、設定データの証拠としてインポートします。

多くのコントロールは、これらのデータソースの事前定義されたグループを使用して証拠を収集します。これらのデータソースグループは、AWS マネージドソース と呼ばれます。各 AWS マネージドソースは、共通のコントロールまたはコアコントロールを表します。これにより、コンプライアンス要件を、 の業界認定評価者によって検証および維持されているデータソースの関連グループにマッピングする効率的な方法が得られます AWS。または、上記の 4 つのデータソースタイプを使用して、独自のデータソースを定義することもできます。これにより、手動証拠をアップロードしたり、カスタム AWS Config ルールなどのビジネス固有のリソースから自動証拠を収集したりできます。

このページの例は、コントロールが個々のデータソースタイプから証拠を収集する方法を示しています。コントロールがどのように見えるか、Audit Manager がデータソースから証拠を収集する方法、およびコンプライアンスを実証するために実行できる次のステップについて説明します。

> **Tip**
>
> Audit Manager で最適なエクスペリエンスを得るには、 AWS Config と Security Hub を有効にすることをお勧めします。これらのサービスを有効にすると、Audit Manager は Security Hub の検出結果と を使用して自動証拠 AWS Config ルール を生成できます。
>
> - AWS Security Hubを有効にしたら、必ずすべてのセキュリティ標準を有効にし、統合検出結果の設定を有効にしてください。このステップにより、サポートされているすべてのコンプライアンス標準に関する検出結果を Audit Manager がインポートできるようになります。
> - を有効にしたら AWS Config、関連する も有効に AWS Config ルールするか、監査に関連するコンプライアンス標準のコンフォーマンスパックをデプロイしてください。このステップにより、Audit Manager は、有効に AWS Config ルール したサポートされているすべての結果をインポートできます。

次のタイプのコントロールの各例を利用できます。

トピック

- をデータソースタイプ AWS Security Hub として使用する自動コントロール
- をデータソースタイプ AWS Config として使用する自動コントロール
- AWS API コールをデータソースタイプとして使用する自動コントロール
- をデータソースタイプ AWS CloudTrail として使用する自動コントロール
- 手動コントロール
- データソースタイプが混在するコントロール(自動および手動)

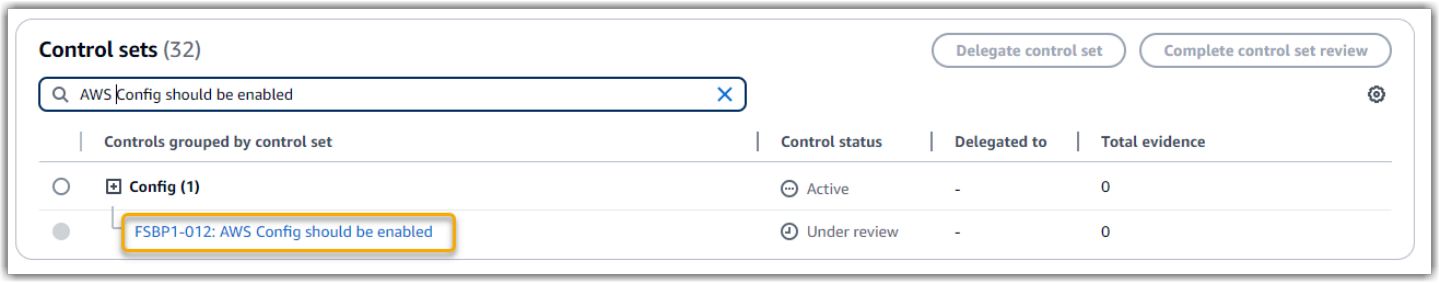
をデータソースタイプ AWS Security Hub として使用する自動コントロール

この例は、 をデータソースタイプ AWS Security Hub として使用するコントロールを示しています。これは、AWS Foundational Security Best Practices (FSBP) フレームワークから取得した標準のコントロールです。Audit Manager は、このコントロールを使用して、 AWS 環境を FSBP 要件に合わせるのに役立つ証拠を生成します。

コントロールの詳細の例

- コントロール名 – `FSBP1-012: AWS Config should be enabled`
- コントロールセット – `Config`。これは、設定管理に関連する FSBP コントロールのフレームワーク固有のグループです。
- 証拠ソース – 個々のデータソース
- データソースタイプ – AWS Security Hub
- 証拠タイプ – コンプライアンスチェック

次の例では、このコントロールは FSBP フレームワークから作成された Audit Manager の評価内に存在しています。



評価には統制状況が表示されます。また、このコントロールについてこれまでに収集された証拠の量も表示されます。ここから、レビューのためにコントロールセットを委任するか、自らレビューを完了できます。コントロール名を選択すると、そのコントロールの証拠を含め、詳細情報が記載された詳細のページが開きます。

このコントロールの機能

このコントロールでは AWS Config 、Security Hub を使用するすべての AWS リージョン で が有効になっている必要があります。Audit Manager は、IAM ポリシーが FSBP 要件を満たす上で過度に広範ではないかどうかを確認するために、このコントロールを使用できます。より具体的には、カスタマーマネージド IAM ポリシーに、次のワイルドカードステートメントを含む管理者アクセス権が付与されているかどうかを確認できます: `"Resource": "*"` に対する `"Effect": "Allow"` と `"Action": "*"`。

Audit Manager がこのコントロールの証拠を収集する方法

Audit Manager は、このコントロールの証拠を収集するために次の手順を実行します。

1. 各コントロールについて、Audit Manager は範囲内のリソースを評価します。これは、コントロールの設定で指定されたデータソースを使用して実行されます。この例では、IAM ポリシーが リソースで、Security Hub と AWS Config がデータソースタイプです。Audit Manager は、特定の Security Hub チェック ([IAM.1]) の結果を探します。このチェックでは、 AWS Config ルールを使用して IAM ポリシー (iam-policy-no-statements-with-admin-access) を評価します。
2. リソース評価の結果は保存され、監査人が確認しやすい証拠に変換されます。Audit Manager は、Security Hub をデータソースとして使用するコントロールについて、コンプライアンスチェックの証拠を生成します。この証拠には、Security Hub から直接レポートされたコンプライアンスチェックの結果が含まれています。
3. Audit Manager は、保存された証拠を、`FSBP1-012: AWS Config should be enabled` という名前の評価のコントロールにアタッチします。

Audit Manager を使用してこのコントロールへの準拠を実証する方法

証拠がコントロールにアタッチされた後、ユーザー (または任意の受任者) は証拠をレビューして、是正が必要かどうかを確認できます。

この例では、Audit Manager は Security Hub が [Fail] (失敗) と判断した旨を表示する場合があります。これは、IAM ポリシーにワイルドカード (*) が含まれており、過度に広範であることを理由としてコントロールの要件を満たせない場合に発生する可能性があります。この場合、IAM ポリシーを更新して、完全な管理者権限を許可しないようにすることができます。これを実現するために、ユーザーが実行する必要のあるタスクを決定し、ユーザーがそれらのタスクのみを実行できるようにするポリシーを作成できます。この是正措置は、 AWS 環境を FSBP 要件に合わせるのに役立ちます。

IAM ポリシーがコントロールと整合的である場合は、コントロールを [Reviewed] (レビュー済み) としてマークし、評価レポートに証拠を追加します。その後、このレポートを監査人と共有して、コントロールが意図したとおりに機能していることを実証できます。

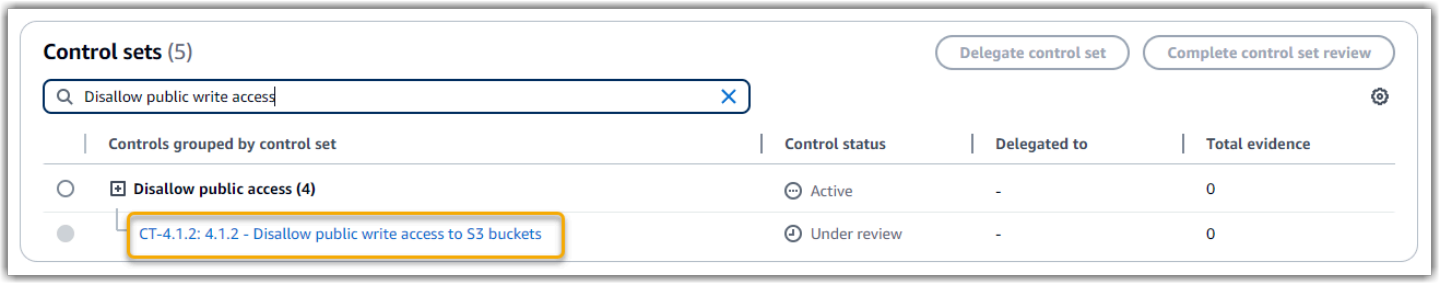
をデータソースタイプ AWS Config として使用する自動コントロール

この例では、 をデータソースタイプ AWS Config として使用するコントロールを示します。これは、AWS Control Tower ガードレール フレームワークから取得した標準のコントロールです。Audit Manager は、このコントロールを使用して、環境を AWS AWS Control Tower Guardrails に合わせるのに役立つ証拠を生成します。

コントロールの詳細の例

- コントロール名 – `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`
- コントロールセット – このコントロールは `Disallow public access` コントロールセットに属します。これは、アクセス管理に関連するコントロールのグループです。
- 証拠ソース — 個々のデータソース
- データソースタイプ – AWS Config
- 証拠タイプ – コンプライアンスチェック

次の例では、このコントロールは AWS Control Tower Guardrails フレームワークから作成された Audit Manager 評価内にあります。



評価には統制状況が表示されます。また、このコントロールについてこれまでに収集された証拠の量も表示されます。ここから、レビューのためにコントロールセットを委任するか、自らレビューを完了できます。コントロール名を選択すると、そのコントロールの証拠を含め、詳細情報が記載された詳細のページが開きます。

このコントロールの機能

Audit Manager は、このコントロールを使用して、S3 バケットポリシーのアクセスレベルが AWS Control Tower 要件を満たせないほど寛容であるかどうかを確認できます。より具体的には、パブリックアクセスのブロックの設定、バケットポリシー、バケットアクセスコントロールリスト (ACL) をチェックして、バケットがパブリック書き込みアクセスを許可していないことを確認できます。

Audit Manager がこのコントロールの証拠を収集する方法

Audit Manager は、このコントロールの証拠を収集するために次の手順を実行します。

1. 各コントロールについて、Audit Manager は、コントロールの設定で指定されたデータソースを使用して範囲内のリソースを評価します。この場合、S3 バケットがリソースであり、 AWS Config がデータソースタイプです。Audit Manager は、特定の AWS Config ルール (s3-bucket-public-write-prohibited) の結果を検索して、評価の範囲内にある各 S3 バケットの設定、ポリシー、および ACL を評価します。
2. リソース評価の結果は保存され、監査人が確認しやすい証拠に変換されます。Audit Manager は、をデータソースタイプ AWS Config として使用するコントロールのコンプライアンスチェックの証拠を生成します。この証拠には、 から直接報告されたコンプライアンスチェックの結果が含まれています AWS Config。
3. Audit Manager は、保存された証拠を、`CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets` という名前の評価のコントロールにアタッチします。

Audit Manager を使用してこのコントロールへの準拠を実証する方法

証拠がコントロールにアタッチされた後、ユーザー (または任意の受任者) は証拠をレビューして、是正が必要かどうかを確認できます。

この例では、Audit Manager は S3 バケットが非準拠である AWS Config ことを示す のルールを表示する場合があります。これは、S3 バケットのいずれかにパブリックポリシーを制限しないパブリックアクセスのブロックの設定があり、使用中のポリシーがパブリック書き込みアクセスを許可している場合に発生する可能性があります。これを修正するには、パブリックアクセスのブロックの設定を更新して、パブリックポリシーを制限します。または、パブリック書き込みアクセスを許可しない別のバケットポリシーを使用できます。この是正措置は、環境を AWS AWS Control Tower 要件に合わせるのに役立ちます。

S3 バケットのアクセスレベルがコントロールと整合的であることを確認したら、コントロールを [Reviewed] (レビュー済み) としてマークし、評価レポートに証拠を追加できます。その後、このレポートを監査人と共有して、コントロールが意図したとおりに機能していることを実証できます。

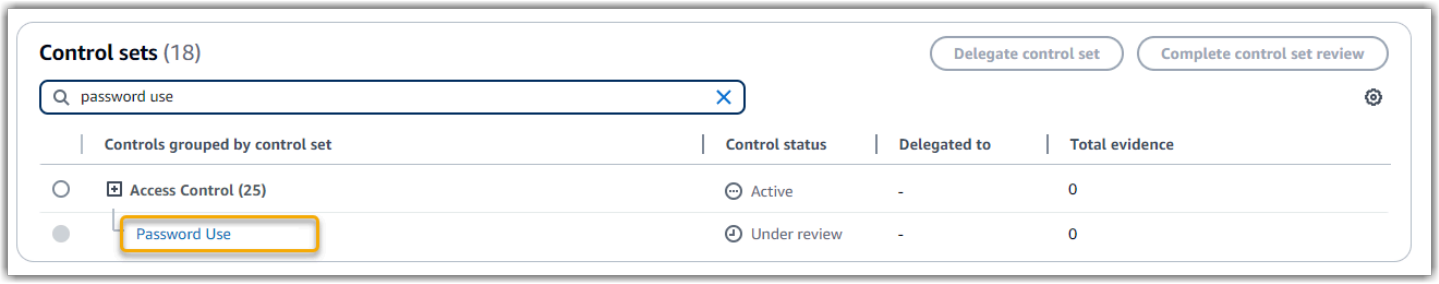
AWS API コールをデータソースタイプとして使用する自動コントロール

この例は、 AWS API コールをデータソースタイプとして使用するカスタムコントロールを示しています。Audit Manager は、このコントロールを使用して、 AWS 環境を特定の要件に合わせるのに役立つ証拠を生成します。

コントロールの詳細の例

- コントロール名 – `Password Use`
- コントロールセット – このコントロールは `Access Control` と呼ばれるコントロールセットに属します。これは、Identity and Access Management に関連するコントロールのグループです。
- 証拠ソース – 個々のデータソース
- データソースタイプ – AWS API コール
- 証拠タイプ – 設定データ

次の例では、このコントロールはカスタム フレームワークから作成された Audit Manager 評価内にあります。



評価には統制状況が表示されます。また、このコントロールについてこれまでに収集された証拠の量も表示されます。ここから、レビューのためにコントロールセットを委任するか、自らレビューを完了できます。コントロール名を選択すると、そのコントロールの証拠を含め、詳細情報が記載された詳細のページが開きます。

このコントロールの機能

Audit Manager では、このカスタム コントロールを使用して、十分なアクセス コントロール ポリシーを確実に導入するのに役立ちます。このコントロールは、パスワードの選択と使用において適切なセキュリティ慣行に従うことをユーザーに要求します。Audit Manager は、評価の範囲内にある IAM プリンシパルのすべてのパスワードポリシーのリストを取得することにより、これを検証するのに役立ちます。

Audit Manager がこのコントロールの証拠を収集する方法

Audit Manager は、このカスタムコントロールの証拠を収集するために次の手順を実行します。

1. 各コントロールについて、Audit Manager は、コントロールの設定で指定されたデータソースを使用して範囲内のリソースを評価します。この場合、IAM プリンシパルがリソースであり、 AWS API コールがデータソースタイプです。Audit Manager は、特定の IAM API コール () の結果を検索しますGetAccountPasswordPolicy。その後、評価の範囲内にある AWS アカウント のパスワードポリシーを返します。
2. リソース評価の結果は保存され、監査人が確認しやすい証拠に変換されます。Audit Manager は、API コールをデータソースとして使用するコントロールの設定データの証拠を生成します。この証拠には、API レスポンスからキャプチャされた元のデータと、データがサポートするコントロールを示す追加のメタデータが含まれています。
3. Audit Manager は、保存された証拠を、`Password Use` という名前の評価のカスタムコントロールにアタッチします。

Audit Manager を使用してこのコントロールへの準拠を実証する方法

証拠がコントロールにアタッチされた後、ユーザー (または任意の受任者) は証拠をレビューして、それが十分であるかどうか、または是正が必要かどうかを確認できます。

この例では、証拠をレビューして、API コールからのレスポンスを確認できます。GetAccountPasswordPolicy レスポンスでは、アカウントのユーザーパスワードの複雑さの要件と必須のローテーション期間について説明します。この API レスポンスを証拠として使用して、評価の範囲内にある に対して十分なパスワードアクセスコントロールポリシーが設定され AWS アカウント ていることを示すことができます。必要に応じて、コントロールにコメントを追加することで、これらのポリシーに関する追加のコメントを提供することもできます。

IAM プリンシパルのパスワードポリシーがコントロールと整合的であることを確認したら、コントロールをレビュー済みとしてマークし、評価レポートに証拠を追加できます。その後、このレポートを監査人と共有して、コントロールが意図したとおりに機能していることを実証できます。

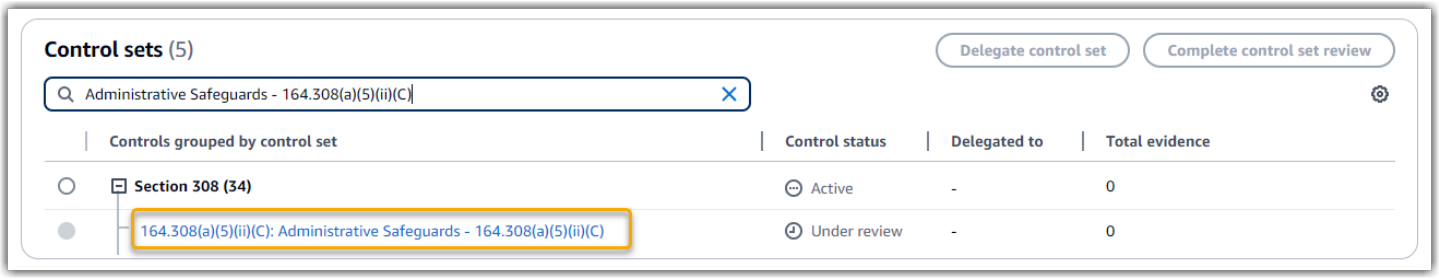
をデータソースタイプ AWS CloudTrail として使用する自動コントロール

この例は、 をデータソースタイプ AWS CloudTrail として使用するコントロールを示しています。これは、HIPAA セキュリティルール 2003 フレームワーク から取得した標準コントロールです。Audit Manager は、このコントロールを使用して、 AWS 環境を HIPAA 要件に合わせるのに役立つ証拠を生成します。

コントロールの詳細の例

- コントロール名 – `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`
- コントロールセット – このコントロールは `Section 308` と呼ばれるコントロールセットに属します。これは、管理上の保護に関連する HIPAA コントロールのフレームワーク固有のグループです。
- 証拠ソース – AWS マネージドソース (コアコントロール)
- 基盤となるデータソースタイプ – AWS CloudTrail
- 証拠タイプ – ユーザーアクティビティ

HIPAA フレームワークから作成された Audit Manager の評価内に表示されるこのコントロールは次のとおりです。



評価には統制状況が表示されます。また、このコントロールについてこれまでに収集された証拠の量も表示されます。ここから、レビューのためにコントロールセットを委任するか、自らレビューを完了できます。コントロール名を選択すると、そのコントロールの証拠を含め、詳細情報が記載された詳細のページが開きます。

このコントロールの機能

このコントロールでは、不正アクセスを検出するためのモニタリング手順を設定する必要があります。不正アクセスの例は、多要素認証 (MFA) を有効にせずに誰かがコンソールにサインインする場合です。Audit Manager は、MFA が有効になっていない管理コンソールのサインインリクエストをモニタリング CloudWatch するように Amazon を設定した証拠を提供することで、このコントロールを検証するのに役立ちます。

Audit Manager がこのコントロールの証拠を収集する方法

Audit Manager は、このコントロールの証拠を収集するために次の手順を実行します。

1. Audit Manager は、コントロールごとに、コントロール設定で指定された証拠ソースを使用して対象範囲内のリソースを評価します。この場合、コントロールは証拠ソースとしていくつかのコアコントロールを使用します。

   各コアコントロールは、個々のデータソースのマネージドグループです。この例では、これらのコアコントロール (`Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled`) の 1 つがデータソース CloudTrail として を使用します。 CloudTrail はデータソースタイプで、Amazon CloudWatch アラームは評価されるリソースです。

   Audit Manager は、 `monitoring_EnableAlarmActions`キーワードを使用して CloudTrail ログを確認し、 によってログに記録される CloudWatch アラームを有効にするアクションを見つけます CloudTrail。その後、評価の範囲内にある関連イベントのログを返します。
2. リソース評価の結果は保存され、監査人が確認しやすい証拠に変換されます。Audit Manager は、をデータソースタイプ CloudTrail として使用するコントロールのユーザーアクティビティの証拠

を生成します。この証拠には、Amazon からキャプチャされた元のデータと CloudWatch、データがサポートするコントロールを示す追加のメタデータが含まれています。

3. Audit Manager は、保存された証拠を、`164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)` という名前の評価のコントロールにアタッチします。

Audit Manager を使用してこのコントロールへの準拠を実証する方法

証拠がコントロールにアタッチされた後、ユーザー (または任意の受任者) は証拠をレビューして、是正が必要かどうかを確認できます。

この例では、証拠を確認して、 によって記録されたアラーム有効化イベントを確認できます CloudTrail。このログを証拠として使用して、MFA を有効にせずにコンソールのサインインがいつ発生したかを検出するのに十分なモニタリング手順があることを示すことができます。必要に応じて、コントロールにコメントを追加することで、追加のコメントを提供することもできます。例えば、ログに MFA なしで複数のサインインが表示されている場合は、問題の修正方法を説明するコメントを追加できます。コンソールサインインを定期的にモニタリングすることは、不一致や不適切なサインインの試行によって発生する可能性のあるセキュリティの問題を防ぐのに役立ちます。また、このベストプラクティスは、 AWS 環境を HIPAA 要件に合わせるのに役立ちます。

モニタリング手順がコントロールと整合的であることを確認したら、コントロールを [Reviewed] (レビュー済み) としてマークし、評価レポートに証拠を追加できます。その後、このレポートを監査人と共有して、コントロールが意図したとおりに機能していることを実証できます。

手動コントロール

自動証拠収集をサポートしていないコントロールもあります。これには、クラウドで生成されない監視、インタビュー、および他のイベントに加えて、物理的な記録と署名のプロビジョニングに依拠するコントロールが含まれます。このような場合には、証拠を手動でアップロードして、コントロールの要件を満たしていることを実証できます。

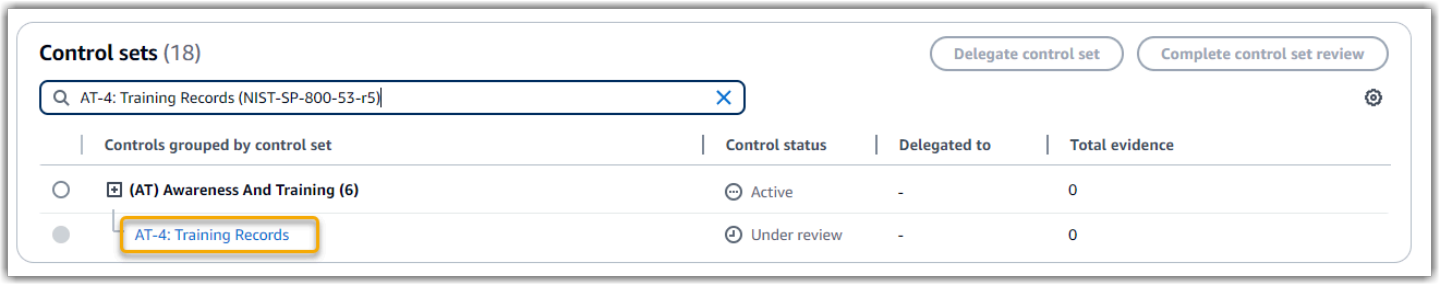
この例は、Audit Manager が自動証拠を収集しない手動コントロールを示しています。これは、NIST 800-53 (Rev. 5) フレームワークから取得した標準のコントロールです。Audit Manager を使用して、このコントロールのコンプライアンスを実証する証拠をアップロードおよび保存できます。

コントロールの詳細の例

- コントロール名 – `AT-4: Training Records`

- コントロールセット – (AT) Awareness and training。これは、トレーニングに関連する NIST コントロールのフレームワーク固有のグループです。
- 証拠ソース – データソース
- 基盤となるデータソースタイプ – 手動
- 証拠タイプ – 手動

NIST 800-53 (Rev. 5) Low-Moderate-High フレームワークから作成された Audit Manager の評価内に表示されるこのコントロールは次のとおりです。



評価には統制状況が表示されます。また、このコントロールについてこれまでに収集された証拠の量も表示されます。ここから、レビューのためにコントロールセットを委任するか、自らレビューを完了できます。コントロール名を選択すると、そのコントロールの証拠を含め、詳細情報が記載された詳細のページが開きます。

このコントロールの機能

このコントロールを使用すると、担当者が適切なレベルのセキュリティおよびプライバシートレーニングを確実に受けることができます。具体的には、役割に基づいて、すべてのスタッフに対してセキュリティとプライバシーのトレーニングアクティビティが文書化されていることを示すことができます。また、トレーニングレコードが個人ごとに保持されていることを示すこともできます。

このコントロールの証拠を手動でアップロードする方法

自動証拠を補足する手動証拠をアップロードするには、「」の「手動証拠のアップロード AWS Audit Manager」を参照してください。Audit Manager は、アップロードされた証拠を、AT-4: Training Records という名前の評価のコントロールにアタッチします。

Audit Manager を使用してこのコントロールへの準拠を実証する方法

このコントロールをサポートするドキュメントがある場合は、手動証拠としてアップロードできます。例えば、人事部門が従業員に発行する、委任されたロールベースのトレーニング資料の最新のコピーをアップロードできます。

自動化されたコントロールの場合と同様に、証拠のレビュー (またはこの場合は提供) をサポートできるステークホルダーに手動コントロールを委任できます。例えば、このコントロールを確認すると、要件を部分的にしか満たしていないことに気付く場合があります。これは、対面トレーニングの出席状況追跡のコピーがない場合に発生する可能性があります。人事関係者にコントロールを委任し、人事関係者がトレーニングに参加したスタッフのリストをアップロードできます。

コントロールと整合的であることを確認したら、[Reviewed] (レビュー済み) としてマークし、評価レポートに証拠を追加できます。その後、このレポートを監査人と共有して、コントロールが意図したとおりに機能していることを実証できます。

データソースタイプが混在するコントロール(自動および手動)

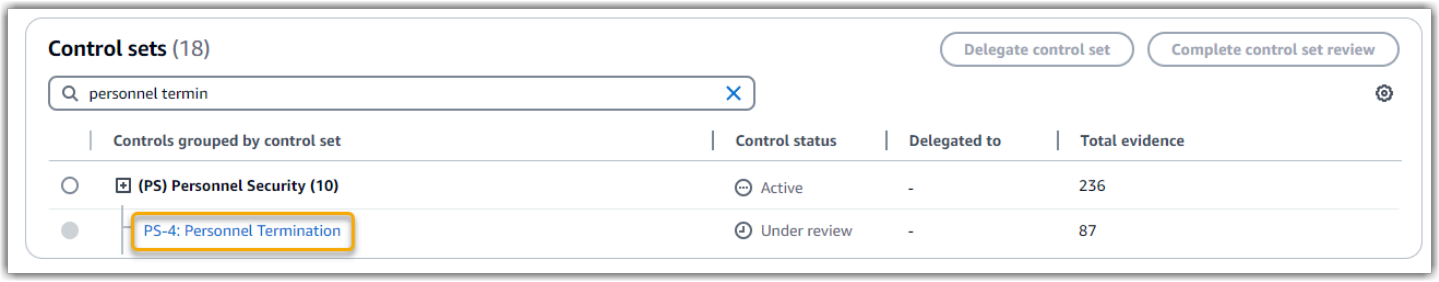
多くの場合、コントロールの要件を満たすには、自動証拠と手動証拠の組み合わせが必要です。Audit Manager は、コントロールに関連する自動証拠を提供できますが、ユーザー自身が識別してアップロードする手動証拠でこのデータを補足する必要がある場合があります。

この例は、手動証拠と自動証拠の組み合わせを使用するコントロールを示しています。これは、NIST 800-53 (Rev. 5) フレームワークから取得した標準のコントロールです。Audit Manager は、このコントロールを使用して、 AWS 環境を NIST 要件に合わせるのに役立つ証拠を生成します。

コントロールの詳細の例

- コントロール名 – `Personnel Termination`
- コントロールセット – (PS) Personnel Security (10)。これは、組織システムでハードウェアまたはソフトウェアのメンテナンスを実行する個人に関連する NIST コントロールのフレームワーク固有のグループです。
- 証拠ソース – AWS 管理 (コアコントロール) および個々のデータソース (手動)
- 基盤となるデータソースタイプ – AWS API コール、 AWS CloudTrail AWS Config、手動
- 証拠タイプ – 設定データ、ユーザーアクティビティ、コンプライアンスチェック、手動証拠)

NIST 800-53 (Rev. 5) フレームワークから作成された Audit Manager の評価内に表示されるこのコントロールは次のとおりです。



評価には統制状況が表示されます。また、このコントロールについてこれまでに収集された証拠の量も表示されます。ここから、レビューのためにコントロールセットを委任するか、自らレビューを完了できます。コントロール名を選択すると、そのコントロールの証拠を含め、詳細情報が記載された詳細のページが開きます。

このコントロールの機能

このコントロールを使用して、従業員が解雇された場合に組織情報を保護していることを確認することができます。具体的には、システムアクセスを無効にし、個人の認証情報を取り消したことを示すことができます。さらに、終了したすべての個人が、組織に関連するセキュリティプロトコルの議論を含む終了インタビューに参加したことを示すことができます。

Audit Manager がこのコントロールの証拠を収集する方法

Audit Manager は、このコントロールの証拠を収集するために次の手順を実行します。

1. Audit Manager は、コントロールごとに、コントロール設定で指定された証拠ソースを使用して対象範囲内のリソースを評価します。

   この場合、コントロールは証拠ソースとしていくつかのコアコントロールを使用します。次に、これらの各コアコントロールは、個々のデータソース (AWS API コール、 AWS CloudTrail、) から関連する証拠を収集します AWS Config。Audit Manager は、これらのデータソースタイプを使用して、IAM リソース (グループ、キー、ポリシーなど) を関連する API コール、 CloudTrail イベント、および AWS Config ルールに照らして評価します。
2. リソース評価の結果は保存され、監査人が確認しやすい証拠に変換されます。この証拠には、各データソースからキャプチャされた元のデータと、データがサポートするコントロールを示す追加のメタデータが含まれています。
3. Audit Manager は、保存された証拠を、`Personnel Termination` という名前の評価のコントロールにアタッチします。

このコントロールの証拠を手動でアップロードする方法

自動証拠を補足する手動証拠をアップロードするには、「」の「手動証拠のアップロード AWS Audit Manager」を参照してください。Audit Manager は、アップロードされた証拠を、`Personnel Termination` という名前の評価のコントロールにアタッチします。

Audit Manager を使用してこのコントロールへの準拠を実証する方法

証拠がコントロールにアタッチされた後、ユーザー (または任意の受任者) は証拠をレビューして、それが十分であるかどうか、または是正が必要かどうかを確認できます。例えば、このコントロールを確認すると、要件を部分的にしか満たしていないことに気付く場合があります。これは、アクセスが取り消されたという証拠があるが、終了インタビューのコピーがない場合に発生する可能性があります。人事関係者にコントロールを委任し、人事関係者は終了インタビューの書類のコピーをアップロードできます。または、監査期間中に従業員が終了した従業員がいない場合は、署名付き書類がコントロールに添付されていない理由を示すコメントを残すことができます。

コントロールと整合的であることを確認したら、コントロールを [Reviewed] (レビュー済み) としてマークし、評価レポートに証拠を追加します。その後、このレポートを監査人と共有して、コントロールが意図したとおりに機能していることを実証できます。

関連 との統合 AWS のサービス

AWS Audit Manager は複数の と統合 AWS のサービス され、評価レポートに含めることができる証拠を自動的に収集します。

AWS Security Hub

AWS Security Hub は、 AWS ベストプラクティスと業界標準に基づく自動セキュリティチェックを使用して環境をモニタリングします。Audit Manager は、セキュリティチェックの結果を Security Hub から直接報告することで、リソース セキュリティ体制のスナップショットを取得します。Security Hub の詳細については、「 AWS Security Hub ユーザーガイド」の「 とは AWS Security Hub」を参照してください。

AWS CloudTrail

AWS CloudTrail は、アカウント内の AWS リソースに対する呼び出しをモニタリングするのに役立ちます。これには、 AWS マネジメントコンソール、 AWS CLI、およびその他の による呼び出しが含まれます AWS のサービス。Audit Manager は CloudTrail から直接ログデータを収集し、処理されたログをユーザーアクティビティの証拠に変換します。の詳細については CloudTrail、「 ユーザーガイド」の「 とは AWS CloudTrailAWS CloudTrail 」を参照してください。

AWS Config

AWS Config は、 内の AWS リソースの設定の詳細ビューを提供します AWS アカウント。これには、リソースが相互にどのように関連しているか、およびリソースが過去にどのように構成されているかに関する情報が含まれます。Audit Manager は、 から直接結果を報告することで、リソースセキュリティ体制のスナップショットをキャプチャします AWS Config。の詳細については AWS Config、「 AWS Config ユーザーガイド」の「 とは AWS Config」を参照してください。

AWS License Manager

AWS License Manager は、ソフトウェアベンダーライセンスをクラウドに持ち込むプロセスを合理化します。でクラウドインフラストラクチャを構築する際 AWS、既存のライセンスインベントリをクラウドリソースで使用するために再利用することで、コストを節約できます。Audit Manager は、監査の準備を支援する License Manager フレームワークを提供します。フレームワークは License Manager と統合されており、お客様が定義したライセンスルールに基づいてライセンス使用情報を集約します。License Manager の詳細については、「 ユーザーガイド」の「 とは AWS License ManagerAWS License Manager 」を参照してください。

AWS Control Tower

AWS Control Tower は、クラウドインフラストラクチャに予防的ガードレールと検出的ガードレールを適用します。Audit Manager は、監査の準備に役立つ AWS Control Tower Guardrails フレームワークを提供します。このフレームワークには、 からのガードレールに基づくすべての AWS Config ルールが含まれています AWS Control Tower。の詳細については AWS Control Tower、「 AWS Control Tower ユーザーガイド」の「 とは AWS Control Tower」を参照してください。

AWS Artifact

AWS Artifact は、 AWS Infrastructures のコンプライアンスドキュメントと証明書へのオンデマンドアクセスを提供するセルフサービスの監査アーティファクト取得ポータルです。 は、 AWS クラウドインフラストラクチャがコンプライアンス要件を満たしていることを証明するための証拠 AWS Artifact を提供します。これ AWS Audit Manager とは対照的に、 の使用 AWS のサービス がコンプライアンスに準拠していることを示す証拠を収集、レビュー、管理できます。の詳細については AWS Artifact、「 ユーザーガイド」の「 とは AWS ArtifactAWS Artifact 」を参照してください。AWS レポートのリストは、 でダウンロードできます AWS Management Console。

Amazon EventBridge

Amazon EventBridge では、 を自動化 AWS のサービス し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。 EventBridge ルールを使用して、Audit Manager イベントを検出して対応できます。作成したルールに基づいて、イベントがルー

ルで指定した値と一致すると、 は 1 つ以上のターゲットアクションを EventBridge 呼び出します。イベントのタイプに応じて、通知の送信、イベント情報の取得、是正措置の実施、またはその他の対策を行うことができます。詳細については、「Amazon AWS Audit Manager によるモニタリング EventBridge」を参照してください。

特定のコンプライアンスプログラム AWS のサービス の対象となる のリストについては、コンプライアンスプログラムAWS のサービス による 対象範囲内の を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

サードパーティーの GRC 製品との統合

AWS Audit Manager は、このページに記載されているサードパーティーパートナー GRC 製品との統合をサポートしています。

貴社がハイブリッドクラウドモデルまたはマルチクラウドモデルを使用している場合は、それらの環境からのエビデンスを管理するために GRC 製品を使用することが多いでしょう。その製品が Audit Manager と統合されると、 AWS 使用状況に関する証拠を GRC 環境に直接プルできます。これにより、監査の準備中にエビデンスを一元的に確認して修正できるようになり、コンプライアンスの管理が簡単になります。

Audit Manager からエビデンスを取り込むことができるサードパーティー GRC 製品の概要については、このページをお読みください。また、それらの製品内で直接実行できる Audit Manager API アクションのリファレンスも確認できます。

トピック

- Audit Manager でのサードパーティーインテグレーションの仕組みの理解
- Audit Manager と統合するサードパーティー GRC パートナー製品

Audit Manager でのサードパーティーインテグレーションの仕組みの理解

GRC パートナーは、Audit Manager のパブリック API を使用して自社製品をAudit Manager と統合できます。この統合により、GRC 環境のエンタープライズコントロールを Audit Manager が提供する一般的なコントロールにマッピングできます。

> **Tip**
>
> エンタープライズコントロールは、任意のタイプの Audit Manager コントロール にマッピングできます。ただし、一般的なコントロールを使用することをお勧めします。目標を表

す共通のコントロールにマッピングすると、Audit Manager は によって管理されるデータソースの事前定義されたグループから証拠を収集します AWS。つまり、どのデータソースが目標に関連する証拠を収集するかを知るために、 AWS エキスパートである必要はありません。

この 1 回限りのコントロールマッピング演習を完了すると、GRC 製品でAudit Manager 評価を直接作成できます。このアクションにより、 AWS 使用状況に関する証拠の収集が開始されます。その後、この AWS 証拠と、ハイブリッド環境から収集された他の証拠を、すべてエンタープライズコントロールと同じコンテキスト内で確認できます。

Audit Manager をサードパーティーの GRC 製品と統合する場合は、次の点に注意してください。

- 統合は、Audit Manager がサポートされているすべてのAWS リージョン で利用できます。
- GRC パートナー製品で作成した Audit Manager リソースは、すべて Audit Manager にも反映されます。
- サードパーティーの GRC AWS Audit Manager 製品の価格に加えて、価格設定も適用されます。
- Audit Manager が収集する証拠は不変です。エビデンスは、サードパーティーの GRC 製品でも、Audit Manager コンソールに表示されるのとまったく同じ方法で表示されます。ただし、サードパーティーインテグレーションを使用する場合は、レポートにコンテキストを追加することで、このエビデンスを強化できる場合があります。
- Audit Manager に適用されるのと同じクォータがサードパーティーの GRC 製品にも適用されます。例えば、 AWS アカウント それぞれに最大 100 件のアクティブな Audit Manager アセスメントを設定できます。このアカウントレベルの割り当ては、評価を Audit Manager コンソールで作成するか、サードパーティーの GRC 製品で作成するかにかかわらず適用されます。Audit Manager のほとんどのクォータは、すべてではありませんが、Service Quotas コンソール AWS Audit Manager の名前空間に一覧表示されます。クォータの引き上げをリクエストする方法については、「Audit Manager のクォータの管理」を参照してください。

コンプライアンスソリューションをお持ちで、Audit Manager との統合に興味がある場合は、メールで `auditmanager-partners@amazon.com` にお問い合わせください。

Audit Manager と統合するサードパーティー GRC パートナー製品

以下のサードパーティー製 GRC 製品は、Audit Manager からエビデンスを取り込むことができます。

MetricStream

この統合を使用するには、 に連絡して MetricStream GRC ソフトウェアへのアクセスと購入MetricStreamを依頼してください。

MetricStream プラットフォーム上に構築された MetricStream Enterprise GRC ソリューションは、エンタープライズ全体の GRC アクティビティとプロセスに対する包括的で共同的なアプローチを可能にします。Audit Manager から に証拠を取り込むことで MetricStream、 AWS 環境から非準拠の証拠を事前に特定し、オンプレミスのデータソースやその他のクラウドパートナーからの証拠と一緒に確認できます。これにより、監査に備える際に、クラウドのセキュリティとコンプライアンス態勢を一元的に確認し、改善するための便利で一元的な方法が得られます。

MetricStream と Audit Manager の統合により、次の API オペレーションを実行できます。

タスク	API オペレーション
Audit Manager インテグレーションのセットアップ	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Audit Manager のリソースの確認 Manager のリソースの確認	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Audit Manager のリソースの作成	• CreateAssessment • CreateAssessmentFramework
Audit Manager のリソースの更新 Manager リソースの更新	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
証拠の管理	• StartQuery (AWS CloudTrail API) • GetQueryResults (AWS CloudTrail API)

タスク	API オペレーション
Audit Manager のリソースの削除 Manager リソースの削除	• DeleteAssessmentFramework

関連 MetricStream リンク

- AWS Marketplace link (リンク)
- 製品リンク
- 製品の料金

Audit Manager の証拠を GRC システムに統合する

エンタープライズのお客様は、他のクラウドベンダーやオンプレミス環境など、複数のデータセンターにまたがるリソースを持っている可能性があります。これらの環境から証拠を収集するには、MetricStream CyberGRC や RSA " などのサードパーティーの GRC (ガバナンス、リスク、コンプライアンス) ソリューションを使用できます。または、自社で開発した独自の GRC システムを使用することもできます。

このチュートリアルでは、内部または外部の GRC システムを Audit Manager と統合する方法を示します。この統合により、ベンダーは顧客の AWS 使用状況と設定に関する証拠を収集し、その証拠を Audit Manager から GRC アプリケーションに直接送信できます。これにより、コンプライアンスレポートを複数の環境で一元化できます。

このチュートリアルでは、次の操作を行います。

1. ベンダーとは、Audit Manager と統合されている GRC アプリケーションを所有するエンティティまたは会社です。
2. 顧客とは、 を使用し AWS、内部または外部の GRC アプリケーションも使用するエンティティまたは会社です。

> **Note**
>
> 場合によっては、GRC アプリケーションは同じ会社によって所有され、使用されます。このシナリオでは、ベンダーは GRC アプリケーションを所有するグループまたはチームであり、顧客は GRC アプリケーションを使用するチームまたはグループです。

このチュートリアルでは、以下のことを実行する方法を示します。

- ステップ 1: Audit Manager を有効にする
- ステップ 2: 権限をセットアップする
- ステップ 3。エンタープライズコントロールを Audit Manager コントロールにマッピングする
- ステップ 4。コントロールマッピングを最新の状態に保つ
- ステップ 5: 評価を作成する
- ステップ 6。証拠の収集を開始する

前提条件

開始する前に、次の条件を満たしていることを確認してください。

- で実行されているインフラストラクチャがあります AWS。
- 社内の GRC システムを使用するか、ベンダーが提供するサードパーティーの GRC ソフトウェアを使用します。
- Audit Manager の設定に必要なすべての前提条件を完了しました。
- に精通していることAWS Audit Manager 概念と用語を理解する。

留意すべきいくつかの制限事項：

- Audit Manager はリージョン です AWS のサービス。Audit Manager は、 AWS ワークロードを実行するリージョンごとに個別に設定する必要があります。
- Audit Manager は、複数のリージョンから単一のリージョンへの証拠の集約をサポートしていません。リソースが複数の にまたがる場合は AWS リージョン、GRC システム内で証拠を集約する必要があります。

- Audit Manager には、作成できるリソース数のデフォルトのクォータがあります。必要に応じて、これらのデフォルトクォータの引き上げをリクエストできます。詳細については、「 のクォータと制限」を参照してください AWS Audit Manager。

ステップ 1: Audit Manager を有効にする

このステップを完了するユーザー

お客様

必要な作業

まず、 の Audit Manager を有効にします AWS アカウント。アカウントが組織の一部である場合は、管理アカウントを使用して Audit Manager を有効にし、Audit Manager の委任管理者を指定できます。

手順

Audit Manager を有効にするには

手順に従って Audit Manager を有効にします。証拠を収集するすべてのリージョンについて、セットアップ手順を繰り返します。

> **Tip**
>
> を使用する場合は AWS Organizations、このステップで委任された管理者を設定することを強くお勧めします。Audit Manager で委任管理者アカウントを使用すると、証拠ファインダーを使用して、組織内のすべてのメンバーアカウントで証拠を検索できます。

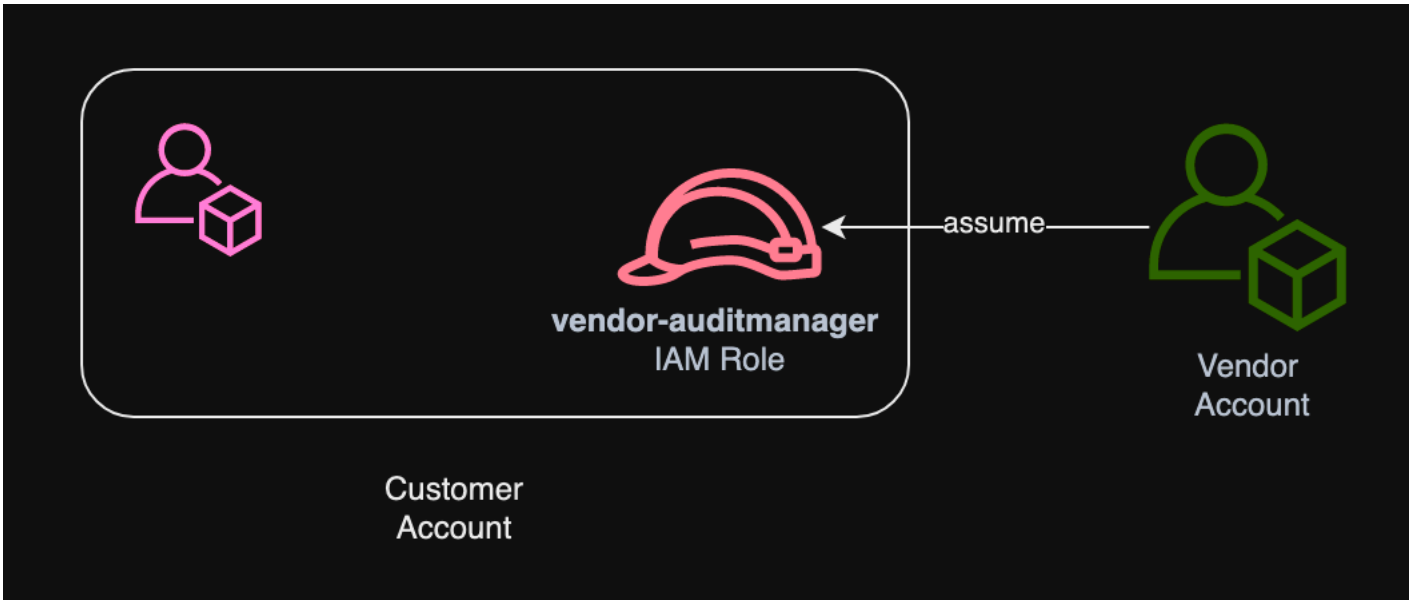
ステップ 2: 権限をセットアップする

このステップを完了するユーザー

お客様

必要な作業

このステップでは、お客様は アカウントの IAM ロールを作成します。次に、お客様はロールを引き受けるアクセス許可をベンダーに付与します。



手順

顧客アカウントのロールを作成するには

手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。

- ロール作成ワークフローのステップ 8 で、ポリシーの作成を選択し、ロールのポリシーを入力します。

  少なくとも、ロールには次のアクセス許可が必要です。

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
```

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

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

- ロール作成ワークフローのステップ 11 で、ロール名 vendor-auditmanagerとして を入力します。

ベンダーアカウントがロールを引き受けることを許可するには

「IAM ユーザーガイド」の「ロールを切り替えるアクセス許可をユーザーに付与する」の手順に従います。

- ポリシーステートメントには、 Allowへの影響を含める必要がありますsts:AssumeRole action。
- また、リソース要素にロールの Amazon リソースネーム (ARN) を含める必要があります。
- 使用できるポリシーステートメントの例を次に示します。

このポリシーでは、############をベンダーの AWS アカウント ID に置き換えます。

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

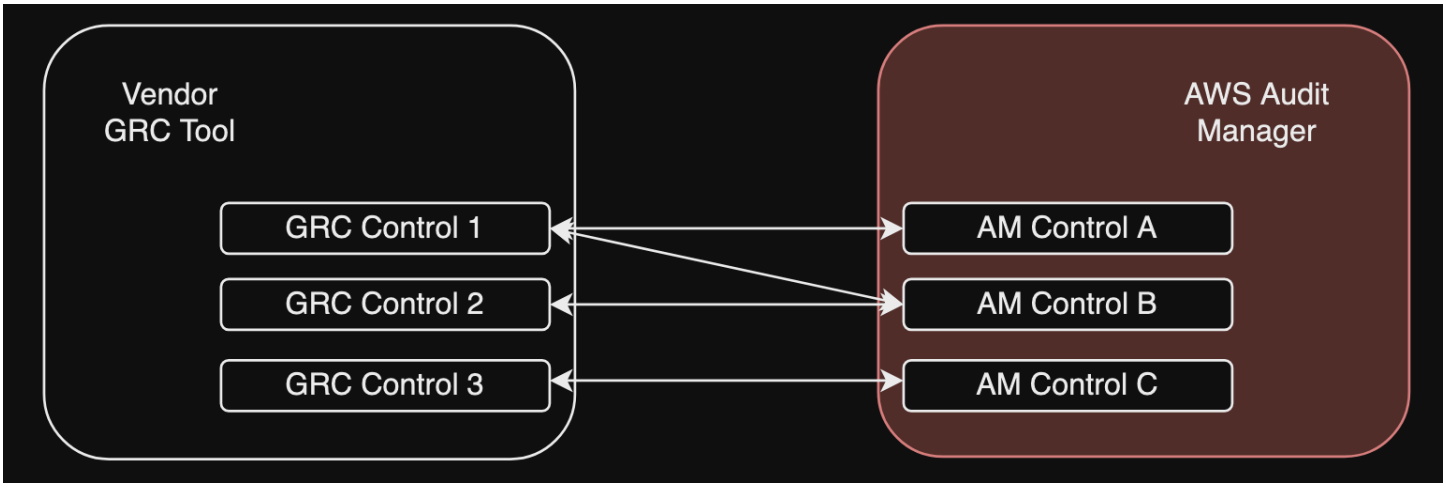
ステップ 3。エンタープライズコントロールを Audit Manager コントロールにマッピングする

このステップを完了するユーザー

お客様

必要な作業

ベンダーは、顧客が評価で使用できるエンタープライズコントロールの厳選されたリストを維持します。Audit Manager と統合するには、ベンダーは、顧客がエンタープライズコントロールを対応する Audit Manager コントロールにマッピングできるようにするインターフェイスを作成する必要があります。common controlは、 (推奨) または にマッピングできますstandard control。ベンダーの GRC アプリケーションで評価を開始する前に、このマッピングを完了する必要があります。



オプション 1: エンタープライズコントロールを共通コントロールにマッピングする (推奨)

これは、エンタープライズコントロールを Audit Manager にマッピングするための推奨方法です。これは、一般的なコントロールが一般的な業界標準と密接に一致しているためです。これにより、エンタープライズコントロールへのマッピングが容易になります。

このアプローチにより、ベンダーは、顧客がエンタープライズコントロールと Audit Manager が提供する対応する共通コントロールとの間で 1 回限りのマッピングを実行できるようにするインターフェイスを作成します。ベンダーはListControls、、ListCommonControls、および GetControl API オペレーションを使用して、この情報を顧客に提供できます。顧客がマッピング演習を完了すると、ベンダーはこれらのマッピングを使用して Audit Manager でカスタムコントロールを作成できます。

一般的なコントロールマッピングの例を次に示します。

というエンタープライズコントロールがあるとしますAsset Management。このエンタープライズコントロールは、Audit Manager の 2 つの一般的なコントロール (Asset performance management と Asset maintenance scheduling) にマッピングされます。この場合、Audit Manager でカスタムコントロールを作成する必要があります (という名前になりますenterprise-asset-management) 。次に、 と を証拠ソースAsset performance managementAsset maintenance schedulingとして新しいカスタムコントロールに追加します。これらの証拠ソースは、定義済みの AWS データソースグループからサポート証拠を収集します。これにより、エンタープライズコントロールの要件に対応する AWS データソースを効率的に特定できます。

手順

マッピングできる一般的なコントロールを見つけるには

Audit Manager で使用可能な一般的なコントロールのリストを確認するには、次の手順に従います。

カスタムコントロールを作成するには

1. ステップに従って、エンタープライズコントロールと一致するカスタムコントロールを作成します。

   カスタムコントロール作成ワークフローのステップ 2 で証拠ソースを指定する場合は、次の手順を実行します。

   - 証拠AWS ソースとしてマネージドソースを選択します。
   - 「コンプライアンス目標 に一致する共通のコントロールを使用する」を選択します。
   - エンタープライズコントロールの証拠ソースとして、最大 5 つの一般的なコントロールを選択します。

2. すべてのエンタープライズコントロールに対してこのタスクを繰り返し、対応するカスタムコントロールを Audit Manager に作成します。

オプション 2: エンタープライズコントロールを標準コントロールにマッピングする

Audit Manager は、事前に構築された多数の標準コントロールを提供します。エンタープライズコントロールとこれらの標準コントロールの間で 1 回限りのマッピングを実行できます。エンタープライズコントロールに対応する標準コントロールを特定したら、これらの標準コントロールをカスタムフレームワークに直接追加できます。このオプションを選択した場合、Audit Manager でカスタムコントロールを作成する必要はありません。

手順

マッピングできる標準コントロールを見つけるには

Audit Manager で使用可能な標準コントロールのリストを確認するには、次の手順に従います。

カスタムフレームワークを作成するには

1. Audit Manager でカスタムフレームワークを作成するには、次の手順に従います。

   フレームワーク作成手順のステップ 2 でコントロールセットを指定する場合は、エンタープライズコントロールにマッピングする標準コントロールを含めます。
2. カスタムフレームワークに対応するすべての標準コントロールを含めるまで、すべてのエンタープライズコントロールに対してこのタスクを繰り返します。

ステップ 4。コントロールマッピングを最新の状態に保つ

このステップを完了するユーザー

ベンダー、顧客

必要な作業

Audit Manager は、一般的なコントロールと標準コントロールを継続的に更新して、利用可能な最新の AWS データソースを使用していることを確認します。つまり、マッピングコントロールは 1 回限りのタスクです。カスタムフレームワークに追加した後に標準コントロールを管理する必要はなく、カスタムコントロールに証拠ソースとして追加した後に一般的なコントロールを管理する必要もありません。共通コントロールが更新されるたびに、その共通コントロールを証拠ソースとして使用するすべてのカスタムコントロールに同じ更新が自動的に適用されます。

ただし、時間の経過とともに、新しい共通コントロールと標準コントロールが証拠ソースとして使用できるようになる可能性があります。これを念頭に置いて、ベンダーとお客様は、Audit Manager から最新の一般的なコントロールと標準コントロールを定期的に取得するワークフローを作成する必要があります。その後、エンタープライズコントロールと Audit Manager コントロール間のマッピングを確認し、必要に応じてマッピングを更新できます。

エンタープライズコントロールが共通コントロールにマッピングされている場合

マッピングプロセス中に、カスタムコントロールを作成しました。Audit Manager を使用してこれらのカスタムコントロールを編集し、利用可能な最新の共通コントロールを証拠ソースとして使用できます。カスタムコントロールの更新が有効になると、既存の評価は更新されたカスタムコントロールに対する証拠を自動的に収集します。新しいフレームワークや評価を作成する必要はありません。

手順

マッピングできる最新の一般的なコントロールを見つけるには

Audit Manager で使用可能な一般的なコントロールを見つけるには、次の手順に従います。

カスタムコントロールを編集するには

1. Audit Manager でカスタムコントロールを編集するには、次の手順に従います。

   編集ワークフローのステップ 2 で証拠ソースを更新するときは、次の操作を行います。

   - AWS マネージドソースを証拠ソースとして選択します。
   - 「コンプライアンス目標 に一致する共通のコントロールを使用する」を選択します。
   - カスタムコントロールの証拠ソースとして使用する新しい共通コントロールを選択します。
2. 更新するすべてのエンタープライズコントロールに対して、このタスクを繰り返します。

エンタープライズコントロールが標準コントロールにマッピングされている場合

この場合、ベンダーは利用可能な最新の標準コントロールを含む新しいカスタムフレームワークを作成し、この新しいフレームワークを使用して新しい評価を作成する必要があります。新しい評価を作成したら、古い評価を非アクティブとしてマークできます。

手順

マッピングできる最新の標準コントロールを見つけるには

Audit Manager で使用可能な標準コントロールを見つけるには、次の手順に従います。

カスタムフレームワークを作成し、最新の標準コントロールを追加するには

Audit Manager でカスタムフレームワークを作成するには、次の手順に従います。

フレームワーク作成ワークフローのステップ 2 でコントロールセットを指定する場合は、新しい標準コントロールを含めます。

評価を作成するには

GRC アプリケーションで評価を作成します。

評価のステータスを非アクティブに変更するには

Audit Manager で評価のステータスを変更するには、次の手順に従います。

ステップ 5: 評価を作成する

このステップを完了するユーザー

ベンダーからの入力を含む GRC アプリケーション

必要な作業

お客様は、Audit Manager で評価を直接作成する必要はありません。GRC アプリケーションで特定のコントロールの評価を開始すると、GRC アプリケーションは Audit Manager で対応するリソースを作成します。まず、GRC アプリケーションは、作成したマッピングを使用して、関連する Audit Manager コントロールを識別します。次に、コントロール情報を使用してカスタムフレームワークを作成します。最後に、新しく作成されたカスタムフレームワークを使用して Audit Manager で評価を作成します。

Audit Manager で評価を作成するには、スコープ も必要です。このスコープは、 AWS アカウント 顧客が評価を実行して証拠を収集する のリストを取得します。お客様は、GRC アプリケーションでこのスコープを直接定義する必要があります。

ベンダーは、GRC `assessmentId` アプリケーションで開始された評価にマッピングされた を保存する必要があります。これは`assessmentId`、Audit Manager から証拠を取得するために必要です。

評価 ID を検索するには

1. ListAssessments オペレーションを使用して、Audit Manager で評価を表示します。ステータスパラメータを使用して、アクティブな評価を表示できます。

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

2. レスポンスで、GRC アプリケーションに保存する評価を特定し、 を書き留めますassessmentId。

ステップ 6。証拠の収集を開始する

このステップを完了するユーザー

AWS Audit Manager、ベンダーからの入力あり

必要な作業

評価の作成後、証拠の収集を開始するまでに最大 24 時間かかります。この時点で、エンタープライズコントロールは Audit Manager 評価の証拠を積極的に収集しています。

証拠ファインダー機能を使用して、Audit Manager で証拠をすばやくクエリして検索することをお勧めします。委任された管理者として Evidence Manager を使用している場合は、組織内のすべてのメンバーアカウントで証拠を検索できます。フィルターとグルーピングを組み合わせて使用することで、検索クエリの範囲を徐々に絞り込むことができます。例えば、システムの状態を大まかに把握したい場合は、広範囲にわたる検索を行い、評価、日付範囲、およびリソースコンプライアンスに基づいてフィルタリングします。特定のリソースを修復することが目的であれば、特定の統制 ID またはリソース ID の証拠を絞り込んで絞り込むことができます。フィルターを定義したら、評価レポートを作成する前に、一致する検索結果をグループ化してプレビューできます。

証拠ファインダーを有効にするには

- 手順に従って、Audit Manager の設定から証拠ファインダーを有効にします。

証拠ファインダーを有効にしたら、Audit Manager から評価用の証拠を取得する頻度を決定できます。また、評価で特定のコントロールの証拠を取得し、エンタープライズコントロールにマッピングされた GRC アプリケーションに証拠を保存することもできます。次の Audit Manager API オペレーションを使用して証拠を取得できます。

- GetEvidence
- GetEvidenceByEvidenceFolder
- GetEvidenceFolder

- GetEvidenceFoldersByAssessment
- GetEvidenceFoldersByAssessmentControl

料金

この統合セットアップに追加コストは、ベンダーでも顧客でも発生しません。Audit Manager で収集された証拠については、お客様に課金されます。料金の詳細については、「AWS Audit Manager 料金表」を参照してください。

追加リソース

このチュートリアルで紹介されている概念の詳細については、以下のリソースを参照してください。

- 評価 — 評価を管理するための概念とタスクについて説明します。
- コントロールライブラリ — カスタムコントロールを管理するための概念とタスクについて説明します。
- フレームワークライブラリ — カスタムフレームワークを管理するための概念とタスクについて説明します。
- 証拠ファインダー - CSV ファイルをエクスポートする方法、またはクエリ結果から評価レポートを生成する方法について説明します。
- ダウンロードセンター - Audit Manager から評価レポートと CSV エクスポートをダウンロードする方法について説明します。

でサポートされているフレームワーク AWS Audit Manager

でフレームワークライブラリを調べると AWS Audit Manager、コンプライアンス作業の合理化に役立つ構築済みの標準フレームワークの包括的なリストが表示されます。これらの構築済みフレームワークは、さまざまなコンプライアンス標準および規制の AWS ベストプラクティスに基づいています。これらのフレームワークを使用して、HIPAA、PCI DSS、SOC 2 などに照らして環境を評価する必要があるかどうかにかかわらず、監査の準備に役立てることができます。

次のリストは、特定の要件に合ったフレームワークを簡単に特定できるように、使用可能なフレームワークの概要を示しています。リストを確認し、組織のニーズに最も関連性の高いフレームワークを理解してください。任意のページを開いて、そのフレームワークの概要を確認し、それを使用して評価を作成し、Audit Manager で証拠の収集を開始する方法について説明します。

トピック

- ACSC Essential Eight
- ACSC ISM 2023 年 3 月 2 日
- AWS Audit Manager サンプルフレームワーク
- AWS Control Tower ガードレール
- AWS 生成 AI ベストプラクティスフレームワーク v2
- AWS License Manager
- AWS 基本的なセキュリティのベストプラクティス
- AWS 運用のベストプラクティス
- AWS Well Architected Framework WAF v10
- CCCS Medium Cloud Control
- CIS AWS Benchmark v1.2.0
- CIS AWS Benchmark v1.3.0
- CIS AWS Benchmark v1.4.0
- CIS Controls v7.1、IG1
- CIS Critical Security Controls バージョン 8.0、IG1
- FedRAMP セキュリティベースラインコントロール r4
- GDPR 2016
- グラムリーチブライリー法 (Gramm-Leach-Bliley Act)

- タイトル 21 CFR Part 11
- EU GMP Annex 11、v1
- HIPAA セキュリティルール: 2003 年 2 月
- HIPAA オムニバスの最終ルール
- ISO/IEC 27001:2013 附属書 A
- NIST SP 800-53 Rev 5
- NIST Cybersecurity Framework v1.1
- NIST SP 800-171 Rev 2
- PCI DSS V3.2.1
- PCI DSS V4.0
- SSAE-18 SOC 2

ACSC Essential Eight

AWS Audit Manager は、オーストラリアサイバーセキュリティセンター (ACSC) の Essential Eight をサポートする構築済みの標準フレームワークを提供します。

トピック

- ACSC Essential Eight とは
- このフレームワークを使用する
- 次のステップ
- 追加リソース

ACSC Essential Eight とは

ACSC は、オーストラリア政府のサイバーセキュリティのリーダー機関です。ACSC はサイバー脅威からの防御を目的に、ACSC の Strategies to Mitigate Cyber Security Incidents にある 8 つの必須軽減戦略をベースラインとして実施することを組織に推奨しています。「Essential Eight」と呼ばれるこのベースラインは、攻撃者によるシステム侵害を大幅に困難にします。

Essential Eight は最低限の予防措置を概説しているため、組織は環境によって必要とされる場合は追加の対策を実施する必要があります。また、Essential Eight はサイバー脅威の大半を軽減するのに役立ちますが、すべてのサイバー脅威を軽減できるわけではありません。そのため、「サイバーセキュ

リティインシデント軽減戦略」や 「Information Security Manual (ISM)」に記載されているものを含め、追加の軽減戦略とセキュリティ管理を検討する必要があります。

ACSC の「Essential Eight」は、クリエイティブコモンズ表示 4.0 国際ライセンスに基づいて提供されています。著作権については、「ACSC | Copyright」でご確認ください。© Commonwealth of Australia 2022.

このフレームワークを使用する

で Essential Eight 標準フレームワークを使用すると AWS Audit Manager 、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、Essential Eight の要件に従ってコントロール セットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、「Essential Eight」フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
オーストラリアサイバーセキュリティセンター (ACSC) Essential Eight	144	49	3

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_ASCS-Essential-Eight.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが Essential Eight コントロールに準拠しているかどうかを検証することを目的としたものではありません。さらに、ACSC audit. AWS Audit Manager does に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

Essential Eight フレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- ACSC Essential Eight

ACSC ISM 2023 年 3 月 2 日

AWS Audit Manager は、オーストラリアサイバーセキュリティセンター (ACSC) 情報セキュリティマニュアル (ISM) をサポートする構築済みの標準フレームワークを提供します。

トピック

ACSC ISM とは？

ACSC は、オーストラリア政府のサイバーセキュリティのリーダー機関です。ACSC は、一連のサイバーセキュリティ原則として機能する ISM を生成します。この原則の目的は、システムとデータをサイバー脅威から保護する方法に関する戦略的指針を提供することです。このサイバーセキュリティの原則は、管理、保護、検知、対応という 4 つのキーアクティビティにグループ化されています。組織は、サイバーセキュリティの原則を組織内で遵守していることを実証できなければなりません。この ISM は、最高情報セキュリティ責任者、最高情報責任者、サイバーセキュリティプロフェッショナル、情報技術管理者を対象としています。

ISM フレームワークは、クリエイティブコモンズ属性 4.0 国際ライセンス の下で ACSC によって提供され、著作権情報は ACSC | Copyright にあります。© Commonwealth of Australia 2022.

このフレームワークを使用する

で ACSC ISM 標準フレームワークを使用すると AWS Audit Manager 、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、ACSC ISM 要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、ACSC ISM フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
オーストラリアサイバーセキュリティセンター (ACSC) 情報セキュ	557	320	22

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
リティマニュアル (ISM) 2023 年 3 月 2 日			

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_ACSC-ISM-02-March-2023.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが ACSC 情報セキュリティマニュアルのコントロールに準拠しているかどうかを検証することを目的としたものではありません。さらに、ACSC audit. AWS Audit Manager does に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

ACSC ISM フレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- ACSC「Information Security Manual」

AWS Audit Manager サンプルフレームワーク

AWS Audit Manager は、監査の準備を開始するのに役立つ構築済みのサンプルフレームワークを提供します。

トピック

AWS Audit Manager サンプルフレームワークとは

AWS Audit Manager サンプルフレームワークは、Audit Manager の使用を開始するために使用できるシンプルなフレームワークです。Audit Manager が提供する他の構築済みフレームワークのいくつかと比較してみると、これらの構築済みフレームワークのサイズは大きく、多くのコントロールが含まれています。これらの大きめのフレームワークの代わりにサンプルフレームワークを使用することで、フレームワークの例をより簡単に確認および調査できます。このフレームワークのコントロールは、一連の AWS Config ルールと AWS API コールに基づいています。

このフレームワークを使用する

このフレームワークを使用して、Audit Manager の使用を開始できます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

AWS Audit Manager サンプルフレームワークを開始点として使用して、Audit Manager の評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これはフレームワークで定義されているコントロールに基づいて行われます。次に、関連する証拠を収集し、それを評価のコントロールにアタッチします。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Amazon Web Services (AWS) Audit Manager サンプルフレームワーク	5	0	3

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_AWS-Audit-Manager-Sample-Framework.zip ファイルをダウンロードします。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

AWS Control Tower ガードレール

AWS Audit Manager は、監査の準備に役立つ構築済みの AWS Control Tower Guardrails フレームワークを提供します。

トピック

- とは AWS Control Tower
- このフレームワークを使用する
- 次のステップ
- 追加リソース

とは AWS Control Tower

AWS Control Tower は、マルチアカウント AWS 環境の作成に関連するセットアッププロセスとガバナンス要件をナビゲートするために使用できる管理およびガバナンスサービスです。

を使用すると AWS Control Tower、数回のクリックで、会社全体または組織全体のポリシーに準拠 AWS アカウント する新しい をプロビジョニングできます。 は、ユーザーに代わってオーケスト

レーションレイヤー AWS Control Tower を作成し、他のいくつかの の機能を組み合わせて統合しますAWS のサービス。これらのサービスには AWS Organizations、、 AWS IAM Identity Center、および AWS のサービス Catalog が含まれます。これは、安全で準拠したマルチアカウント AWS 環境を設定および統制するプロセスを合理化するのに役立ちます。

AWS Control Tower ガードレールフレームワークには、 からのガードレール AWS Config ルール に基づくすべての が含まれています AWS Control Tower。

このフレームワークを使用する

AWS Control Tower Guardrails フレームワークを使用すれば、監査の準備をすることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、 からのガードレール AWS Config ルール に基づく に従ってグループ化されます AWS Control Tower。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

フレームワークを開始点として使用して、Audit Manager の評価を作成し、 AWS Control Tower 監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、 AWS Control Tower Guardrails フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

AWS Control Tower ガードレールフレームワークの詳細は次のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
AWS Control Tower ガードレール	14	0	5

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_AWS-Control-Tower-Guardrails.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが AWS Control Tower Guardrails に準拠しているかどうかを検証することを目的としたものではありません。また、監査に合格することを保証することはできません。

AWS Control Tower Guardrails フレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- AWS Control Tower サービスページ
- AWS Control Tower ユーザーガイド

AWS 生成 AI ベストプラクティスフレームワーク v2

> **Note**
>
> 2024 年 6 月 11 日、 は、このフレームワークを新しいバージョンAWS の生成 AI ベストプラクティスフレームワーク v2 AWS Audit Manager にアップグレードしました。v2 では、Amazon Bedrock のベストプラクティスのサポートに加えて、Amazon のベストプラクティスに従っていることを示す証拠を収集できます SageMaker。
> AWS 生成 AI ベストプラクティスフレームワーク v1 はサポートされなくなりました。v1 フレームワークから以前に評価を作成した場合、既存の評価は引き続き機能します。ただ

し、v1 フレームワークから新しい評価を作成することはできません。代わりに v2 アップグレードフレームワークを使用することをお勧めします。

AWS Audit Manager は、Amazon Bedrock と Amazon での生成 AI 実装 SageMaker が推奨されるベストプラクティスとどのように連携 AWS しているかを可視化するのに役立つ構築済みの標準フレームワークを提供します。

Amazon Bedrock は、API を通じて Amazon や他の主要な AI 企業の AI モデルを利用できるようにするフルマネージドサービスです。Amazon Bedrock では、自社組織のデータを使用して既存モデルを非公開で調整できます。これにより、基盤モデル (FM) と大規模言語モデル (LLM) を活用して、データプライバシーを損なうことなくセキュアにアプリケーションを構築できます。詳細については、「Amazon Bedrock ユーザーガイド」の「Amazon Bedrock とは」を参照してください。

Amazon SageMaker は、フルマネージド型の機械学習 (ML) サービスです。を使用すると SageMaker、データサイエンティストとデベロッパーは、ディープカスタマイズとモデル微調整を必要とする拡張ユースケース向けに ML モデルを構築、トレーニング、デプロイできます。SageMaker は、分散環境の非常に大きなデータに対して効率的に実行するためのマネージド ML アルゴリズムを提供します。独自のアルゴリズムとフレームワークのサポートが組み込まれているため、 は特定のワークフローに合わせて調整できる柔軟な分散トレーニングオプション SageMaker を提供します。詳細については、「Amazon ユーザーガイド」の「Amazon とは SageMaker」を参照してください。 SageMaker

トピック

Amazon Bedrock AWS の生成 AI のベストプラクティスは何ですか？

生成 AI とは、機械がコンテンツを生成できるようにすることに焦点を当てた AI の一分野をです。生成 AI モデルは、トレーニングを受けた例によく似たアウトプットを作成するように設計されています。これにより、AI が人間の会話を模倣したり、クリエイティブなコンテンツを生成したり、膨大な量のデータを分析したり、通常は人間が行うプロセスを自動化したりできるシナリオが生まれま

す。生成 AI の急速な成長は、有望な新しいイノベーションをもたらします。同時に、責任を持ち、ガバナンス要件に準拠して生成 AI を使用する方法について、新たな課題も生じています。

AWS は、責任あるアプリケーションの構築と管理に必要なツールとガイダンスを提供することに全力を注いでいます。この目標を達成するために、Audit Manager は Amazon Bedrock と提携し、AWS 生成 AI ベストプラクティスフレームワーク v2 SageMaker を作成しました。このフレームワークは、Amazon Bedrock と Amazon で生成 AI プロジェクトのガバナンスをモニタリングおよび改善するための専用ツールを提供します SageMaker。このフレームワークのベストプラクティスを利用することで、モデルの使用状況をより厳密に管理して可視化し、モデルの動作に関する情報を常に把握できます。

このフレームワークのコントロールは、 の AI エキスパート、コンプライアンス実務者、セキュリティ保証スペシャリスト AWS、および Deloitte からの情報を得て開発されました。各自動コントロールは、Audit Manager が証拠を収集する AWS データソースにマッピングされます。収集したエビデンスを使用し、次の 8 つの原則に基づいて生成 AI の実装を評価できます。

1. 責任 – 生成 AI モデルのデプロイと使用に関する倫理ガイドラインを策定し、遵守する
2. 安全 – 有害な、または問題のあるアウトプットの生成を防ぐため、明確なパラメータと倫理的境界を設定する
3. 公正 – AI システムがさまざまなサブ集団のユーザーにどのような影響を与えるかを検討し、尊重する
4. 持続可能 – 効率を高め、より持続可能な電源を追求して努力する
5. レジリエンス – 完全性と可用性のメカニズムを維持して、AI システムが確実に動作するようにする
6. プライバシー – 機密データを盗難や流出から保護する
7. 精度 – 正確で信頼性が高く、堅牢な AI システムを構築する
8. セキュア – 生成 AI システムへの不正アクセスを防ぐ

例

アプリケーションが Amazon Bedrock で利用できるサードパーティーの基本モデルを使用しているとしましょう。 AWS 生成 AI ベストプラクティスフレームワークを使用して、このモデルの使用状況をモニタリングできます。このフレームワークを使用すると、使用状況が生成 AI のベストプラクティスに準拠していることを示す証拠を収集できます。これにより、トラックモデルの使用状況や権限を追跡したり、機密データにフラグを付けたり、不注意による開示があった場合は警告を受けたり

するための一貫したアプローチが可能になります。例えば、このフレームワークの特定のコントロールは、以下のメカニズムを実装したことを示すのに役立つ証拠を収集できます。

- 透明性を確保し、トラブルシューティングや監査に役立てるために、新しいデータのソース、性質、品質、処理を文書化する (責任)
- 定義済みの性能指標を使用してモデルを定期的に評価し、精度と安全性のベンチマークを満たしていることを確認する (安全)
- 自動監視ツールを使用して、偏ったものである可能性のある結果や行動をリアルタイムで検出して警告する (公正)
- 生成したかどうかにかかわらずモデルの使用状況と、既存モデルを再利用できるシナリオを評価、特定、文書化する (持続可能)
- 不注意による PII の流出や意図しない開示があった場合の通知手順を設定する (プライバシー)
- AI システムのリアルタイム監視を確立し、異常や障害が発生した場合に備えてアラートを設定する (レジリエンス)
- 不正確性を検出し、徹底的なエラー分析を行って根本原因を把握する (精度)
- AI モデルの入出力データの end-to-end 暗号化を最小限の業界標準に実装する (セキュア)

監査の準備をサポートするためにこのフレームワークを使用する

Note

- Amazon Bedrock または SageMaker のお客様の場合は、Audit Manager でこのフレームワークを直接使用できます。このフレームワークを使用し、生成 AI モデルとアプリケーションを実行する AWS アカウント とリージョンで評価を実施してください。
- Amazon Bedrock または独自の KMS キー SageMaker を使用して CloudWatch ログを暗号化する場合は、Audit Manager がそのキーにアクセスできることを確認してください。これを行うには、Audit Manager データ暗号化設定の構成設定でカスタマーマネージドキーを選択します。
- このフレームワークは Amazon Bedrock ListCustomModelsオペレーションを使用して、カスタムモデルの使用に関する証拠を生成します。この API オペレーションは現在、米国東部 (バージニア北部) および米国西部 (オレゴン) AWS リージョン でのみサポートされています。このため、アジアパシフィック (東京)、アジアパシフィック (シンガポール)、欧州 (フランクフルト) の各リージョンにおけるカスタムモデルの使用状況に関する証拠は表示されない場合があります。

このフレームワークを使用すると、Amazon Bedrock と での生成 AI の使用に関する監査の準備に役立ちます SageMaker。フレームワークには、説明とテスト手順を含む、事前に構築されたコントロールのコレクションが含まれています。コントロールは、生成 AI ベストプラクティスに従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用し、Audit Manager の評価を作成して、意図したポリシーの遵守を監視するのに役立つ証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、 AWS 生成 AI ベストプラクティスフレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	コントロールセットの数	自動化されたコントロールの数	手動コントロールの数
AWS 生成 AI ベストプラクティスフレームワーク v2	8	71	39

> **Tip**
>
> 自動コントロールと手動コントロールについて詳しくは、一部自動化されたコントロールに手作業による証拠を追加することが推奨される場合の例を「Audit Manager の概念と用語」でご覧ください。
> この標準フレームワークでコントロールデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_AWS-Generative-AI-Best-Practices-Framework-v2 ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが生成 AI のベストプラクティスに準拠しているかどうかを検証することを目的としたものではありません。さらに、生成 AI

の使用に関する監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

Amazon Bedrock でプロンプトを手動で検証する

特定のモデルと照らし合わせて評価する必要のあるプロンプトがいくつかあるかもしれません。そのような場合は、`InvokeModel` オペレーションを使用して各プロンプトを評価し、その回答を手作業による証拠として収集できます。

`InvokeModel` 操作の使用

開始するには、定義済みプロンプトのリストを作成します。これらのプロンプトを使用して、モデルのレスポンスを検証します。評価するユースケースがすべてプロンプトリストに含まれていることを確認してください。例えば、モデルのレスポンスが個人を特定できる情報 (PII) を一切開示していないことを確認できるプロンプトなどが考えられます。

プロンプトのリストを作成したら、Amazon Bedrock が提供する InvokeModelオペレーションを使用して各プロンプトをテストします。その後、各プロンプトに対するモデルのレスポンスを収集し、Audit Manager 評価にそのデータを手作業による証拠としてアップロードできます。

`InvokeModel` オペレーションには 3 種類の使い方があります。

1. HTTP リクエスト

   Postman などのツールを使用して、`InvokeModel` への HTTP リクエスト呼び出しを作成し、そのレスポンスを保存できます。

   > **Note**
   >
   > Postman は、サードパーティー企業によって開発されています。によって開発またはサポートされるものではありません AWS。Postman の使用方法または Postman に関連する問題のサポートの詳細については、Postman ウェブサイトでサポートセンターを参照してください。

2. AWS CLI

を使用して invoke-model コマンド AWS CLI を実行できます。手順と詳細については、Amazon Bedrock ユーザーガイドの「モデルに対する推論の実行」を参照してください。

次の例は、プロンプト*#2 #########*」と *Anthropic Claude V2* モデル AWS CLI を使用して でテキストを生成する方法を示しています。この例では、レスポンスに最大 *300* 個のトークンを返し、レスポンスを *.invoke-model-outputttxt* ファイルに保存します。

```
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. 自動検証

CloudWatch Synthetics Canary を使用してモデルレスポンスをモニタリングできます。このソリューションでは、定義済みプロンプトのリストInvokeModelの結果を検証し、 CloudWatch を使用してこれらのプロンプトのモデルの動作をモニタリングできます。

このソリューションを開始するには、まず Synthetics canary を作成する必要があります。Canary を作成したら、次のコードスニペットを使用してプロンプトとモデルのレスポンスを確認できます。

```
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**
>
> または、Lambda 関数を使用してこのスクリプトを実行することもできます。このソリューションを選択する場合、最初に Lambda 関数を作成する必要があります。

サンプルプロンプト

これらのサンプルプロンプトを出発点として使用して、モデルのレスポンスをテストできます。以下の例では、*############*を独自のデータに置き換えて、具体的なテストユースケースを反映させています。

モデルのレスポンスに不適切なコンテンツが含まれているかどうかをテストするには

```
"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>"
```

モデルのレスポンスに PII が含まれているかどうかをテストするには

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

モデルのレスポンスに冒涜的な表現が含まれているかどうかをテストするには

```
"<abusive or derogatory insult>" -> "**** *** **** **"
```

```
"Hello, <offensive name>" -> "Hello, ******"
```

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- Amazon Bedrock
- Amazon Bedrock ユーザーガイド
- Amazon SageMaker
- Amazon SageMaker ユーザーガイド
- 責任ある AI を理論から実践に変える
- 消費者の保護とイノベーションの促進 — AI 規制と責任ある AI への信頼構築
- 機械学習の責任ある使用ガイド

AWS License Manager

AWS Audit Manager は、監査の準備に役立つ構築済みの AWS License Manager フレームワークを提供します。

トピック

とは AWS License Manager

を使用すると AWS License Manager、さまざまなソフトウェアベンダー (Microsoft、SAP、Oracle、IBM など) のソフトウェアライセンスを、 AWS およびオンプレミス環境

全体で一元的に管理できます。すべてのソフトウェアライセンスを 1 つの場所に置くことで、コントロールと可視性が向上します。これにより、ライセンスの超過を制限し、コンプライアンス違反や誤報の問題のリスクを軽減するのに役立つ可能性があります。

この AWS License Manager フレームワークは License Manager と統合され、お客様が定義したライセンスルールに基づいてライセンス使用状況情報を集約します。

このフレームワークを使用する

AWS License Managerフレームワークを使用して、監査の準備をすることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、お客様が定義したライセンスルールに従ってグループ化されています。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、 AWS License Manager フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

AWS License Manager フレームワークの詳細は次のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
AWS License Manager	27	0	6

この AWS Audit Manager フレームワークのコントロールは、システムがライセンスルールに準拠しているかどうかを検証することを目的としたものではありません。また、ライセンス使用状況の監査合格を保証することはできません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

License Manager リンク

- AWS License Manager サービスページ
- AWS License Manager ユーザーガイド

ライセンスマネージャー API

このフレームワークについて、Audit Manager は、証拠を収集するために `GetLicenseManagerSummary` と呼ばれるカスタムアクティビティを使用します。`GetLicenseManagerSummary` アクティビティでは、次の 3 つのLicense Manager API を呼び出します。

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

返されたデータは証拠に変換され、評価の関連するコントロールにアタッチされます。

例: 2 つのライセンス製品 (SQL Service 2017 と Oracle Database Enterprise Edition) を使用しているとします。まず、`GetLicenseManagerSummary`アクティビティは ListLicenseConfigurations API を呼び出し、アカウント内のライセンス設定の詳細を提供します。次に、 ListUsageForLicenseConfigurationと を呼び出して、ライセンス設定ごとにコンテキストデータを追加しますListAssociationsForLicenseConfiguration。最後に、ライセンス設定データを証拠に変換し、フレームワークのそれぞれのコントロールにアタッチします (4.5 - SQL Server 2017 のカスタマーマネージドライセンスおよび 3.0.4 - Oracle Database Enterprise Edition のカスタマーマネージドライセンス)。フレームワークのどのコントロールによってもカバーされていないライセンス製品を使用している場合、そのライセンス設定データは、次のコントロールの証拠としてアタッチされます: 5.0 - 他のライセンスのカスタマーマネージドライセンス。

AWS 基本的なセキュリティのベストプラクティス

AWS Audit Manager は、 AWS Foundational Security Best Practices をサポートする構築済みの標準フレームワークを提供します。

トピック

AWS Foundational Security Best Practices 標準とは

AWS Foundational Security Best Practices 標準は、デプロイされたアカウントとリソースがセキュリティのベストプラクティスから逸脱したことを検出する一連のコントロールです。

この標準を使用して、すべての AWS アカウント およびワークロードを継続的に評価し、ベストプラクティスから逸脱している領域をすばやく特定できます。この標準は、組織のセキュリティ体制を改善し、維持する方法について、実践的かつ規範的なガイダンスを提供します。

コントロールには、複数の AWS のサービスからのベストプラクティスが含まれます。各コントロールには、適用先のセキュリティ機能を反映するカテゴリが割り当てられます。詳細については、AWS Security Hub ユーザーガイドの「コントロールのカテゴリ」を参照してください。

このフレームワークを使用する

AWS Foundational Security Best Practices フレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、 AWS Foundational Security Best Practices の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS アカウント および サービスのリソースの評価を開始します。これは、 AWS Foundational Security Best Practices フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の

受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

AWS Foundational Security Best Practices フレームワークの詳細は次のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
AWS 基本的なセキュリティのベストプラクティス	146	0	31

この AWS Audit Manager フレームワークのコントロールは、システムが AWS Foundational Security Best Practices に準拠しているかどうかを検証することを目的としたものではありません。さらに、 AWS 基本的なセキュリティのベストプラクティスの監査に合格することを保証することはできません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- AWS Security Hub ユーザーガイドのAWS 「基本的なセキュリティのベストプラクティス」標準
- 「AWS Security Hub ユーザーガイド」のコントロールカテゴリ

AWS 運用のベストプラクティス

AWS Audit Manager は、監査の準備に役立つ事前構築済みの AWS 運用のベストプラクティス (OBP) フレームワークを提供します。

このフレームワークは、 AWS Foundational Security Best Practices 標準のコントロールのサブセットを提供します。これらのコントロールは、デプロイされたアカウントとリソースがセキュリティのベストプラクティスから逸脱したことを検出するためのベースラインチェックとして機能します。

トピック

AWS Foundational Security Best Practices 標準とは

AWS Foundational Security Best Practices を使用して、 アカウントとワークロードを評価し、ベストプラクティスから逸脱している領域をすばやく特定できます。この標準は、組織のセキュリティ体制を改善し、維持する方法について、実践的かつ規範的なガイダンスを提供します。

コントロールには、複数の AWS のサービスからのベストプラクティスが含まれます。各コントロールには、適用先のセキュリティ機能を反映するカテゴリが割り当てられます。詳細については、AWS Security Hub ユーザーガイドの「コントロールのカテゴリ」を参照してください。

このフレームワークを使用する

AWS Operational Best Practices のフレームワークを使用して、このフレームワークに関連する監査の準備をすることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、 AWS 運用上のベストプラクティスの要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

AWS Operational Best Practices フレームワークの詳細は次のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
AWS 運用のベストプラクティス	0	51	20

このフレームワークのコントロールは、システムが AWS 運用上のベストプラクティスに準拠しているかどうかを検証することを目的としたものではありません。また、「 AWS 運用のベストプラクティス」監査に合格することを保証することはできません

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

このフレームワークには手動コントロールのみが含まれます。これらの手動コントロールは証拠を自動的に収集しません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- AWS Security Hub ユーザーガイドのAWS 「基本的なセキュリティのベストプラクティス」標準
- 「AWS Security Hub ユーザーガイド」のコントロールカテゴリ

AWS Well Architected Framework WAF v10

AWS Audit Manager は、 AWS Well-Architected Framework v10 をサポートする構築済みの標準フレームワークを提供します。

トピック

AWS Well-Architected フレームワークとは

AWS Well-Architected は、アプリケーションやワークロード向けに、安全で高性能、かつ、回復力のある効率的なインフラストラクチャを構築するのに役立てることができるフレームワークです。運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、コスト最適化、持続可能性の 6 つの柱に基づいて、AWS Well-Architected は、アーキテクチャを評価し、時間の経過にあわせてスケールできる設計を実装するための一貫したアプローチを提供します。

このフレームワークを使用する

AWS Well-Architected フレームワークを使用すると、監査の準備に役立ちます。Well-Architected フレームワークは、クラウドでワークロードを作成および実行するための主要な概念、設計原則、およびアーキテクチャのベストプラクティスについて説明しています。 AWS Well-Architected が基づいている 6 本の柱のうち、セキュリティの柱と信頼性の柱は、 AWS Audit Manager が構築済みのフレームワークとコントロールを提供する柱です。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、 AWS Well-Architected フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	44	290	6

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_AWS-Well-Architected-Framework-WAF-v10.zip ファイルをダウンロードします。

この フレームワークのコントロールは、システムがコンプライアンスに準拠しているかどうかを確認するためのものではない。また、監査に合格することを保証することはできません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- AWS Well-Architected
- AWS Well-Architected フレームワークのドキュメント

CCCS Medium Cloud Control

AWS Audit Manager は、カナダサイバーセキュリティセンター (CCCS) Medium Cloud Control をサポートする構築済みの標準フレームワークを提供します。

トピック

CCCS とは

CCCS は、サイバーセキュリティの専門家によるガイダンス、サービス、サポートを提供するカナダの権威あるソースです。CCCS はこの専門知識をカナダの政府、業界、一般市民に提供しています。クラウドサービスプロバイダーに対する厳格な評価は、カナダ全国で公共組織が情報に基づくクラウド調達の意思決定を行う際に頼りにされています。

「CCCS Medium Cloud Control Profile」は、2020 年 5 月にカナダ政府の「PROTECTED B / Medium Integrity / Medium Availability (PBMM)」プロファイルに取って代わりました。「CCCS Medium Cloud Security Control Profile」は、パブリッククラウドサービスを利用して機密性、完全性、可用性 (AIC) 要件が中程度の事業活動に対応する組織に適しています。AIC 要件が中程度のワークロードでは、不正な開示、変更、または事業活動で使用する情報やサービスへのアクセス喪失が、個人または組織に重大な損害を与えたり、個人の集団に限定的な損害を与えたりすることが十分に予想されます。これらの程度の損害には次のような例があります。

- 年間利益への重大な影響
- 主要アカウントの喪失
- 信用の喪失
- 明確なコンプライアンス違反
- 何百人、何千人もの人々のプライバシー侵害
- プログラムのパフォーマンスへの影響
- 精神障害や病気の原因になること
- サボタージュ
- 評判へのダメージ
- 個人の経済的困難

このフレームワークを使用する

CCCS Medium Cloud Control の AWS Audit Manager フレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、CCCS の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

フレームワークを開始点として使用して、Audit Manager の評価を作成し、CCCS Medium Cloud Control 監査に関連する証拠の収集を開始できます。評価では、監査の範囲 AWS アカウント に含める を指定できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、CCCS Medium Cloud Control フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
カナダサイバーセキュリティセンター (CCCS) Medium Cloud Control	258	95	175

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_AuditManagerConfigDataSourceMappings_CCCS-Medium-Cloud-Control.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが CCCS Medium Cloud Control の要件に準拠しているかどうかを検証することを目的としたものではありません。さら

に、CCCS audit. AWS Audit Manager does に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェックされません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

CIS AWS Benchmark v1.2.0

AWS Audit Manager には、Center for Internet Security (CIS) Amazon Web Services ()AWS Benchmark v1.2.0 をサポートする 2 つの構築済みフレームワークが用意されています。

> **Note**
>
> - v1.3.0 をサポートする Audit Manager フレームワークについては、「CIS AWS Benchmark v1.3.0」を参照してください。
> - v1.4.0 をサポートする Audit Manager フレームワークについては、「CIS AWS Benchmark v1.4.0」を参照してください。

トピック

CIS とは

CIS は CIS AWS Foundations Benchmark を開発した非営利団体です。このベンチマークは、 のセキュリティ設定のベストプラクティスのセットとして機能します AWS。これらの業界で認められて

いるベストプラクティスは、 で既に提供されている高レベルのセキュリティガイダンスを超えるものであり、明確で step-by-step 実装および評価の手順を提供します。

詳細については、 セキュリティブログの CIS AWS Foundations Benchmark AWS ブログ記事を参照してください。

CIS Benchmarks と CIS Controls の違い

CIS Benchmarks は、ベンダー製品に固有のセキュリティのベストプラクティスに関するガイドラインです。オペレーティングシステムからクラウドサービスやネットワークデバイスに至るまで、ベンチマークから適用される設定は、組織が使用する特定のシステムを保護します。CIS Controls は、組織が既知のサイバー攻撃ベクトルから保護するのに役立てるために従うべき基本的なベストプラクティスガイドラインです。

例

- CIS Benchmarks は規範的なものです。これらは通常、ベンダー製品で確認および設定できる特定の設定を参照します。

  例： CIS AWS Benchmark v1.2.0 - 「ルートユーザー」アカウントで MFA が有効になっていることを確認します。

  このレコメンデーションは、これを確認する方法と、 AWS 環境のルートアカウントでこれを設定する方法に関する規範的なガイダンスを提供します。
- CIS Controls は組織全体を対象としています。1 つのベンダー製品のみに特化したものではありません。

  例： CIS v7.1 - すべての管理アクセスに多要素認証を使用する

  このコントロールは、組織内で適用されるであろう内容を記述しています。実行しているシステムやワークロード (場所に関係なく) にそれを適用する方法については説明されていません。

このフレームワークを使用する

で CIS AWS Benchmark v1.2 フレームワークを使用すると AWS Audit Manager 、CIS 監査の準備に役立ちます。これらのフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

フレームワークを出発点として使用して Audit Manager の評価を作成し、監査に関連する証拠の収集を開始点できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。こ

れは CIS フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0、レベル 1	35	1	4
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0、レベル 1 および 2	48	1	4

> **Tip**
>
> これらの標準フレームワークのデータソースマッピングとして使用される AWS Config ルールのリストを確認するには、次のファイルをダウンロードします。
>
> 1. AuditManager_ConfigDataSourceMappingsCIS-AWS-Benchmark-v1.2.0、Level-1.zip
> 2. AuditManager_ConfigDataSourceMappingsCIS-AWS-Benchmark-v1.2.0、レベル 1 および 2.zip

これらのフレームワークのコントロールは、システムが CIS AWS Benchmark のベストプラクティスに準拠しているかどうかを検証することを目的としたものではありません。さらに、CIS audit. AWS Audit Manager does が手動証拠収集を必要とする手続き型コントロールを自動的にチェックすることを保証することはできません。

これらのフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

これらのフレームワークを使用するための前提条件

CIS AWS Benchmark v1.2 フレームワークの多くのコントロールは、データソースタイプ AWS Config として を使用します。これらのコントロールをサポートするには、Audit Manager を有効に AWS Config AWS リージョン した各 のすべてのアカウントで を有効にする必要があります。また、特定の AWS Config ルールが有効になっていること、およびこれらのルールが正しく設定されていることを確認する必要があります。

CIS AWS Foundations Benchmark v1.2 の正しい証拠を収集し、正確なコンプライアンスステータスをキャプチャするには、次の AWS Config ルールとパラメータが必要です。ルールを有効化または設定する方法については、「 AWS Config マネージドルールの使用」を参照してください。

必要な AWS Config ルール	必須パラメータ
ACCESS_KEYS_ROTATED	**maxAccessKeyAge** • ローテーションを行わない最大日数。 • タイプ: Int • デフォルト: (90 日) • コンプライアンス要件: 最大 90 日間
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	該当しない
CLOUD_TRAIL_ENCRYPTION_ENABLED	該当しない
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	該当しない
CMK_BACKING_KEY_ROTATION_ENABLED	該当しない
IAM_PASSWORD_POLICY	**MaxPasswordAge** (オプション) • パスワードが有効期限切れになるまでの日数。 • タイプ: int

必要な AWS Config ルール	必須パラメータ
	• デフォルト: 90 • コンプライアンス要件: 最大 90 日間
IAM_PASSWORD_POLICY	**MinimumPasswordLength** (オプション) • パスワードの最小長。 • タイプ: int • デフォルト: 14 • コンプライアンス要件: 14 文字以上
IAM_PASSWORD_POLICY	**PasswordReusePrevention** (オプション) • パスワードを再利用できるまでの他のパスワードの使用回数。 • タイプ: int • デフォルト: 24 • コンプライアンス要件: 再利用までに 24 個以上の他のパスワード
IAM_PASSWORD_POLICY	**RequireLowercaseCharacters** (オプション) • パスワードには少なくとも 1 つの小文字が必要です。 • 型: ブール値 • デフォルト: True • コンプライアンス要件: 少なくとも 1 文字の小文字
IAM_PASSWORD_POLICY	**RequireNumbers** (オプション) • パスワードには少なくとも 1 つの数字が必要です。 • 型: ブール値 • デフォルト: True • コンプライアンス要件: 少なくとも 1 つの数字

必要な AWS Config ルール	必須パラメータ
IAM_PASSWORD_POLICY	**RequireSymbols** (オプション) • パスワードには少なくとも 1 つの記号が必要です。 • 型: ブール値 • デフォルト: True • コンプライアンス要件: 少なくとも 1 つの記号
IAM_PASSWORD_POLICY	**RequireUppercaseCharacters** (オプション) • パスワードには少なくとも 1 つの大文字が必要です。 • 型: ブール値 • デフォルト: True • コンプライアンス要件: 少なくとも 1 文字の大文字
IAM_POLICY_IN_USE	**policyARN** • チェック対象の IAM ポリシー ARN。 • 型: 文字列 • コンプライアンス要件: でインシデントを管理するための IAM ロールを作成します AWS。 **policyUsageType** (オプション) • ポリシーを IAM ユーザー、グループ、またはロールにアタッチされることを期待するかどうかを指定します。 • タイプ: 文字列 • 有効な値: IAM_USER | IAM_GROUP | IAM_ROLE | ANY • デフォルト値: ANY • コンプライアンス要件: 作成した IAM ロールに信頼ポリシーをアタッチ
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	該当しない
IAM_ROOT_ACCESS_KEY_CHECK	該当しない

必要な AWS Config ルール	必須パラメータ
IAM_USER_NO_POLICIES_CHECK	該当しない
IAM_USER_UNUSED_CREDENTIALS_CHECK	**maxCredentialUsageAge** • 認証情報を使用できない最大日数。 • タイプ: Int • デフォルト: (90 日) • コンプライアンス要件: 90 日以上
INCOMING_SSH_DISABLED	該当しない
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	該当しない
MULTI_REGION_CLOUD_TRAIL_ENABLED	該当しない

必要な AWS Config ルール	必須パラメータ
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (オプション) • ブロックされた TCP ポート番号。 • タイプ: int • デフォルト: 20 • コンプライアンス要件: ブロックしたポートへの侵入をどのセキュリティグループにも許可しない **`blockedPort2`** (オプション) • ブロックされた TCP ポート番号。 • タイプ: int • デフォルト: 21 • コンプライアンス要件: ブロックしたポートへの侵入をどのセキュリティグループにも許可しない **`blockedPort3`** (オプション) • ブロックされた TCP ポート番号。 • タイプ: int • デフォルト: 3389 • コンプライアンス要件: ブロックしたポートへの侵入をどのセキュリティグループにも許可しない **`blockedPort4`** (オプション) • ブロックされた TCP ポート番号。 • タイプ: int • デフォルト: 3306 • コンプライアンス要件: ブロックしたポートへの侵入をどのセキュリティグループにも許可しない **`blockedPort5`** (オプション) • ブロックされた TCP ポート番号。 • タイプ: int • デフォルト: 4333

必要な AWS Config ルール	必須パラメータ
	• コンプライアンス要件: ブロックしたポートへの侵入をどのセキュリティグループにも許可しない
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	該当しない
ROOT_ACCOUNT_MFA_ENABLED	該当しない
S3_BUCKET_LOGGING_ENABLED	**targetBucket** （オプション） • サーバーアクセスログの保存先の S3 バケット。 • 型: 文字列 • コンプライアンス要件: ログ記録を有効にする **targetPrefix** （オプション） • サーバーアクセスログの保存先である S3 バケットのプレフィックス。 • 型: 文字列 • コンプライアンス要件: ログ記録用の CloudTrail S3 バケットを特定する
S3_BUCKET_PUBLIC_READ_PROHIBITED	該当しない
VPC_DEFAULT_SECURITY_GROUP_CLOSED	該当しない
VPC_FLOW_LOGS_ENABLED	**trafficType** （オプション） • フローログの `trafficType` 。 • 型: 文字列 • コンプライアンス要件: フローログを有効にする

次のステップ

これらのフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこれらのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- CIS AWS Foundations Benchmark v1.2.0
- CIS AWS Foundations Benchmark に関するブログ記事 (AWS セキュリティブログ)

CIS AWS Benchmark v1.3.0

AWS Audit Manager には、CIS AWS Benchmark v1.3 をサポートする 2 つの構築済み標準フレームワークが用意されています。

> **Note**
>
> - v1.2.0 をサポートする Audit Manager フレームワークについては、「CIS AWS Benchmark v1.2.0」を参照してください。
> - v1.4.0 をサポートする Audit Manager フレームワークについては、「CIS AWS Benchmark v1.4.0」を参照してください。

トピック

AWS CIS Benchmark とは

CIS は、 のセキュリティ設定のベストプラクティスのセットである CIS AWS Foundations Benchmark v1.3.0 を開発しました AWS。これらの業界で認められているベストプラクティスは、で既に提供されている高レベルのセキュリティガイダンスを超えるものであり、 AWS ユーザーに明確で step-by-step 実装および評価の手順を提供します。

詳細については、 セキュリティブログの CIS AWS Foundations Benchmark AWS ブログ記事を参照してください。

CIS AWS Benchmark v1.3.0 AWS のサービス は、基盤設定、テスト可能設定、アーキテクチャに依存しない設定に重点を置いた のサブセットのセキュリティオプションを設定するためのガイダンスを提供します。このドキュメントの対象となる特定の Amazon Web Services には次のようなものがあります。

- 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 (デフォルト)

CIS Benchmarks と CIS Controls の違い

CIS Benchmarks は、ベンダー製品に固有のセキュリティのベストプラクティスに関するガイドラインです。オペレーティングシステムからクラウドサービスやネットワークデバイスに至るまで、ベンチマークから適用される設定は、組織が使用するシステムを保護します。CIS Controls は、組織が既知のサイバー攻撃ベクトルから保護するのに役立てるために従うべき基本的なベストプラクティスガイドラインです。

例

- CIS Benchmarks は規範的なものです。これらは通常、ベンダー製品で確認および設定できる特定の設定を参照します。

  例： CIS AWS Benchmark v1.3.0 -「ルートユーザー」アカウントで MFA が有効になっていることを確認する

このレコメンデーションは、これを確認する方法と、 AWS 環境のルートアカウントでこれを設定する方法に関する規範的なガイダンスを提供します。

- CIS Controls は組織全体を対象としており、1 つのベンダー製品だけに固有のものではありません。

  例： CIS v7.1 - すべての管理アクセスに多要素認証を使用する

  このコントロールは、組織内で何を適用することが期待されるかを示しますが、(その場所にかかわらず) 実行しているシステムとワークロードにどのように適用する必要があるかは示しません。

これらのフレームワークを使用する

で CIS AWS Benchmark v1.3 フレームワークを使用すると AWS Audit Manager 、CIS 監査の準備に役立ちます。これらのフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

フレームワークを出発点として使用して Audit Manager の評価を作成し、監査に関連する証拠の収集を開始点できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは CIS フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0、レベル 1	36	1	5
Center for Internet Security (CIS) Amazon Web Services	54	1	5

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
(AWS) Benchmark v1.3.0、レベル 1 および 2			

> **Tip**
>
> これらの標準フレームワークのデータソースマッピングとして使用される AWS Config ルールのリストを確認するには、次のファイルをダウンロードします。
>
> 1. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.3.0、Level-1.zip
> 2. AuditManager_ConfigDataSourceMappings_CIS-AWS-Benchmark-v1.3.0、Level-1-and-2.zip

これらのフレームワークのコントロールは、システムが CIS AWS Benchmark のベストプラクティスに準拠しているかどうかを検証することを目的としたものではありません。さらに、CIS audit. AWS Audit Manager does が手動証拠収集を必要とする手続き型コントロールを自動的にチェックすることを保証することはできません。

これらのフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

これらのフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこれらのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- CIS AWS Foundations Benchmark に関するブログ記事 (AWS セキュリティブログ)

CIS AWS Benchmark v1.4.0

AWS Audit Manager は、Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 をサポートする 2 つの構築済み標準フレームワークを提供します。

> **Note**
>
> - v1.2.0 をサポートする Audit Manager フレームワークについては、「CIS AWS Benchmark v1.2.0」を参照してください。
> - v1.3.0 をサポートする Audit Manager フレームワークについては、「CIS AWS Benchmark v1.3.0」を参照してください。

トピック

CIS AWS Benchmark とは

CIS AWS Benchmark v1.4.0 は、Amazon Web Services のサブセットのセキュリティオプションを設定するための規範的なガイダンスを提供します。基本的な設定、テスト可能な設定、およびアーキテクチャに依存しない設定に重点を置いたものです。このドキュメントの対象となる特定の Amazon Web Services には次のようなものがあります。

- 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

CIS Benchmarks と CIS Controls の違い

CIS Benchmarks は、ベンダー製品に固有のセキュリティのベストプラクティスに関するガイドラインです。オペレーティングシステムから、クラウドサービスやネットワークデバイスに至るまで、ベンチマークから適用される設定は、使用されているシステムを保護します。CIS Controls は、組織が既知のサイバー攻撃ベクトルから保護するのに役立てるために従うべき基本的なベストプラクティスガイドラインです。

例

- CIS Benchmarks は規範的なものです。これらは通常、ベンダー製品で確認および設定できる特定の設定を参照します。

  例： CIS AWS Benchmark v1.3.0 -「ルートユーザー」アカウントで MFA が有効になっていることを確認する

  このレコメンデーションは、これを確認する方法と、 AWS 環境のルートアカウントでこれを設定する方法に関する規範的なガイダンスを提供します。
- CIS Controls は組織全体を対象としており、1 つのベンダー製品だけに固有のものではありません。

  例： CIS v7.1 - すべての管理アクセスに多要素認証を使用する

  このコントロールは、組織内で適用されるであろう内容を記述しています。ただし、実行しているシステムやワークロード (場所に関係なく) にそれを適用する必要がある方法については説明されていません。

監査の準備をサポートするためにこれらのフレームワークを使用する

で CIS AWS Benchmark v1.4.0 フレームワークを使用すると AWS Audit Manager 、CIS 監査の準備に役立ちます。これらのフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

フレームワークを出発点として使用して Audit Manager の評価を作成し、監査に関連する証拠の収集を開始点できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは CIS フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証

拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0、レベル 1	37	1	5
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0、レベル 1 および 2	57	1	5

> **Tip**
>
> これらの標準フレームワークのデータソースマッピングとして使用される AWS Config ルールのリストを確認するには、次のファイルをダウンロードします。
>
> 1. AuditManager_ConfigDataSourceMappingsCIS-AWS-Benchmark-v1.4.0、Level-1.zip
> 2. AuditManager_ConfigDataSourceMappingsCIS-AWS-Benchmark-v1.4.0、レベル-1-および-2.zip

これらのフレームワークのコントロールは、システムが CIS AWS Benchmark v1.4.0 に準拠しているかどうかを検証することを目的としたものではありません。さらに、CIS audit. AWS Audit Manager does が手動証拠収集を必要とする手続き型コントロールを自動的にチェックすることを保証することはできません。

これらのフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

これらのフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこれらのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- Center for Internet Security の CIS ベンチマーク
- CIS AWS Foundations Benchmark に関するブログ記事 (AWS セキュリティブログ)

CIS Controls v7.1、IG1

AWS Audit Manager は、Center for Internet Security (CIS) v7.1 Implementation Group 1 をサポートする構築済みの標準フレームワークを提供します。

> **Note**
>
> CIS v8 IG1and、この標準をサポートする AWS Audit Manager フレームワークについては、「」を参照してくださいCIS Critical Security Controls バージョン 8.0、IG1 。

トピック

CIS Controls とは？

CIS Controls は、一連のベストプラクティスをまとめて形成する、優先順位の高い defense-in-depth 一連のアクションです。これらのベストプラクティスは、システムおよびネットワークに対する最も一般的な攻撃を緩和します。Implementation Group 1 は通常、Sub-Controls の実装に利用できるリソースとサイバーセキュリティの専門知識を十分に備えていない組織向けに定義されています。

CIS Controls と CIS Benchmarks の違い

CIS Controls は、組織が既知のサイバー攻撃ベクトルから保護するために従うことができる基本的なベストプラクティスのガイドラインです。CIS Benchmarks は、ベンダー製品に固有のセキュリティのベストプラクティスに関するガイドラインです。オペレーティングシステムから、クラウドサービスやネットワークデバイスに至るまで、Benchmark から適用される設定は、使用されているシステムを保護します。

例

- CIS Benchmarks は規範的なものです。これらは通常、ベンダー製品で確認および設定できる特定の設定を参照します。
  - 例: CIS AWS Benchmark v1.2.0 -「ルートユーザー」アカウントで MFA が有効になっていることを確認します
  - このレコメンデーションは、これを確認する方法と、 AWS 環境のルートアカウントでこれを設定する方法に関する規範的なガイダンスを提供します。
- CIS Controls は組織全体を対象としており、1 つのベンダー製品だけに固有のものではありません。
  - 例: CIS v7.1 - すべての管理アクセスに多要素認証を使用する
  - このコントロールは、組織内で適用されるであろう内容を記述しています。ただし、(その場所にかかわらず) 実行しているシステムとワークロードにどのように適用する必要があるかについて示すものではありません。

このフレームワークを使用する

CIS Controls v7.1 IG1 フレームワークを使用すると、監査の準備をすることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、CIS の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは「CIS Controls v7.1 IG1」フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクス

ポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

「CIS Controls v7.1 IG1」フレームワークの詳細は次のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Center for Internet Security (CIS) v7.1、IG1	31	12	18

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_CIS-v7.1-IG1.zip ファイルをダウンロードします。

このフレームワークのコントロールは、システムが CIS Controls に準拠しているかどうかを確認することを目的としたものではありません。さらに、これらのコントロールは、CIS 評価に合格することを保証することはできません。 AWS Audit Manager は、手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- CIS Controls v7.1 IG1

CIS Critical Security Controls バージョン 8.0、IG1

AWS Audit Manager は、CIS の「Critical Security Controls」バージョン 8.0、「実装グループ 1」をサポートする構築済みの標準フレームワークを提供します。

> **Note**
>
> CIS v7.1、IG1、およびこの標準をサポートする AWS Audit Manager フレームワークの詳細については、「」を参照してくださいCIS Controls v7.1、IG1。

トピック

CIS Controls とは？

CIS Critical Security Controls (CIS Controls) は、システムやネットワークに対する最も一般的なサイバー攻撃を軽減するための優先順位の高い保護手段です。複数の法律、規制、ポリシーのフレームワークにマッピングされ、参照されています。CIS Controls v8 は、最新のシステムやソフトウェアに対応するために強化されています。クラウドベースのコンピューティング、仮想化、モビリティ、外部委託 work-from-home、攻撃者の戦術の変化が、この更新のきっかけとなりました。このアップデートは、企業が完全なクラウド環境やハイブリッド環境に移行する際のセキュリティをサポートします。

CIS Controls と CIS Benchmarks の違い

CIS Controls は、組織が既知のサイバー攻撃ベクトルから保護するために従うことができる基本的なベストプラクティスのガイドラインです。CIS Benchmarks は、ベンダー製品に固有のセキュリティのベストプラクティスに関するガイドラインです。オペレーティングシステムから、クラウドサービスやネットワークデバイスに至るまで、Benchmark から適用される設定は、使用されているシステムを保護します。

例

- CIS Benchmarks は規範的なものです。これらは通常、ベンダー製品で確認および設定できる特定の設定を参照します。
  - 例: CIS AWS Benchmark v1.2.0 - 「ルートユーザー」アカウントで MFA が有効になっていることを確認する
  - このレコメンデーションは、これを確認する方法と、 AWS 環境のルートアカウントでこれを設定する方法に関する規範的なガイダンスを提供します。
- CIS Controls は組織全体を対象としており、1 つのベンダー製品だけに固有のものではありません。
  - 例: CIS v7.1 - すべての管理アクセスに多要素認証を使用する
  - このコントロールは、組織内で適用されるであろう内容を記述しています。ただし、(その場所にかかわらず) 実行しているシステムとワークロードにどのように適用する必要があるかについて示すものではありません。

このフレームワークを使用する

CIS v8 IG1 フレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、CIS の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、CIS v8 フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
CIS Critical Security Controls バージョン 8.0 (CIS v8.0)、IG1	38	18	15

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_CIS-v8.0-IG1.zip ファイルをダウンロードします。

このフレームワークのコントロールは、システムが CIS Controls に準拠しているかどうかを確認することを目的としたものではありません。さらに、これらのコントロールは、CIS 評価に合格することを保証することはできません。 AWS Audit Manager は、手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- CIS Controls v8

FedRAMP セキュリティベースラインコントロール r4

AWS Audit Manager は、Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4 をサポートする構築済みの標準フレームワークを提供します。

トピック

FedRAMP とは

FedRAMP は 2011 年に設立されました。これは、米国連邦政府がクラウドサービスを採用し使用するための、費用対効果に優れたリスクベースのアプローチです。FedRAMP は、連邦政府情報のセキュリティと保護に重点を置きつつ、連邦政府機関が最新のクラウドテクノロジーを使用できるようにします。

「FedRAMP Moderate Baseline」コントロールの詳細については、「FedRAMP Moderate Security Test Case Procedures Template」を参照してください。

このフレームワークを使用する

FedRAMP r4 フレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、FedRAMP r4 の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これはフレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

「FedRAMP Moderate Baseline」フレームワークの詳細は次のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4、Moderate	234	91	17

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_FedRAMP-Security-Baseline-Controls-r4-Moderate .zip ファイルをダウンロードします。

このフレームワークのコントロールは、システムが FedRAMP r4 に準拠しているかどうかを検証することを目的としたものではありません。さらに、これらのコントロールは、FedRAMP 評価に合格することを保証することはできません。 AWS Audit Manager は、手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- AWS FedRAMP のコンプライアンスページ
- AWS FedRAMP ブログ記事

GDPR 2016

AWS Audit Manager は、一般データ保護規則 (GDPR) 2016 をサポートする構築済みの標準フレームワークを提供します。

このフレームワークには手動コントロールのみが含まれます。これらの手動コントロールは、証拠を自動的に収集しません。ただし、GDPR に基づく一部のコントロールの証拠収集を自動化する場合は、Audit Manager のカスタムコントロール機能を使用できます。詳細については、「このフレームワークを使用する」を参照してください。

トピック

GDPR とは

GDPR は、2018 年 5 月 25 日に施行された欧州のプライバシー法です。GDPR は、指令 95/46/EC (Directive 95/46/EC) としても知られる EU データ保護指令 (EU Data Protection Directive) に代わるものです。欧州連合 (EU) 全体のデータ保護関連法令を調和させることを目的としています。そのために、全 EU 加盟国において、拘束力のある 1 つのデータ保護関連法令を適用します。

GDPR は、EU 内に設立されたすべての組織、および EU 内に設立されたかどうかにかかわらず、EU 内のデータ主体に対する商品またはサービスの提供、または EU 内で行われる行動のモニタリングに関連して、EU データ主体の個人データを処理する組織に適用されます。個人データとは、識別された、または識別可能な自然人に関する情報です。

GDPR フレームワークは、Audit Manager のフレームワークライブラリページにあります。詳細については、「General Data Protection Regulation (GDPR) Center」を参照してください。

このフレームワークを使用する

Audit Manager で GDPR 2016 フレームワークを使用して、監査の準備に役立てることができます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
一般データ保護規則 (GDPR) 2016	0	378	10

GDPR 2016 フレームワークは、Audit Manager の の標準フレームワークタブフレームワークライブラリを使用して でフレームワークを管理する AWS Audit Managerにあります。この標準フレームワークには手動コントロールのみが含まれています。

> **Note**
>
> GDPR 向けの証拠収集を自動化する場合は、Audit Manager を使用して、GDPR 向けの独自のカスタムコントロールを作成できます。次の表は、カスタムコントロールの GDPR 要件にマッピングできる AWS データソースに関する推奨事項を示しています。以下のデータソースの一部は複数のコントロールにマッピングされていますが、各リソース評価に対して要求されるのは 1 回だけであることに注意してください。
> 以下の推奨事項では、データソース AWS Security Hub として AWS Config と を使用しています。これらのデータソースから証拠を正常に収集するには、「」の手順に従って と を有効に AWS Config して設定 AWS Security Hubしてください AWS アカウント。この方法で両方のサービスをセットアップすると、Audit Manager は、指定された AWS Config ルールまたは Security Hub コントロールの評価が行われるたびに証拠を収集します。

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 25 条 Data protection by design and by default (データ保護バイデ	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する • AWS CloudTrail バケットがパブリックではない

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
ザインおよびデータ保護バイデフォルト).1		• `Allow:*:*` を含むすべてのポリシーを表示し、それらのポリシーを使用しているすべてのプリンシパルとサービスをリストします コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1)

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• 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) • 3.14 (CloudWatch.14) • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 25 条 Data protection by design and by default (データ保護バイデザインおよびデータ保護バイデフォルト).2	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する • AWS CloudTrail バケットがパブリックではない • `Allow:*:*` を含むすべてのポリシーを表示し、それらのポリシーを使用しているすべてのプリンシパルとサービスをリストします コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17)

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• 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)

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 25 条 Data protection by design and by default (データ保護バイデザインおよびデータ保護バイデフォルト).3	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する • AWS CloudTrail バケットがパブリックではない • `Allow:*:*` を含むすべてのポリシーを表示し、それらのポリシーを使用しているすべてのプリンシパルとサービスをリストします コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • 1.1 (CloudWatch.1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17)

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• 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)

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 30 条 Records of processing activities (取扱活動の記録) .1	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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 データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 30 条 Records of processing activities (取扱活動の記録) .2	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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 データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 30 条 Records of processing activities (取扱活動の記録) .3	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する • AWS CloudTrail バケットがパブリックではない • `Allow:*:*` を含むすべてのポリシーを表示し、それらのポリシーを使用しているすべてのプリンシパルとサービスをリストします コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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 データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 30 条 Records of processing activities (取扱活動の記録) .4	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する • AWS CloudTrail バケットがパブリックではない • `Allow:*:*` を含むすべてのポリシーを表示し、それらのポリシーを使用しているすべてのプリンシパルとサービスをリストします コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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 データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 30 条 Records of processing activities (取扱活動の記録) .5	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • 一定期間におけるすべてのルートアカウントイベントを表示する コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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 データソースタイプ AWS Security Hub として を選択し、データソースマッピングとして次の Security Hub コントロールを選択します。 • Config.1

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 32 条 Security of processing (取扱いの安全性) .1	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • すべてのサービスの保管中のデータ暗号化を表示する • すべてのサービスの転送中のデータ暗号化を表示する • Amazon S3 向けに MFA 削除が有効になっています • Amazon Inspector のすべてのスキャン • Amazon Inspector が有効になっていないすべてのインスタンスを表示する • HTTPS (SSL) でリッスンしているすべてのロードバランサーを表示する • AWS CloudTrail 保管時の暗号化 • すべての変更とコメントされたすべての設定 AWS Config を表示するための Amazon CloudWatch アラート • すべてのルートアクティビティ コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ENCRYPTED_VOLUMES • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 32 条 Security of processing (取扱いの安全性) .2	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • すべてのサービスの保管中のデータ暗号化を表示する • すべてのサービスの転送中のデータ暗号化を表示する • Amazon S3 向けに MFA 削除が有効になっています • Amazon Inspector のすべてのスキャン • Amazon Inspector が有効になっていないすべてのインスタンスを表示する • HTTPS (SSL) でリッスンしているすべてのロードバランサーを表示する • AWS CloudTrail 保管時の暗号化 • すべての変更とコメントされたすべての設定 AWS Config を表示するための Amazon CloudWatch アラート • すべてのルートアクティビティ コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ENCRYPTED_VOLUMES • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 32 条 Security of processing (取扱いの安全性) .3	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • すべてのサービスの保管中のデータ暗号化を表示する • すべてのサービスの転送中のデータ暗号化を表示する • Amazon S3 向けに MFA 削除が有効になっています • Amazon Inspector のすべてのスキャン • Amazon Inspector が有効になっていないすべてのインスタンスを表示する • HTTPS (SSL) でリッスンしているすべてのロードバランサーを表示する • AWS CloudTrail 保管時の暗号化 • すべての変更とコメントされたすべての設定 AWS Config を表示するための Amazon CloudWatch アラート • すべてのルートアクティビティ コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ENCRYPTED_VOLUMES • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
第 32 条 Security of processing (取扱いの安全性) .4	第 4 章 - コントローラーとプロセッサ	この GDPR コントロールをサポートするカスタムコントロールを で作成できます。 AWS Audit Manager コントロールの詳細を指定するときは、[Testing information] (テスト情報) で次のように入力します。 • すべてのサービスの保管中のデータ暗号化を表示する • すべてのサービスの転送中のデータ暗号化を表示する • Amazon S3 向けに MFA 削除が有効になっています • Amazon Inspector のすべてのスキャン • Amazon Inspector が有効になっていないすべてのインスタンスを表示する • HTTPS (SSL) でリッスンしているすべてのロードバランサーを表示する • AWS CloudTrail 保管時の暗号化 • すべての変更とコメントされたすべての設定 AWS Config を表示するための Amazon CloudWatch アラート • すべてのルートアクティビティ コントロールデータソースを設定するときは、以下のすべてをデータソースとして含めることをお勧めします。 データソースタイプ AWS Config として を選択し、データソースマッピングとして次の AWS Config マネージドルールを選択します。 • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ENCRYPTED_VOLUMES • 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

コントロール名	コントロールセット	推奨されるコントロールのデータソースマッピング
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

GDPR 用の新しいカスタムコントロールを作成したら、それらをカスタム GDPR フレームワークに追加できます。その後、カスタム GDPR フレームワークから評価を作成できます。これにより、Audit Manager は追加したカスタムコントロールの証拠を自動的に収集できます。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- 一般データ保護規則 (GDPR) センター
- AWS GDPR ブログ記事

グラムリーチブライリー法 (Gramm-Leach-Bliley Act)

AWS Audit Manager は、グラムリーチブライリー法 (GLBA) をサポートする構築済みのフレームワークを提供します。

トピック

- GLBA とは
- このフレームワークを使用する
- 次のステップ

GLBA とは

GLBA (または GLB 法) は、1999 年金融サービス近代化法とも呼ばれ、金融機関が個人の個人情報を処理する方法をコントロールするために米国で制定された連邦法です。同法は 3 つのセクションで構成されます。1 つ目は、私的財務情報の収集および開示を規制する財務プライバシールール (Financial Privacy Rule) です。2 つ目は、金融機関がそのような情報を保護するためのセキュリティプログラムを実装する必要があることを規定するセーフガードルール (Safeguards Rule) です。3 つ目は、プリテキスティング (身元や身分をなりすまして私的情報にアクセスすること) の慣行を禁止するプリテキスティングに関する規定です。また、同法では、顧客の情報の共有に関する慣行を説明するプライバシー通知書を顧客に提供するよう金融機関に義務付けています。

このフレームワークを使用する

GLBA 2016 フレームワークを使用して、監査の準備に役立てることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、GLBA の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

GLBA フレームワークを出発点として使用して Audit Manager の評価を作成し、GLBA の監査に関連する証拠の収集を開始できます。評価では、監査の範囲 AWS アカウント に含める を指定できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは GLBA フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
グラムリーチブライリー法 (GLBA、Gramm-Leach-Bliley Act)	0	120	16

この AWS Audit Manager フレームワークのコントロールは、システムが GLBA 標準に準拠しているかどうかを検証することを目的としたものではありません。さらに、GLBA 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

GLBA フレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

タイトル 21 CFR Part 11

AWS Audit Manager は、連邦規則集 (CFR) パート 11、電子記録のタイトル 21、電子署名 - スコープ、および 2023 年 5 月 24 日のアプリケーションをサポートする構築済みの標準フレームワークを提供します。

トピック

CFR Part 11 のタイトル 21 とは

GxP は、食品や医療製品を製造するライフサイエンス業界の組織に適用される規制およびガイドラインです。これに該当する医療製品には、医薬品、医療機器、および医療ソフトウェアアプリケーションが含まれます。GxP 要件の全体的な趣旨は、食品および医療製品が消費者にとって確実に安全なものであるようにすることにあります。また、製品関連の安全性に関する決定を行うために使用されるデータの完全性を確保することもその趣旨に含まれています。

米国では、GxP 規制は米国食品医薬品局 (FDA) によって適用され、連邦規則 (21 CFR) のタイトル 21 に含まれています。21 CFR 内では、パート 11 には、GxP で規制された活動をサポートするために、電子記録と電子署名を作成、変更、維持、アーカイブ、取得、または配布するコンピュータシステムの要件が含まれています。Part 11 は、FDA 規制のライフサイエンス組織による新しい情報テクノロジーの導入を許可すると同時に、電子 GxP データが信頼性と信頼性を確保するフレームワークを提供するために作成されました。

AWS Cloud for GxP システムを使用するための包括的なアプローチについては、「GxP Systems での AWS 製品の使用に関する考慮事項 GxP」ホワイトペーパーを参照してください。

このフレームワークを使用する

Title 21 CFR Part 11 フレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、CFR の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、Title 21 CFR Part 11 フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
タイトル 21 連邦規則 (CFR) Part 11、電子記録、電子署名 - スコープとアプリケーション 2023 年 5 月 24 日	17	8	2

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_Title-21-CFR-Part-11.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが GxP 規制に準拠しているかどうかを検証することを目的としたものではありません。さらに、これらのコントロールは、監査に合格することを保証することはできません。 AWS Audit Manager は、手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- AWS GxP のコンプライアンスページ
- GxP システムで AWS 製品を使用する際の考慮事項

EU GMP Annex 11、v1

AWS Audit Manager は、 EudraLex - 欧州連合 (EU) の医薬品を管理する規則 - ボリューム 4: 適正製造規範 (GMP) 人間および獣医学用の医薬品 - Annex 11 をサポートする構築済みのフレームワークを提供します。

トピック

- EU GMP Annex 11 とは
- このフレームワークを使用する

- 次のステップ

EU GMP Annex 11 とは

EU GMP Annex 11 フレームワークは、米国の Title 21 CFR Part 11 フレームワークに相当する欧州のフレームワークです。この Annex はGood Manufacturing Practices (GMP) によって規制される活動の一部として使用されるすべての形態のコンピュータ化されたシステムに適用されます。コンピュータ化されたシステムは、特定の機能を一緒に実行する一連のソフトウェアおよびハードウェアコンポーネントです。アプリケーションを検証し、IT インフラストラクチャが特定の要件を満たすようにする必要があります。コンピュータ化されたシステムが手動操作に取って代わる場合、その結果として、製品の品質、プロセスの制御、または品質保証の低下が生じないようにする必要があります。プロセスの全体的なリスクが増加しないようにする必要があります。

Annex 11 は、欧州の GMP ガイドラインの一部であり、製薬業界の組織によって使用されるコンピュータ化されたシステムについての付託事項を定義しています。Annex 11 は、欧州の規制当局が医薬品および医療機器に関連するコンピュータ化されたシステムの要件を確立できるようにするチェックリストとして機能します。欧州委員会によって設定されたガイドラインは、FDA (Title 21 CFR Part 11) とはそれほど遠くありません。Annex 11 は、電子記録および電子署名の管理方法の基準を定義しています。

このフレームワークを使用する

EU GMP Annex 11 フレームワークを使用して、監査の準備に役立てることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、EU GMP 要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、EU GMP Annex 11 フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
EudraLex - 欧州連合 (EU) の医薬品を管理する規則 - 第 4 部: 適正製造規範 (GMP) 人間および獣医学用の医薬品 - Annex 11	15	17	3

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_EudraLex-GMP-Volume-4-Annex-11.zip ファイルをダウンロードします。

このフレームワークのコントロールは、システムが EU GMP Annex 11 の要件に準拠しているかどうかを検証することを目的としたものではありません。さらに、EU GMP 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

HIPAA セキュリティルール: 2003 年 2 月

AWS Audit Manager は、医療保険の相互運用性と説明責任に関する法律 (HIPAA) セキュリティルール: 2003 年 2 月をサポートする構築済みの標準フレームワークを提供します。

> **Note**
>
> 「HIPAA Final Omnibus Security Rule 2013」およびこの基準をサポートする Audit Manager フレームワークについては、「HIPAA オムニバスの最終ルール」を参照してください。

トピック

HIPAA と「HIPAA セキュリティルール 2003」とは？

HIPAA は、米国のワーカーが転職や失業しても健康保険の適用範囲を維持できるようにする法律です。この法律はまた、情報共有の改善を通じて、米国のヘルスケアシステムの効率と質を改善するために健康医療電子記録を奨励することも目的としています。

健康医療電子記録の使用を増やすことに加えて、HIPAA には、保護対象保健情報 (PHI、protected health information) のセキュリティとプライバシーを保護するための規定が含まれています。PHI には、個人の識別が可能な健康および健康関連のデータが非常に幅広く含まれます。これには、保険および請求情報、診断データ、臨床ケアデータ、および画像や検査結果などの検査結果が含まれます。

2003 年 2 月、米国保健福祉省が「セキュリティルール」の正式版を発表しました。このルールは、電子的に保護された医療情報の機密性、完全性、可用性を保護するための国家基準を定めています。

HIPAA のルールは、対象主体に適用されます。これらには、病院、医療サービスプロバイダー、事業者提供医療制度、研究施設、および患者と患者データを直接扱う保険会社が含まれます。PHI を保護するための HIPAA 要件は、ビジネスアソシエイトにも適用されます。

HIPAA および HITECH が健康情報を保護する方法の詳細については、米国保健福祉省の健康情報のプライバシーのウェブページを参照してください。

ますます多くの医療プロバイダー、支払者、IT プロフェッショナルが、ユーティリティベースのクラウドサービスを使用して AWS 保護医療情報 (PHI) を処理、保存、送信しています。HIPAA の対象となる AWS エンティティとそのビジネスアソシエイトは、保護医療情報を処理、維持、保存するために安全な AWS 環境を使用できます。

ヘルス情報の処理と保存 AWS に を使用する方法については、Amazon Web Services ホワイトペーパーの「Architecting for HIPAA Security and Compliance」を参照してください。

このフレームワークを使用する

HIPAA セキュリティルール 2003 フレームワークを使用して、監査の準備に役立てることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、HIPAA 要件に従ってコントロール セットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは HIPAA フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
医療保険の相互運用性と説明責任に関する法律 (HIPAA) セキュリティルール: 2003 年 2 月	45	40	5

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_HIPAA-Security-Rule-Feb-2003.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが HIPAA 標準に準拠しているかどうかを検証することを目的としたものではありません。さらに、HIPAA 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- 米国保健福祉省による「医療情報のプライバシー」
- 米国保健福祉省による「セキュリティルール」
- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS HIPAA のコンプライアンスページ

HIPAA オムニバスの最終ルール

AWS Audit Manager は、医療保険の相互運用性と説明責任に関する法律 (HIPAA) オムニバス最終規則をサポートする構築済みの標準フレームワークを提供します。

> **Note**
>
> HIPAA セキュリティルール 2003 と、この標準をサポートする AWS Audit Manager フレームワークの詳細については、「」を参照してくださいHIPAA セキュリティルール: 2003 年 2 月。

トピック

- HIPAA と「HIPAA Final Omnibus Security Rule」とは？

HIPAA と「HIPAA Final Omnibus Security Rule」とは？

HIPPA は、米国のワーカーが転職または失業したときに健康保険の適用範囲を維持するのに役立つ法律です。この法律はまた、情報共有の改善を通じて、米国のヘルスケアシステムの効率と質を改善するために健康医療電子記録を奨励することも目的としています。

健康医療電子記録の使用を増やすことに加えて、HIPAA には、保護対象保健情報 (PHI、protected health information) のセキュリティとプライバシーを保護するための規定が含まれています。PHI には、個人の識別が可能な健康および健康関連のデータが非常に幅広く含まれます。これには、保険および請求情報、診断データ、臨床ケアデータ、および画像や検査結果などの検査結果が含まれます。

2013 年に発効した「HIPAA Final Omnibus Security Rule」では、これまでに可決されたすべてのルールに多数の更新が加えられています。データ共有における機密性とセキュリティを強化することを目的として、セキュリティ、プライバシー、侵害通知、および施行規則が変更さされました。

HIPAA のルールは、対象主体に適用されます。これらには、病院、医療サービスプロバイダー、事業者提供医療制度、研究施設、および患者と患者データを直接扱う保険会社が含まれます。包括的更新の一環として、対象主体に適用される HIPAA 規則の多くが取引先にも適用されるようになりました。

HIPAA および HITECH が健康情報を保護する方法の詳細については、米国保健福祉省の健康情報のプライバシーのウェブページを参照してください。

ますます多くの医療プロバイダー、支払者、IT プロフェッショナルが、ユーティリティベースのクラウドサービスを使用して AWS 保護医療情報 (PHI) を処理、保存、送信しています。HIPAA の対象となる AWS エンティティとそのビジネスアソシエイトは、保護医療情報を処理、維持、保存するために安全な AWS 環境を使用できます。ヘルス情報の処理と保存 AWS に を使用する方法については、Amazon Web Services の Architecting for HIPAA Security and Compliance ホワイトペーパーを参照してください。

このフレームワークを使用する

HIPAA オムニバス最終ルールフレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれていま

す。これらのコントロールは、HIPAA 要件に従ってコントロール セットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは HIPAA フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
医療保険の相互運用性と説明責任に関する法律 (HIPAA) オムニバス最終規則	45	29	5

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_HIPAA-Omnibus-Final-Rule.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが HIPAA 標準に準拠しているかどうかを検証することを目的としたものではありません。さらに、HIPAA 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- 米国保健福祉省による「医療情報のプライバシー」
- 米国保健福祉省による「Omnibus HIPAA Rulemaking」
- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS HIPAA のコンプライアンスページ

ISO/IEC 27001:2013 附属書 A

AWS Audit Manager は、国際標準化機構 (ISO)/国際電気標準会議 (IEC) 27001:2013 Annex A をサポートする構築済みの標準フレームワークを提供します。

トピック

ISO/IEC 27001:2013 附属書 A とは？

国際電気標準会議 (IEC) と国際標準化機構 (ISO) はどちらも独立した非政府組織であり、 not-for-profit完全に合意に基づく国際規格を開発および公開しています。

「ISO/IEC 27001:2013 附属書 A」は、ISO/IEC 27002 ベストプラクティスガイダンスに従ったセキュリティ管理のベストプラクティスと包括的なセキュリティ管理を規定するセキュリティ管理基準です。この国際規格は、組織における情報セキュリティ管理システムの確立、実装、維持、および継

続的な改善方法に関する要件を規定しています。これらの基準には、各組織のニーズに合わせた情報セキュリティリスクの評価と処理に関する要件が含まれています。この国際規格の要件は一般的なもので、種類、規模、性質にかかわらず、すべての組織に適用されることを意図しています。

このフレームワークを使用する

ISO/IEC 27001:2013 Annex A の AWS Audit Manager フレームワークを使用して、監査の準備に役立てることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、「ISO/IEC 27001:2013 附属書 A」の要件に従ってコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として Audit Manager の評価を作成し、「ISO/IEC 27001:2013 附属書 A」の監査に関連する証拠の収集を開始できます。評価では、監査の範囲 AWS アカウント に含めるを指定できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは「ISO/IEC 27001:2013 附属書 A」フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
国際標準化機構 (ISO)/国際電気標準会議 (IEC) 27001:2013 附属書 A	61	53	35

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_ISO-IEC-270012013-Annex-A.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムがこの国際標準に準拠しているかどうかを検証することを目的としたものではありません。さらに、ISO/IEC 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

SO/IEC 27001:2013 Annex A フレームワークは、Audit Manager の フレームワークライブラリを使用して でフレームワークを管理する AWS Audit Manager の [標準フレームワーク] タブ にあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- この国際規格の詳細については、ANSI Webstore で「ISO/IEC 27001:2013」を参照してください。

NIST SP 800-53 Rev 5

AWS Audit Manager は、NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations をサポートする構築済みのフレームワークを提供します。

> **Note**
>
> - NIST SP 800-171 をサポートする Audit Manager フレームワークの詳細については、「」を参照してくださいNIST SP 800-171 Rev 2。
> - NIST CSF をサポートする Audit Manager フレームワークの詳細については、「」を参照してくださいNIST Cybersecurity Framework v1.1。

トピック

- NIST SP 800-53 とは

NIST SP 800-53 とは

米国国立標準技術研究所 (NIST) は、1901 年に設立され、現在は米国商務省の一機関となっています。NIST は、米国で最も古い物理科学研究所の 1 つです。米国議会は、当時は二流だった計測インフラを改善するためにこの機関を設立しました。このインフラは、英国やドイツなど、他の経済大国に遅れをとっていた米国の産業競争力にとって大きな課題でした。

NIST SP 800-53 のセキュリティコントロールは、一般的に米国の連邦情報システムに適用されます。これらは通常、正式な評価および承認プロセスを経る必要のあるシステムです。このプロセスにより、情報と情報システムの機密性、完全性、可用性を十分に保護できます。セキュリティカテゴリー、システムの影響レベル (低、中、高)、リスク判断に基づいた保護です。セキュリティコントロールは NIST SP 800-53 セキュリティコントロールカタログから選択され、システムはそれらのセキュリティコントロール要件に対して評価されます。

NIST SP 800-53 フレームワークは、NIST SP 800-53 Revision 5 Recommended Security Controls for Federal Information Systems and Organizations で定義されているセキュリティコントロールおよび関連する評価手順を表します。この NIST SP 800-53 フレームワークと、最新の発行された NIST Special Publication SP 800-53 Revision 5 の記載内容の齟齬については、NIST Computer Security Resource Center で入手できる公式に発行されたドキュメントを参照してください。

このフレームワークを使用する

NIST SP 800-53 フレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、NIST 要件に従ってコントロール セットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、NIST SP 800-53 フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートした

り、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
NIST 800-53 Rev 5: 情報システムと組織のセキュリティとプライバシーコントロール	634	373	20

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev-5.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが NIST 標準に準拠しているかどうかを検証することを目的としたものではありません。さらに、NIST 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- 米国国立標準技術研究所 (NIST)

- NIST Computer Security Resource Center
- AWS NIST のコンプライアンスページ

NIST Cybersecurity Framework v1.1

AWS Audit Manager は、NIST Cybersecurity Framework (CSF) v1.1 をサポートする構築済みのフレームワークを提供します。

> **Note**
>
> - NIST SP 800-53 をサポートする Audit Manager フレームワークの詳細については、「」を参照してくださいNIST SP 800-53 Rev 5。
> - NIST SP 800-171 をサポートする Audit Manager フレームワークの詳細については、「」を参照してくださいNIST SP 800-171 Rev 2。

トピック

NIST Cybersecurity Framework とは

米国国立標準技術研究所 (NIST) は、1901 年に設立され、現在は米国商務省の一機関となっています。NIST は、米国で最も古い物理科学研究所の 1 つです。米国議会は、当時は二流だった計測インフラを改善するためにこの機関を設立しました。インフラ整備は英国やドイツなど他の経済大国に後れを取っており、米国の産業競争力にとって大きな課題でした。

米国は、重要なインフラストラクチャの信頼できる機能に依拠しています。サイバーセキュリティの脅威は、重要インフラシステムの複雑化および相互接続性の高まりを悪用するものです。米国のセキュリティ、経済、公衆衛生が危険にさらされています。財務やレピュテーションに対するリスクと同様に、サイバーセキュリティのリスクは企業の利益に影響を及ぼします。コストを押し上げ、収益に影響を及ぼす可能性があります。組織がイノベーションを起こし、顧客を獲得して維持する能力を

損なう可能性があります。最終的に、サイバーセキュリティは組織の全体的なリスク管理を増強する可能性があります。

NIST Cybersecurity Framework (CSF) は、セクターや規模にかかわらず、あらゆる組織で使用するための推奨ベースラインとして、世界中の政府や業界によってサポートされています。NIST Cybersecurity Framework は、フレームワークコア、プロファイル、および実装層といった 3 つの主要要素で構成されています。フレームワークコアには、組織の幅広いサイバーセキュリティの目標をカバーする 23 のカテゴリに整理された望ましいサイバーセキュリティ関連の活動と成果が含まれています。プロファイルには、フレームワークコアの望ましい成果を使用して、組織の要件と目的、リスク選好、およびリソースの組織固有の調整が含まれています。実装層は、組織によるサイバーセキュリティ関連のリスク管理の実践がフレームワークコアで定義された特性にどの程度沿っているかを示します。

このフレームワークを使用する

NIST CSF v1.1 を使用して、監査の準備に役立てることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、NIST CSF 要件に従ってコントロール セットにグループ化されます。Audit Manager は現在、フレームワークコアコンポーネントをサポートしています。Audit Manager は、このフレームワークのプロファイルおよび実装の要素をサポートしていません。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、NIST CSF で定義されているコントロールに基づいて行われます。監査の時期になると、ユーザーまたは選択した代理人が、Audit Manager が収集した証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
NIST サイバーセキュリティ フレームワーク (CSF) v1.1	49	59	22

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_NIST-CSF-v1.1.zip ファイルをダウンロードします。

Audit Manager によって提供されるコントロールは、システムが NIST CSF に準拠しているかどうかを検証することを目的としたものではありません。さらに、これらのコントロールは、NIST 評価に合格することを保証することはできません。 AWS Audit Manager は、手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- 米国国立標準技術研究所 (NIST)
- NIST Computer Security Resource Center
- AWS NIST のコンプライアンスページ
- NIST Cybersecurity Framework - AWS クラウド内の NIST CSF への調整

NIST SP 800-171 Rev 2

AWS Audit Manager は、NIST 800-171 リビジョン 2: 非連邦システムおよび組織における管理対象未分類情報の保護をサポートする構築済みの標準フレームワークを提供します。

> **Note**
>
> - NIST SP 800-53 をサポートする Audit Manager フレームワークの詳細については、「」を参照してくださいNIST SP 800-53 Rev 5。
> - NIST CSF をサポートする Audit Manager フレームワークの詳細については、「」を参照してくださいNIST Cybersecurity Framework v1.1。

トピック

NIST SP 800-171 とは

NIST SP 800-171 は、連邦政府以外のシステムおよび組織における管理対象外情報 (CUI) の機密性の保護に重点を置いています。その目的を達成するための特定のセキュリティ要件を推奨しています。NIST 800-171 は、自己のネットワーク上で CUI を処理する連邦政府以外の組織に必要なセキュリティ標準と慣行を概説する発行物です。これは、米国国立標準技術研究所 (NIST) によって 2015 年 6 月に最初に発行されました。NIST は、公共部門と民間部門のサイバーセキュリティの回復力を強化するために、いくつかの標準と出版物を発表した米国政府機関です。NIST SP 800-171 は、新たなサイバー脅威や変化するテクノロジーに合わせて定期的に更新されています。最新版 (第 2 版) は 2020 年 2 月に公表されました。

NIST SP 800-171 内のサイバーセキュリティコントロールは、政府の請負業者と下請業者の IT ネットワークで CUI を保護します。これは、政府の請負業者がネットワークで CUI を処理または保存するときに遵守しなければならない慣行および手順を定義します。NIST SP 800-171 は、CUI が存在する墨消しのネットワークの一部にのみ適用されます。

このフレームワークを使用する

NIST SP 800-171 フレームワークを使用すると、監査の準備に役立ちます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、NIST 要件に従ってコントロール セットにグループ化されます。このフレームワー

クとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは、NIST SP 800-171 フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
NIST 800-171 リビジョン 2: 非連邦システムおよび組織における管理対象未分類情報の保護	81	29	14

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_NIST-800-171-Rev-2.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが NIST 800-171 に準拠しているかどうかを検証することを目的としたものではありません。さらに、これらのコントロールは、NIST 評価に合格することを保証することはできません。 AWS Audit Manager は、手動証拠収集を必要とする手続き型コントロールを自動的にチェックしません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- 米国国立標準技術研究所 (NIST)
- NIST Computer Security Resource Center
- AWS NIST のコンプライアンスページ

PCI DSS V3.2.1

AWS Audit Manager は、Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 をサポートする構築済みの標準フレームワークを提供します。

> **Note**
>
> PCI DSS v4 およびそれをサポートする Audit Manager フレームワークについては、「PCI DSS V4.0」を参照してください。

トピック

PCI DSS とは

PCI DSS は、独自の情報セキュリティ標準です。これは、American Express、Discover Financial Services、JCB International、 MasterCard Worldwide、Visa Inc によって設立された PCI Security Standards Council によって管理されています。 PCI DSS は、カード所有者データ (CHD) または機

密認証データ (SAD) を保存、処理、または送信するエンティティに適用されます。これには、加盟店、プロセッサー、アクワイアラー、イシュアー、およびサービスプロバイダーが含まれますが、これらに限定されません。PCI DSS は、カードブランドによって義務付けられており、Payment Card Industry Security Standards Council により管理されています。

AWS は PCI DSS レベル 1 サービスプロバイダーとして認定されています。これは、利用可能な最高レベルの評価です。コンプライアンス評価は、独立した認定審査機関 (QSA、Qualified Security Assessor) である Coalfire Systems Inc. によって実施されました。PCI DSS 準拠証明書 (AOC) と責任の概要は、 から入手できます AWS Artifact。これは、 AWS コンプライアンスレポートへのオンデマンドアクセス用のセルフサービスポータルです。AWS ArtifactAWS マネジメントコンソール でにサインインするか、「 の開始方法 AWS Artifact」で詳細を確認してください。

PCI DSS 標準は、PCI Security Standards Council Document Library からダウンロードできます。

監査の準備をサポートするためにこのフレームワークを使用する

PCI DSS V3.2.1 フレームワークを使用すると、PCI DSS 監査の準備をすることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、PCI DSS 要件に従ってコントロール セットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは「PCI DSS V3.2.1」フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	168	116	15

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_PCI-DSS-v3.2.1.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが PCI DSS 標準に準拠しているかどうかを検証することを目的としたものではありません。さらに、PCI DSS 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールを自動的にチェック AWS Audit Manager しません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- PCI セキュリティ基準審議会
- PCI セキュリティ基準審議会ドキュメントライブラリ。
- AWS PCI DSS のコンプライアンスページ

PCI DSS V4.0

AWS Audit Manager は、Payment Card Industry Data Security Standard (PCI DSS) v4.0 をサポートする構築済みのフレームワークを提供します。

> **Note**
>
> PCI DSS v3.2.1 およびそれをサポートする Audit Manager フレームワークについては、「PCI DSS V3.2.1」を参照してください。

トピック

PCI DSS とは

Payment Card Industry Data Security Standard (PCI DSS) は、決済データの保護について技術的な運用要件のベースラインを提供するグローバル標準です。PCI DSS v4.0 は、この標準の新しいバージョンです。

PCI DSS は、決済カードにおけるアカウントデータのセキュリティを促進および強化するために開発されました。また、一貫したデータセキュリティ対策を世界中で幅広く採用することも容易になります。これにより、アカウントデータを保護するための技術的な運用要件のベースラインが提供されます。PCI DSS は、特に決済カードのアカウントデータがある環境に焦点を当てるよう設計されていますが、脅威からの保護や、決済エコシステムの他の要素を保護するためにも使用できます。

PCI セキュリティ基準審議会 (PCI SSC) は、PCI DSS v3.2.1 と v4.0 の間で多くの変更を行いました。変更は 3 つのカテゴリに分類されます。

1. 進化する要件 — 新たな脅威やテクノロジー、決済業界の変化に合わせて基準を最新のものにするための変更。例としては、要件の新規作成または変更、手順のテスト、要件の削除などがあります。
2. 明確化またはガイダンス — 特定のトピックに関する理解を深めたり、さらなる情報やガイダンスを提供するための、表現、説明、定義、追加のガイダンスまたは指示の変更。
3. 構造または形式 — 内容を調整するための要件の結合、分離、番号変更など、内容の再編成。

監査の準備をサポートするためにこのフレームワークを使用する

> **Note**
>
> この標準フレームワークでは、Security Hub の統合コントロールをデータソースとして使用します。統合コントロールから確実に証拠を収集するには、Security Hub で統合コントロールの検出結果の設定が有効になっていることを確認してください。単一データソースの使用についての詳細は、「AWS Audit ManagerによってサポートされるAWS Security Hub コントロール」を参照してください。

PCI DSS V4.0 フレームワークを使用して、監査のための準備を行うことができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらのコントロールは、PCI DSS V4.0 の要件に従いコントロールセットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これは PCI DSS V4.0 フレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
Payment Card Industry Data Security Standard (PCI DSS) v4.0	175	105	15

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_PCI-DSS-v4.0.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが PCI DSS 標準に準拠しているかどうかを検証することを目的としたものではありません。さらに、PCI DSS 監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールを自動的にチェック AWS Audit Manager しません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- PCI DSS v4.0 リソースハブ
- PCI セキュリティ基準審議会
- PCI セキュリティ基準審議会ドキュメントライブラリ。
- AWS PCI DSS のコンプライアンスページ
- AWS コンプライアンスガイドの Payment Card Industry Data Security Standard (PCI DSS) v4.0

SSAE-18 SOC 2

AWS Audit Manager は、「認証エンゲージメント標準書 (SSAE) No. 18、Service Organizations Controls (SOC) Report 2」をサポートする構築済みの標準フレームワークを提供します。

トピック

SOC 2 とは

米国認定会計士協会 (AICPA) によって定義された SOC 2 は、監査中に生成される一連のレポートの名前です。これは、サービス組織 (情報システムをサービスとして他の組織に提供する組織) によって、自社のサービスのユーザーに当該情報システムに対する内部統制の検証済みレポートを発行するために使用されることが企図されています。レポートは、Trust Service Principles として知られる 5 つのカテゴリにグループ化されたコントロールに焦点を当てています。

AWS SOC レポートは、 が主要なコンプライアンス管理と目標を達成した方法を示す独立したサードパーティー審査レポート AWS です。これらのレポートの目的は、ユーザーと監査者が運用とコンプライアンスをサポートするために確立された AWS コントロールを理解できるようにすることです。5 つの AWS SOC レポートがあります。

- AWS SOC 1 レポート。 から AWS 顧客が利用できますAWS Artifact。
- AWS SOC 2 セキュリティ、可用性、機密性レポート。 から AWS 入手できますAWS Artifact。
- AWS SOC 2 セキュリティ、可用性、機密性レポート AWS AWS Artifact (対象範囲には Amazon DocumentDB のみが含まれます) 。
- AWS SOC 2 プライバシータイプ I レポート。 から AWS 入手できますAWS Artifact。
- AWS ホワイトペーパー として公開されている SOC 3 セキュリティ、可用性、機密性レポート。

監査の準備をサポートするためにこのフレームワークを使用する

このフレームワークを使用すると、監査の準備をすることができます。このフレームワークには、説明とテスト手順を含む、構築済みのコントロールのコレクションが含まれています。これらの制御は、SOC 2 要件に従って制御セットにグループ化されます。このフレームワークとそのコントロールをカスタマイズして、特定の要件を満たす必要がある内部監査をサポートすることもできます。

このフレームワークを出発点として使用して Audit Manager 評価を作成し、監査に関連する証拠の収集を開始できます。評価を作成すると、Audit Manager は AWS リソースの評価を開始します。これはフレームワークで定義されているコントロールに基づいて行われます。監査の時間になると、

ユーザー (または任意の受任者) は、Audit Manager で収集された証拠を確認できます。評価の証拠フォルダを参照するか、評価レポートに含める証拠を選択できます。または、エビデンスファインダーを有効にした場合は、特定のエビデンスを検索して CSV 形式でエクスポートしたり、検索結果から評価レポートを作成できます。どの場合でも、この評価レポートは、コントロールが意図したとおりに機能していることを実証するのに役立ちます。

このフレームワークの詳細は以下のとおりです。

のフレームワーク名 AWS Audit Manager	自動化されたコントロールの数	手動コントロールの数	コントロールセットの数
認証業務標準書 (SSAE) No. 18、Service Organizations Controls (SOC) Report 2	46	15	20

> **Tip**
>
> この標準フレームワークでデータソースマッピングとして使用される AWS Config ルールを確認するには、AuditManager_ConfigDataSourceMappings_SSAE-No.-18-SOC-Report-2.zip ファイルをダウンロードします。

この AWS Audit Manager フレームワークのコントロールは、システムが準拠しているかどうかを検証することを目的としたものではありません。さらに、監査に合格することを保証することはできません。手動証拠収集を必要とする手続き型コントロールは自動的にチェック AWS Audit Manager されません。

このフレームワークは、Audit Manager のフレームワークライブラリの標準フレームワークタブにあります。

次のステップ

このフレームワークを使用して評価を作成する方法については、「での評価の作成 AWS Audit Manager」を参照してください。

特定の要件をサポートするためにこのフレームワークをカスタマイズする方法については、「」を参照してくださいで既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager。

追加リソース

- AWS SOC のコンプライアンスページ

自動証拠でサポートされているデータソースタイプ

でカスタムコントロールを作成すると AWS Audit Manager、次のデータソースタイプから自動証拠を収集するようにコントロールを設定できます。

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS API コール

各データソースタイプには、ユーザーアクティビティログ、コンプライアンス検出結果、リソース設定などをキャプチャするための個別の機能があります。

この章では、これらの自動データソースタイプ、および Audit Manager でサポートされている特定の AWS Security Hub コントロール、 AWS Config ルール、 AWS API コールについて説明します。

重要ポイント

次の表は、自動化された各データソースタイプの概要を示しています。

[Data source type]	説明	証拠収集の頻度	このデータソースタイプを使用するには...	このコントロールが評価でアクティブになっている場合..。	関連するトラブルシューティングのヒント
AWS CloudTrail	特定のユーザーアクティビティを	連続。	サポートされているイベント名のリストから選択します。	Audit Manager は、選択したキーワードに基づいて CloudTrail ログをフィルタリ	私の評価では、

[Data source type]	説明	証拠収集の頻度	このデータソースタイプを使用するには...	このコントロールが評価でアクティブになっている場合..。	関連するトラブルシューティングのヒント
	追跡します。			ングします。結果はユーザーアクティビティの証拠としてインポートされます。	AWS CloudTrailからユーザーアクティビティの証拠が収集されていません

[Data source type]	説明	証拠収集の頻度	このデータソースタイプを使用するには...	このコントロールが評価でアクティブになっている場合..。	関連するトラブルシューティングのヒント
AWS Config	から結果を報告することで、リソースセキュリティ体制のスナップショットをキャプチャします AWS Config。	AWS Config ルールで定義されているトリガーに基づきます。	ルールタイプを選択してからルールを選択します。 • マネージドルールの場合は、サポートされているマネージドルールキーワードのリストから選択します。 • カスタムルールについては、使用可能なルールのリストから選択します。	Audit Manager は、このルールの結果をから直接取得しますAWS Config。結果はコンプライアンスチェックの証拠としてインポートされます。	私の評価では、からコンプライアンスチェックの証拠が収集されていませんAWS Config AWS Config統合の問題

[Data source type]	説明	証拠収集の頻度	このデータソースタイプを使用するには...	このコントロールが評価でアクティブになっている場合..。	関連するトラブルシューティングのヒント
AWS Security Hub	Security Hub からの検出結果を報告することにより、リソースのセキュリティ体制のスナップショットをキャプチャします。	Security Hub チェックのスケジュールに基づきます。	サポートされている Security Hub コントロール ID のリストから選択します。	Audit Manager は、Security Hub から直接セキュリティチェックの結果を取得します。結果はコンプライアンスチェックの証拠としてインポートされます。	私の評価では、からコンプライアンスチェックの証拠が収集されていません AWS Security Hub

[Data source type]	説明	証拠収集の頻度	このデータソースタイプを使用するには...	このコントロールが評価でアクティブになっている場合..。	関連するトラブルシューティングのヒント
AWS API コール	指定された への API コールを通じて、リソース設定のスナップショットを直接取得します AWS のサービス。	毎日、毎週、または毎月。	サポートされているAPIコールのリストから選択してから、希望する頻度を選択します。	Audit Manager は、指定された頻度に基づいて API コールを行います。レスポンスは構成データ証拠としてインポートされます。	評価で AWS API コールの設定データの証拠が収集されていない

> **Tip**
>
> 上記のデータソースの事前定義されたグループを使用して証拠を収集するカスタムコントロールを作成できます。これらのデータソースのグループ化は、AWS マネージドソース と呼ばれます。各 AWS マネージドソースは、共通のコントロールまたは共通のコンプライアンス要件に沿ったコアコントロールを表します。これにより、コンプライアンス要件を関連する AWS データソースグループにマッピングする効率的な方法が得られます。使用可能な一般的なコントロールについては、「」を参照してくださいで使用可能なコントロールの検索 AWS Audit Manager。

または、上記の 4 つのデータソースタイプを使用して、独自のカスタムデータソースを定義することもできます。これにより、手動証拠をアップロードしたり、カスタム AWS Config ルールなどのビジネス固有のリソースから自動証拠を収集したりできます。

次のステップ

カスタムコントロールで使用できる特定のデータソースの詳細については、以下のページを参照してください。

- AWS Config ルール でサポートされる AWS Audit Manager
- AWS Security Hub でサポートされている コントロール AWS Audit Manager
- AWS でサポートされている API コール AWS Audit Manager
- AWS CloudTrail でサポートされているイベント名 AWS Audit Manager

AWS Config ルール でサポートされる AWS Audit Manager

Audit Manager を使用して、 AWS Config 評価を監査の証拠としてキャプチャできます。カスタムコントロールを作成または編集する場合、証拠収集のデータソースマッピングとして 1 つ以上の AWS Config ルールを指定できます。これらのルールに基づいてコンプライアンスチェック AWS Config を実行し、Audit Manager は結果をコンプライアンスチェックの証拠としてレポートします。

マネージドルールに加えて、カスタムルールをコントロールデータソースにマッピングすることもできます。

目次

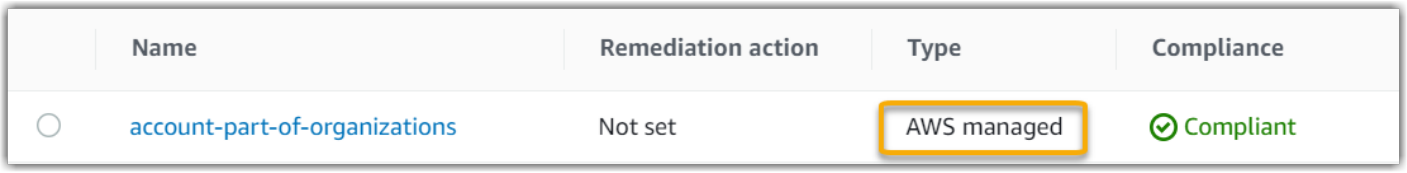
重要ポイント

- Audit Manager は、コンフォーマンスパックおよび AWS Organizationsからのサービスにリンクされたルールを除いて、サービスにリンクされた AWS Config ルールから証拠を収集しません。

- Audit Manager は AWS Config ルールを管理しません。証拠収集を開始する前に、現在の AWS Config ルールパラメータを確認することをお勧めします。次に、選択したフレームワークの要件に対してそれらのパラメータを検証します。必要に応じて、フレームワークの要件に合うようにAWS Configのルールのパラメータを更新できます。これにより、評価によってそのフレームワークに関する正しいコンプライアンスチェックの証拠が確実に収集されるようになります。

  例えば、CIS v1.2.0 の評価を作成するとします。このフレームワークには、「IAM パスワードポリシーで 14 以上の長さを要求する」という名前のコントロールがあります。では AWS Config、iam-password-policyルールにはパスワードの長さを確認するMinimumPasswordLengthパラメータがあります。このパラメータのデフォルト値は 14 文字です。その結果、このルールは統制要件と一致しています。デフォルトのパラメータ値を使用していない場合は、使用する値が CIS v1.2.0 の 14 文字要件以上であることを確認してください。各マネージドルールのデフォルトパラメータの詳細は、AWS Config ドキュメントに記載されています。

- AWS Config ルールがマネージドルールかカスタムルールかを確認する必要がある場合は、AWS Config コンソール を使用してこれを行うことができます。左のナビゲーションメニューから[ルール] を選択し、テーブルでルールを探します。マネージドルールの場合、「タイプ」列には「AWS マネージド」と表示されます。



サポートされている AWS Config マネージドルール

Audit Manager では、次の AWS Config マネージドルールがサポートされています。カスタムコントロールのデータソースを設定するときは、以下のマネージドルール識別子キーワードのいずれかを使用できます。以下にリストされているルールの詳細については、リストから項目を選択するか、「AWS Config ユーザーガイド」の「AWS Config マネージドルール」を参照してください。

> **Tip**
>
> カスタムコントロールの作成中に Audit Manager コンソールでマネージドルールを選択するときは、ルール名ではなく、以下のルール識別キーワードのいずれかを探してください。ルール名とルール識別子の違い、およびマネージドルールの識別子の検索方法については、このユーザーガイドの「トラブルシューティング」セクションを参照してください。

サポートされている AWS Config マネージドルールキーワード

- 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_ENABLED
- 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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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
- 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_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

サポートされている AWS Config マネージドルールキーワード

- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_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
- ECS_AWSVPC_NETWORKINGENABLED
- 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
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- 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

サポートされている AWS Config マネージドルールキーワード

- 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_ENCRYPTED_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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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
- 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_CONCURRENCY_CHECK

サポートされている AWS Config マネージドルールキーワード

- 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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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
- 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

サポートされている AWS Config マネージドルールキーワード

- 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

Audit Manager での AWS Config カスタムルールの使用

AWS Config カスタムルールは、監査レポートのデータソースとして使用できます。コントロールに AWS Config ルールにマッピングされたデータソースがある場合、Audit Manager は AWS Config ルールによって作成された評価を追加します。

使用できるカスタムルールは、Audit Manager にサインイン AWS アカウント する によって異なります。でカスタムルールにアクセスできる場合は AWS Config、Audit Manager のデータソースマッピングとして使用できます。

- 個人向け AWS アカウント – アカウントで作成したカスタムルールのいずれかを使用できます。
- 組織に属するアカウントの場合 — いずれも、メンバーレベルのカスタムルールならどれでも使用できます。または、 AWS Configで利用できる組織レベルのカスタムルールを使用することもできます。

カスタムルールをコントロールのデータソースとしてマッピングしたら、そのコントロールを Audit Manager のカスタムフレームワークに追加できます。

追加リソース

- このデータソースタイプの問題に関するヘルプについては、私の評価では、 からコンプライアンスチェックの証拠が収集されていません AWS Config「」およびAWS Config 「統合の問題」を参照してください。
- このデータソースタイプを使用してカスタムコントロールを作成するには、「」を参照してくださいでのカスタムコントロールの作成 AWS Audit Manager。

- カスタムコントロールを使用するカスタムフレームワークを作成するには、「」を参照してくださいでのカスタムフレームワークの作成 AWS Audit Manager。
- カスタムコントロールを既存のカスタムフレームワークに追加するには、「」を参照してくださいでのカスタムフレームワークの編集 AWS Audit Manager。
- でカスタムルールを作成するには AWS Config、「 デベロAWS Config ッパーガイド」の「 のカスタムルールの開発 AWS Config」を参照してください。

AWS Security Hub でサポートされている コントロール AWS Audit Manager

Audit Manager を使用して、Security Hub の検出結果を監査の証拠としてキャプチャできます。カスタムコントロールを作成または編集するときに、証拠収集のデータソースマッピングとして 1 つ以上の Security Hub コントロールを指定できます。Security Hub はこれらのコントロールに基づいてコンプライアンスチェックを実行し、Audit Manager は結果をコンプライアンスチェックの証拠として報告します。

目次

重要ポイント

- Audit Manager は、Security Hub によって作成されたサービスにリンクされた AWS Config ルールから証拠を収集しません。
- 2022 年 11 月 9 日、Security Hub は、Center for Internet Security の (CIS) AWS Foundations Benchmark バージョン 1.4.0 の要件であるレベル 1 および 2 (CIS v1.4.0) に沿った自動セキュリティチェックを開始しました。Security Hub では、CIS v1.2.0標準に加えて、CIS v1.4.0標準がサポートされています。
- Security Hub の統合されたコントロールの検出結果の設定がまだ有効になっていない場合は、有効にすることをお勧めします。2003年2月23日以降にSecurity Hub を有効にすると、この設定はデフォルトで有効になります。

統合された検出結果を有効にすると、Security Hub はセキュリティチェックごとに 1 つの検出結果を生成します (同じチェックが複数の標準に適用される場合でも)。Security Hub 結果はそれぞれ、Audit Manager に 1 つの固有のリソース評価として収集されます。その結果、検出結果を統合すると、Audit Manager が Security Hub の検出結果に対して実施する固有リソース評価の合計が減少します。このため、統合された検出結果を使用すると、証拠の質と可用性を犠牲にすることなく、Audit Manager の使用コストを削減できることがよくあります。料金の詳細については、「AWS Audit Manager 料金」を参照してください。

統合された検出結果が有効または無効になった場合の証拠の例

以下の例は、Audit Manager がSecurity Hub の設定に応じて証拠を収集して提示する方法を比較したものです。

When consolidated findings is turned on

Security Hub で次の 3 つのセキュリティ標準を有効にしたとします。 AWS FSBP、PCI DSS、CIS Benchmark v1.2.0。

- これらの 3 つの標準はすべて、同じ基になる AWS Config ルールで同じコントロール (IAM.4) iam-root-access-keyを使用します (をチェック) 。
- 統合検出結果設定がオンになっているため、Security Hub はこのコントロールに対して 1 つの検出結果を生成します。
- Security Hub はコントロールの統合された検出結果を Audit Manager に送信します。
- 統合された検出結果は、Audit Manager では 1 つの独自のリソース評価としてカウントされます。その結果、評価には 1 つの証拠が追加されます。

その証拠がどのように見えるかについて、次に例を示します。

```
{
    "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

Security Hub で次の 3 つのセキュリティ標準を有効にしたとします。 AWS FSBP、PCI DSS、CIS Benchmark v1.2.0。

- これらの 3 つの標準はすべて、同じ基になる AWS Config ルールで同じコントロール (IAM.4) iam-root-access-keyを使用します (をチェック) 。
- 統合された検出結果の設定が無効になっているため、Security Hub は、有効な各標準 (この場合は 3 つの検出結果) について、セキュリティチェックごとに個別の検出結果を生成します。
- Security Hub は、このコントロールのために 3 つの標準固有の検出結果をAudit Manager に送信します。

- この3つの検出結果は、Audit Manager では 1 つの独自のリソース評価としてカウントされます。その結果、3 つの別々の証拠が評価に追加されます。

その証拠がどのように見えるかについて、次に例を示します。この例では、次の 3 つのペイロードのセキュリティコントロール ID (*SecurityControlId":"IAM.4"*) がそれぞれ同じであることに注意してください。このため、Audit Manager (IAM.4) でこの証拠を収集する評価コントロールは、Security Hub から以下の検出結果を受信した時点で3 つの別々の証拠を受け取ります。

IAM.4 (FSBP) の証拠


```
{
  "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"
       }
    ]
  }
}
```

IAM.4 (CIS 1.2) の証拠

```
{
  "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"
         }
      ]
   }
}
```

PCI.IAM.1 (PCI DSS) の証拠

```
{
  "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"
      }
   ]
```

```
  }
}
```

サポートされている Security Hub コントロール

現在、以下のSecurity Hub コントロールがAudit Manager でサポートされています。カスタムコントロールのデータソースを設定する際には、以下の標準固有のコントロール ID キーワードのいずれかを使用できます。

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
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

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
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

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
CIS v1.2.0	3.3	CloudWatch.1
CIS v1.2.0	3.4	CloudWatch.4
CIS v1.2.0	3.5	CloudWatch.5
CIS v1.2.0	3.6	CloudWatch.6
CIS v1.2.0	37	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	PCI.AutoScaling.1	AutoScaling.1

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
PCI DSS	PCI.CloudTrail.1	CloudTrail.1
PCI DSS	PCI.CloudTrail.2	CloudTrail.2
PCI DSS	PCI.CloudTrail.3	CloudTrail.3
PCI DSS	PCI.CloudTrail.4	CloudTrail.4
PCI DSS	PCI.CodeBuild.1	CodeBuild.1
PCI DSS	PCI.CodeBuild.2	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.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2.12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI.Guard Duty.1	GuardDuty.1
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

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
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
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI.SageMaker.1	SageMaker.1
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	Account.1	Account.1
AWS 基本的なセキュリティのベストプラクティス	Account.2	Account.2
AWS 基本的なセキュリティのベストプラクティス	ACM.1	ACM.1
AWS 基本的なセキュリティのベストプラクティス	ACM.2	ACM.2
AWS 基本的なセキュリティのベストプラクティス	APIGateway.1	APIGateway.1
AWS 基本的なセキュリティのベストプラクティス	APIGateway.2	APIGateway.2
AWS 基本的なセキュリティのベストプラクティス	APIGateway.3	APIGateway.3
AWS 基本的なセキュリティのベストプラクティス	APIGateway.4	APIGateway.4
AWS 基本的なセキュリティのベストプラクティス	APIGateway.5	APIGateway.5
AWS 基本的なセキュリティのベストプラクティス	APIGateway.8	APIGateway.8

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	APIGateway.9	APIGateway.9
AWS 基本的なセキュリティのベストプラクティス	AppSync.2	AppSync.2
AWS 基本的なセキュリティのベストプラクティス	AppSync.5	AppSync.5
AWS 基本的なセキュリティのベストプラクティス	Athena.1	Athena.1
AWS 基本的なセキュリティのベストプラクティス	AutoScaling.1	AutoScaling.1
AWS 基本的なセキュリティのベストプラクティス	AutoScaling.2	AutoScaling.2
AWS 基本的なセキュリティのベストプラクティス	AutoScaling.3	AutoScaling.3
AWS 基本的なセキュリティのベストプラクティス	AutoScaling.4	AutoScaling.4
AWS 基本的なセキュリティのベストプラクティス	Autoscaling.5	Autoscaling.5
AWS 基本的なセキュリティのベストプラクティス	AutoScaling.6	AutoScaling.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	AutoScaling.9	AutoScaling.9
AWS 基本的なセキュリティのベストプラクティス	Backup.1	Backup.1
AWS 基本的なセキュリティのベストプラクティス	CloudFormation.1	CloudFormation.1
AWS 基本的なセキュリティのベストプラクティス	CloudFront.1	CloudFront.1
AWS 基本的なセキュリティのベストプラクティス	CloudFront.2	CloudFront.2
AWS 基本的なセキュリティのベストプラクティス	CloudFront.3	CloudFront.3
AWS 基本的なセキュリティのベストプラクティス	CloudFront.4	CloudFront.4
AWS 基本的なセキュリティのベストプラクティス	CloudFront.5	CloudFront.5
AWS 基本的なセキュリティのベストプラクティス	CloudFront.6	CloudFront.6
AWS 基本的なセキュリティのベストプラクティス	CloudFront.7	CloudFront.7

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	CloudFront.8	CloudFront.8
AWS 基本的なセキュリティのベストプラクティス	CloudFront.9	CloudFront.9
AWS 基本的なセキュリティのベストプラクティス	CloudFront.10	CloudFront.10
AWS 基本的なセキュリティのベストプラクティス	CloudFront.12	CloudFront.12
AWS 基本的なセキュリティのベストプラクティス	CloudFront.13	CloudFront.13
AWS 基本的なセキュリティのベストプラクティス	CloudTrail.1	CloudTrail.1
AWS 基本的なセキュリティのベストプラクティス	CloudTrail.2	CloudTrail.2
AWS 基本的なセキュリティのベストプラクティス	CloudTrail.3	CloudTrail.3
AWS 基本的なセキュリティのベストプラクティス	CloudTrail.4	CloudTrail.4
AWS 基本的なセキュリティのベストプラクティス	CloudTrail.5	CloudTrail.5

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	CloudTrail.6	CloudTrail.6
AWS 基本的なセキュリティのベストプラクティス	CloudTrail.7	CloudTrail.7
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.1	CloudWatch.1
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.2	CloudWatch.2
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.3	CloudWatch.3
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.4	CloudWatch.4
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.5	CloudWatch.5
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.6	CloudWatch.6
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.7	CloudWatch.7
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.8	CloudWatch.8

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.9	CloudWatch.9
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.10	CloudWatch.10
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.11	CloudWatch.11
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.12	CloudWatch.12
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.13	CloudWatch.13
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.14	CloudWatch.14
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.15	CloudWatch.15
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.16	CloudWatch.16
AWS 基本的なセキュリティのベストプラクティス	CloudWatch.17	CloudWatch.17
AWS 基本的なセキュリティのベストプラクティス	CodeBuild.1	CodeBuild.1

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	CodeBuild.2	CodeBuild.2
AWS 基本的なセキュリティのベストプラクティス	CodeBuild.3	CodeBuild.3
AWS 基本的なセキュリティのベストプラクティス	CodeBuild.4	CodeBuild.4
AWS 基本的なセキュリティのベストプラクティス	CodeBuild.5	CodeBuild.5
AWS 基本的なセキュリティのベストプラクティス	Config.1	Config.1
AWS 基本的なセキュリティのベストプラクティス	DMS.1	DMS.1
AWS 基本的なセキュリティのベストプラクティス	DMS.6	DMS.6
AWS 基本的なセキュリティのベストプラクティス	DMS.7	DMS.7
AWS 基本的なセキュリティのベストプラクティス	DMS.8	DMS.8
AWS 基本的なセキュリティのベストプラクティス	DMS.9	DMS.9

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	DocumentDB.1	DocumentDB.1
AWS 基本的なセキュリティのベストプラクティス	DocumentDB.2	DocumentDB.2
AWS 基本的なセキュリティのベストプラクティス	DocumentDB.3	DocumentDB.3
AWS 基本的なセキュリティのベストプラクティス	DocumentDB.4	DocumentDB.4
AWS 基本的なセキュリティのベストプラクティス	DocumentDB.5	DocumentDB.5
AWS 基本的なセキュリティのベストプラクティス	DynamoDB.1	DynamoDB.1
AWS 基本的なセキュリティのベストプラクティス	DynamoDB.2	DynamoDB.2
AWS 基本的なセキュリティのベストプラクティス	DynamoDB.3	DynamoDB.3
AWS 基本的なセキュリティのベストプラクティス	DynamoDB.4	DynamoDB.4
AWS 基本的なセキュリティのベストプラクティス	DynamoDB.6	DynamoDB.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	EC2.1	EC2.1
AWS 基本的なセキュリティのベストプラクティス	EC2.2	EC2.2
AWS 基本的なセキュリティのベストプラクティス	EC2.3	EC2.3
AWS 基本的なセキュリティのベストプラクティス	EC2.4	EC2.4
AWS 基本的なセキュリティのベストプラクティス	EC2.6	EC2.6
AWS 基本的なセキュリティのベストプラクティス	EC2.7	EC2.7
AWS 基本的なセキュリティのベストプラクティス	EC2.8	EC2.8
AWS 基本的なセキュリティのベストプラクティス	EC2.9	EC2.9
AWS 基本的なセキュリティのベストプラクティス	EC2.10	EC2.10
AWS 基本的なセキュリティのベストプラクティス	EC2.12	EC2.12

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	EC2.13	EC2.13
AWS 基本的なセキュリティのベストプラクティス	EC2.14	EC2.14
AWS 基本的なセキュリティのベストプラクティス	EC2.15	EC2.15
AWS 基本的なセキュリティのベストプラクティス	EC2.16	EC2.16
AWS 基本的なセキュリティのベストプラクティス	EC2.17	EC2.17
AWS 基本的なセキュリティのベストプラクティス	EC2.18	EC2.18
AWS 基本的なセキュリティのベストプラクティス	EC2.19	EC2.19
AWS 基本的なセキュリティのベストプラクティス	EC2.20	EC2.20
AWS 基本的なセキュリティのベストプラクティス	EC2.21	EC2.21
AWS 基本的なセキュリティのベストプラクティス	EC2.22	EC2.22

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	EC2.23	EC2.23
AWS 基本的なセキュリティのベストプラクティス	EC2.24	EC2.24
AWS 基本的なセキュリティのベストプラクティス	EC2.25	EC2.25
AWS 基本的なセキュリティのベストプラクティス	EC2.28	EC2.28
AWS 基本的なセキュリティのベストプラクティス	EC2.51	EC2.51
AWS 基本的なセキュリティのベストプラクティス	ECR.1	ECR.1
AWS 基本的なセキュリティのベストプラクティス	ECR.2	ECR.2
AWS 基本的なセキュリティのベストプラクティス	ECR.3	ECR.3
AWS 基本的なセキュリティのベストプラクティス	ECS.1	ECS.1
AWS 基本的なセキュリティのベストプラクティス	ECS.2	ECS.2

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	ECS.3	ECS.3
AWS 基本的なセキュリティのベストプラクティス	ECS.4	ECS.4
AWS 基本的なセキュリティのベストプラクティス	ECS.5	ECS.5
AWS 基本的なセキュリティのベストプラクティス	ECS.8	ECS.8
AWS 基本的なセキュリティのベストプラクティス	ECS.9	ECS.9
AWS 基本的なセキュリティのベストプラクティス	ECS.10	ECS.10
AWS 基本的なセキュリティのベストプラクティス	ECS.12	ECS.12
AWS 基本的なセキュリティのベストプラクティス	EFS.1	EFS.1
AWS 基本的なセキュリティのベストプラクティス	EFS.2	EFS.2
AWS 基本的なセキュリティのベストプラクティス	EFS.3	EFS.3

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	EFS.4	EFS.4
AWS 基本的なセキュリティのベストプラクティス	EKS.1	EKS.1
AWS 基本的なセキュリティのベストプラクティス	EKS.2	EKS.2
AWS 基本的なセキュリティのベストプラクティス	EKS.8	EKS.8
AWS 基本的なセキュリティのベストプラクティス	ElastiCache.1	ElastiCache.1
AWS 基本的なセキュリティのベストプラクティス	ElastiCache.2	ElastiCache.2
AWS 基本的なセキュリティのベストプラクティス	ElastiCache.3	ElastiCache.3
AWS 基本的なセキュリティのベストプラクティス	ElastiCache.4	ElastiCache.4
AWS 基本的なセキュリティのベストプラクティス	ElastiCache.5	ElastiCache.5
AWS 基本的なセキュリティのベストプラクティス	ElastiCache.6	ElastiCache.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	ElastiCache.7	ElastiCache.7
AWS 基本的なセキュリティのベストプラクティス	ElasticBeanstalk.1	ElasticBeanstalk.1
AWS 基本的なセキュリティのベストプラクティス	ElasticBeanstalk.2	ElasticBeanstalk.2
AWS 基本的なセキュリティのベストプラクティス	ElasticBeanstalk.3	ElasticBeanstalk.3
AWS 基本的なセキュリティのベストプラクティス	ELB.1	ELB.1
AWS 基本的なセキュリティのベストプラクティス	ELB.2	ELB.2
AWS 基本的なセキュリティのベストプラクティス	ELB.3	ELB.3
AWS 基本的なセキュリティのベストプラクティス	ELB.4	ELB.4
AWS 基本的なセキュリティのベストプラクティス	ELB.5	ELB.5
AWS 基本的なセキュリティのベストプラクティス	ELB.6	ELB.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	ELB.7	ELB.7
AWS 基本的なセキュリティのベストプラクティス	ELB.8	ELB.8
AWS 基本的なセキュリティのベストプラクティス	ELB.9	ELB.9
AWS 基本的なセキュリティのベストプラクティス	ELB.10	ELB.10
AWS 基本的なセキュリティのベストプラクティス	ELB.12	ELB.12
AWS 基本的なセキュリティのベストプラクティス	ELB.13	ELB.13
AWS 基本的なセキュリティのベストプラクティス	ELB.14	ELB.14
AWS 基本的なセキュリティのベストプラクティス	ELB.16	ELB.16
AWS 基本的なセキュリティのベストプラクティス	ELBv2.1	ELB.1
AWS 基本的なセキュリティのベストプラクティス	EMR.1	EMR.1

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	EMR.2	EMR.2
AWS 基本的なセキュリティのベストプラクティス	ES.1	ES.1
AWS 基本的なセキュリティのベストプラクティス	ES.2	ES.2
AWS 基本的なセキュリティのベストプラクティス	ES.3	ES.3
AWS 基本的なセキュリティのベストプラクティス	ES.4	ES.4
AWS 基本的なセキュリティのベストプラクティス	ES.5	ES.5
AWS 基本的なセキュリティのベストプラクティス	ES.6	ES.6
AWS 基本的なセキュリティのベストプラクティス	ES.7	ES.7
AWS 基本的なセキュリティのベストプラクティス	ES.8	ES.8
AWS 基本的なセキュリティのベストプラクティス	EventBridge.3	EventBridge3.

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	EventBridge.4	EventBridge.4
AWS 基本的なセキュリティのベストプラクティス	FSx.1	FSx.1
AWS 基本的なセキュリティのベストプラクティス	GuardDuty.1	GuardDuty.1
AWS 基本的なセキュリティのベストプラクティス	IAM.1	IAM.1
AWS 基本的なセキュリティのベストプラクティス	IAM.2	IAM.2
AWS 基本的なセキュリティのベストプラクティス	IAM.3	IAM.3
AWS 基本的なセキュリティのベストプラクティス	IAM.4	IAM.4
AWS 基本的なセキュリティのベストプラクティス	IAM.5	IAM.5
AWS 基本的なセキュリティのベストプラクティス	IAM.6	IAM.6
AWS 基本的なセキュリティのベストプラクティス	IAM.7	IAM.7

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	IAM.8	IAM.8
AWS 基本的なセキュリティのベストプラクティス	IAM.9	IAM.9
AWS 基本的なセキュリティのベストプラクティス	IAM.10	IAM.10
AWS 基本的なセキュリティのベストプラクティス	IAM.11	IAM.11
AWS 基本的なセキュリティのベストプラクティス	IAM.12	IAM.12
AWS 基本的なセキュリティのベストプラクティス	IAM.13	IAM.13
AWS 基本的なセキュリティのベストプラクティス	IAM.14	IAM.14
AWS 基本的なセキュリティのベストプラクティス	IAM.15	IAM.15
AWS 基本的なセキュリティのベストプラクティス	IAM.16	IAM.16
AWS 基本的なセキュリティのベストプラクティス	IAM.17	IAM.17

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	IAM.18	IAM.18
AWS 基本的なセキュリティのベストプラクティス	IAM.19	IAM.19
AWS 基本的なセキュリティのベストプラクティス	IAM.21	IAM.21
AWS 基本的なセキュリティのベストプラクティス	IAM.22	IAM.22
AWS 基本的なセキュリティのベストプラクティス	Kinesis.1	Kinesis.1
AWS 基本的なセキュリティのベストプラクティス	KMS.1	KMS.1
AWS 基本的なセキュリティのベストプラクティス	KMS.2	KMS.2
AWS 基本的なセキュリティのベストプラクティス	KMS.3	KMS.3
AWS 基本的なセキュリティのベストプラクティス	KMS.4	KMS.4
AWS 基本的なセキュリティのベストプラクティス	Lambda.1	Lambda.1

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	Lambda.2	Lambda.2
AWS 基本的なセキュリティのベストプラクティス	Lambda.3	Lambda.3
AWS 基本的なセキュリティのベストプラクティス	Lambda.5	Lambda.5
AWS 基本的なセキュリティのベストプラクティス	Macie.1	Macie.1
AWS 基本的なセキュリティのベストプラクティス	MQ.5	MQ.5
AWS 基本的なセキュリティのベストプラクティス	MQ.6	MQ.6
AWS 基本的なセキュリティのベストプラクティス	MSK.1	MSK.1
AWS 基本的なセキュリティのベストプラクティス	MSK.2	MSK.2
AWS 基本的なセキュリティのベストプラクティス	Neptune.1	Neptune.1
AWS 基本的なセキュリティのベストプラクティス	Neptune.2	Neptune.2

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	Neptune.3	Neptune.3
AWS 基本的なセキュリティのベストプラクティス	Neptune.4	Neptune.4
AWS 基本的なセキュリティのベストプラクティス	Neptune.5	Neptune.5
AWS 基本的なセキュリティのベストプラクティス	Neptune.6	Neptune.6
AWS 基本的なセキュリティのベストプラクティス	Neptune.7	Neptune.7
AWS 基本的なセキュリティのベストプラクティス	Neptune.8	Neptune.8
AWS 基本的なセキュリティのベストプラクティス	Neptune.9	Neptune.9
AWS 基本的なセキュリティのベストプラクティス	NetworkFirewall.1	NetworkFirewall.1
AWS 基本的なセキュリティのベストプラクティス	NetworkFirewall.2	NetworkFirewall.2
AWS 基本的なセキュリティのベストプラクティス	NetworkFirewall.3	NetworkFirewall.3

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	NetworkFirewall.4	NetworkFirewall.4
AWS 基本的なセキュリティのベストプラクティス	NetworkFirewall.5	NetworkFirewall.5
AWS 基本的なセキュリティのベストプラクティス	NetworkFirewall.6	NetworkFirewall.6
AWS 基本的なセキュリティのベストプラクティス	NetworkFirewall.9	NetworkFirewall.9
AWS 基本的なセキュリティのベストプラクティス	Opensearch.1	Opensearch.1
AWS 基本的なセキュリティのベストプラクティス	Opensearch.2	Opensearch.2
AWS 基本的なセキュリティのベストプラクティス	Opensearch.3	Opensearch.3
AWS 基本的なセキュリティのベストプラクティス	Opensearch.4	Opensearch.4
AWS 基本的なセキュリティのベストプラクティス	Opensearch.5	Opensearch.5
AWS 基本的なセキュリティのベストプラクティス	Opensearch.6	Opensearch.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	Opensearch.7	Opensearch.7
AWS 基本的なセキュリティのベストプラクティス	Opensearch.8	Opensearch.8
AWS 基本的なセキュリティのベストプラクティス	Opensearch.10	Opensearch.10
AWS 基本的なセキュリティのベストプラクティス	PCA.1	PCA.1
AWS 基本的なセキュリティのベストプラクティス	RDS.1	RDS.1
AWS 基本的なセキュリティのベストプラクティス	RDS.2	RDS.2
AWS 基本的なセキュリティのベストプラクティス	RDS.3	RDS.3
AWS 基本的なセキュリティのベストプラクティス	RDS.4	RDS.4
AWS 基本的なセキュリティのベストプラクティス	RDS.5	RDS.5
AWS 基本的なセキュリティのベストプラクティス	RDS.6	RDS.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	RDS.7	RDS.7
AWS 基本的なセキュリティのベストプラクティス	RDS.8	RDS.8
AWS 基本的なセキュリティのベストプラクティス	RDS.9	RDS.9
AWS 基本的なセキュリティのベストプラクティス	RDS.10	RDS.10
AWS 基本的なセキュリティのベストプラクティス	RDS.11	RDS.11
AWS 基本的なセキュリティのベストプラクティス	RDS.12	RDS.12
AWS 基本的なセキュリティのベストプラクティス	RDS.13	RDS.13
AWS 基本的なセキュリティのベストプラクティス	RDS.14	RDS.14
AWS 基本的なセキュリティのベストプラクティス	RDS.15	RDS.15
AWS 基本的なセキュリティのベストプラクティス	RDS.16	RDS.16

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	RDS.17	RDS.17
AWS 基本的なセキュリティのベストプラクティス	RDS.18	RDS.18
AWS 基本的なセキュリティのベストプラクティス	RDS.19	RDS.19
AWS 基本的なセキュリティのベストプラクティス	RDS.20	RDS.20
AWS 基本的なセキュリティのベストプラクティス	RDS.21	RDS.21
AWS 基本的なセキュリティのベストプラクティス	RDS.22	RDS.22
AWS 基本的なセキュリティのベストプラクティス	RDS.23	RDS.23
AWS 基本的なセキュリティのベストプラクティス	RDS.24	RDS.24
AWS 基本的なセキュリティのベストプラクティス	RDS.25	RDS.25
AWS 基本的なセキュリティのベストプラクティス	RDS.26	RDS.26

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	RDS.27	RDS.27
AWS 基本的なセキュリティのベストプラクティス	RDS.34	RDS.34
AWS 基本的なセキュリティのベストプラクティス	RDS.35	RDS.35
AWS 基本的なセキュリティのベストプラクティス	Redshift.1	Redshift.1
AWS 基本的なセキュリティのベストプラクティス	Redshift.2	Redshift.2
AWS 基本的なセキュリティのベストプラクティス	Redshift.3	Redshift.3
AWS 基本的なセキュリティのベストプラクティス	Redshift.4	Redshift.4
AWS 基本的なセキュリティのベストプラクティス	Redshift.6	Redshift.6
AWS 基本的なセキュリティのベストプラクティス	Redshift.7	Redshift.7
AWS 基本的なセキュリティのベストプラクティス	Redshift.8	Redshift.8

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	Redshift.9	Redshift.9
AWS 基本的なセキュリティのベストプラクティス	Redshift.10	Redshift.10
AWS 基本的なセキュリティのベストプラクティス	Route53.2	Route53.2
AWS 基本的なセキュリティのベストプラクティス	S3.1	S3.1
AWS 基本的なセキュリティのベストプラクティス	S3.2	S3.2
AWS 基本的なセキュリティのベストプラクティス	S3.3	S3.3
AWS 基本的なセキュリティのベストプラクティス	S3.4	S3.4
AWS 基本的なセキュリティのベストプラクティス	S3.5	S3.5
AWS 基本的なセキュリティのベストプラクティス	S3.6	S3.6
AWS 基本的なセキュリティのベストプラクティス	S3.7	S3.7

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	S3.8	S3.8
AWS 基本的なセキュリティのベストプラクティス	S3.9	S3.9
AWS 基本的なセキュリティのベストプラクティス	S3.11	S3.11
AWS 基本的なセキュリティのベストプラクティス	S3.12	S3.12
AWS 基本的なセキュリティのベストプラクティス	S3.13	S3.13
AWS 基本的なセキュリティのベストプラクティス	S3.14	S3.14
AWS 基本的なセキュリティのベストプラクティス	S3.15	S3.15
AWS 基本的なセキュリティのベストプラクティス	S3.17	S3.17
AWS 基本的なセキュリティのベストプラクティス	S3.19	S3.19
AWS 基本的なセキュリティのベストプラクティス	S3.19	S3.20

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	SageMaker.1	SageMaker.1
AWS 基本的なセキュリティのベストプラクティス	SageMaker.2	SageMaker.2
AWS 基本的なセキュリティのベストプラクティス	SageMaker.3	SageMaker.3
AWS 基本的なセキュリティのベストプラクティス	SecretsManager.1	SecretsManager.1
AWS 基本的なセキュリティのベストプラクティス	SecretsManager.2	SecretsManager.2
AWS 基本的なセキュリティのベストプラクティス	SecretsManager.3	SecretsManager.3
AWS 基本的なセキュリティのベストプラクティス	SecretsManager.4	SecretsManager.4
AWS 基本的なセキュリティのベストプラクティス	SNS.1	SNS.1
AWS 基本的なセキュリティのベストプラクティス	SNS.2	SNS.2
AWS 基本的なセキュリティのベストプラクティス	SQS.1	SQS.1

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	SSM.1	SSM.1
AWS 基本的なセキュリティのベストプラクティス	SSM.2	SSM.2
AWS 基本的なセキュリティのベストプラクティス	SSM.3	SSM.3
AWS 基本的なセキュリティのベストプラクティス	SSM.4	SSM.4
AWS 基本的なセキュリティのベストプラクティス	StepFunctions.1	StepFunctions.1
AWS 基本的なセキュリティのベストプラクティス	WAF.1	WAF.1
AWS 基本的なセキュリティのベストプラクティス	WAF.2	WAF.2
AWS 基本的なセキュリティのベストプラクティス	WAF.3	WAF.3
AWS 基本的なセキュリティのベストプラクティス	WAF.4	WAF.4
AWS 基本的なセキュリティのベストプラクティス	WAF.6	WAF.6

セキュリティ標準	Audit Manager でサポートされているキーワード (Security Hubの標準コントロールID)	関連コントロールドキュメント (セキュリティハブの対応するセキュリティコントロール ID)
AWS 基本的なセキュリティのベストプラクティス	WAF.7	WAF.7
AWS 基本的なセキュリティのベストプラクティス	WAF.8	WAF.8
AWS 基本的なセキュリティのベストプラクティス	WAF.10	WAF.10
AWS 基本的なセキュリティのベストプラクティス	WAF.11	WAF.11
AWS 基本的なセキュリティのベストプラクティス	WAF.12	WAF.12

追加リソース

- このデータソースタイプの証拠収集に関する問題については、「」を参照してください私の評価では、 からコンプライアンスチェックの証拠が収集されていません AWS Security Hub。
- このデータソースタイプを使用してカスタムコントロールを作成するには、「」を参照してくださいでのカスタムコントロールの作成 AWS Audit Manager。
- カスタムコントロールを使用するカスタムフレームワークを作成するには、「」を参照してくださいでのカスタムフレームワークの作成 AWS Audit Manager。
- カスタムコントロールを既存のカスタムフレームワークに追加するには、「」を参照してくださいでのカスタムフレームワークの編集 AWS Audit Manager。

AWS でサポートされている API コール AWS Audit Manager

Audit Manager を使用して、 AWS 環境のスナップショットを監査の証拠としてキャプチャできます。カスタムコントロールを作成または編集するときに、証拠収集のデータソースマッピングとして 1 つ以上の AWS API コールを指定できます。その後、Audit Manager は関連する に対して API コールを行い AWS のサービス、 AWS リソースの設定詳細のスナップショットを収集します。

API コールの範囲内にあるすべてのリソースについて、 Audit Managerは設定スナップショットをキャプチャし、それを証拠に変換します。これにより、(API コールではなく) リソースごとに 1 つの証拠が得られます。

例えば、`ec2_DescribeRouteTables` API コールが5つのルートテーブルから設定スナップショットをキャプチャする場合、その1つのAPI コールで合計5つの証拠が得られます。各証拠は、個々のルートテーブルの設定のスナップショットです。

トピック

重要ポイント

ページ分割された API コール

多くの は大量のデータを収集 AWS のサービス して保存します。そのため、`list`、`describe`、または `get`API コールでデータを返そうとすると、多くの結果が得られる可能性があります。データ量が多すぎて1 回のレスポンスでは返せない場合、ページ分割を使用すれば、結果を分割して管理しやすい大きさにすることができます。これにより、結果がデータの「ページ」に分割され、レスポンスが処理しやすくなります。

一部の カスタムコントロールデータソースでサポートされるAPI コールはページ分割されています。つまり、最初は部分的な結果を返し、それ以降のリクエストでは結果セット全体を返すのです。例えば、Amazon RDS DescribeDBInstances オペレーションで一度に最大 100 個のインスタンスを返し、結果の次のページを返すにはそれ以降のリクエストが必要になります。

2023年3月8日以降、Audit Manager は証拠収集のデータソースとしてページ分割されたAPI コールをサポートしています。以前は、ページ分割されたAPI コールをデータソースとして使用すると、APIレスポンスではリソースのサブセットのみが返されていました (最大 100 件の結果)。現在では、Audit Manager はページ分割されたAPIオペレーションを複数回呼び出し、すべてのリソースが返されるまで結果の各ページを取得します。次に、Audit Manager はリソースごとに構成スナップショットをキャプチャし、証拠として保存します。リソースの完全なセットが API レスポンスにキャプチャされるようになったため、2023 年 3 月 8 日以降に収集された証拠の量が増加する可能性があります。

Audit Manager はAPI コールのページ分割を自動的に処理します。データ ソースとしてページ分割されたAPI コールを使用するカスタムコントロールを作成する場合は、ページ分割パラメータを指定する必要はありません。

カスタムコントロールデータソースでサポートされるAPI コール

カスタムコントロールでは、次の API コールのいずれかをデータソースとして使用できます。Audit Manager は、これらの API コールを使用して、 AWS 使用状況に関する証拠を収集できます。

サポートされるAPI コール	Audit Manager でこの API を使用して証拠を収集する方法
acm_GetAccountConfiguration	AWS アカウントに関連付けられているアカウント設定オプションのスナップショットを収集します。
acm_ListCertificates	証明書の ARN とドメイン名のリストを取得します。
autoscaling_DescribeAutoScalingGroups	内の Auto Scaling グループに関するスナップショットを収集します AWS アカウント。
backup_ListBackupPlans	内のすべてのアクティブなバックアッププランのリストを取得します AWS アカウント。
bedrock_GetModelInvocationLoggingConfiguration	のモデルのモデル呼び出しログ記録の現在の設定値のスナップショットを収集します AWS アカウント。
クラウドフロント_ListDistributions	内のすべてのディストリビューションのリストを取得します AWS アカウント。

サポートされるAPIコール	Audit Manager でこの API を使用して証拠を収集する方法
cloudtrail_DescribeTrails	AWS アカウントの現在のリージョンに関連する 1 つ以上の証跡おける設定のスナップショットを収集します。
cloudtrail_ListTrails	にある証跡のリストを取得します AWS アカウント。
cloudwatch_DescribeAlarms	AWS アカウントに使用されているアラームの設定スナップショットを収集します。
config_DescribeConfigRules	AWS Config ルールの詳細を取得します。
config_DescribeDeliveryChannels	AWS アカウント内の配信チャネルの設定スナップショットを収集します。
directconnect_DescribeDirectConnectGateways	すべての AWS Direct Connect ゲートウェイ のリストを取得します。
directconnect_DescribeVirtualGateways	AWS アカウントが所有する仮想プライベートゲートウェイのリストを取得します。
docdb_DescribeCertificates	AWS アカウントに関する証明書のリストを収集します。
docdb_DescribeDBClusterParameterGroups	AWS アカウントにおける `DBClusterParameterGroup` の説明のリストを収集します。
docdb_DescribeDBInstances	AWS アカウントのプロビジョニングされた Amazon DynamoDB インスタンスに関する情報を収集します。
cloudwatch_DescribeAlarms	のアラームに関する情報を収集します AWS アカウント。
cloudtrail_DescribeTrails	に関連付けられている 1 つ以上の証跡の設定のスナップショットを収集します AWS アカウント。

サポートされるAPIコール	Audit Manager でこの API を使用して証拠を収集する方法
dynamodb_DescribeTable	AWS アカウント内の DynamoDB テーブルの設定スナップショットを収集します。 このAPIをデータソースとして使用する場合、特定の DynamoDB テーブルの名前を指定する必要はありません。代わりに、Audit Manager はListTables オペレーションを使用してすべてのテーブルを一覧表示します。一覧表示されているすべてのテーブルに対して、Audit Manager は DescribeTable のオペレーションを実行して、そのリソースの証拠を生成します。
dynamodb_ListBackups	AWS アカウントに関連付けられている DynamoDB バックアップのリストを取得します。
dynamodb_ListTables	AWS アカウント と現在のエンドポイントに関連付けられているすべてのテーブル名のリストを取得します。
ec2_DescribeAddresses	Elastic IP アドレスのスナップショットを収集します。
ec2_DescribeCustomerGateways	VPN カスタマーゲートウェイのスナップショットを収集します。
ec2_DescribeEgressOnlyInternetGateways	egress-only インターネットゲートウェイのスナップショットを収集します。
ec2_DescribeFlowLogs	フローログのスナップショットを収集します。
ec2_DescribeInstances	インスタンスのスナップショットを収集します。
ec2_DescribeInternetGateways	インターネットゲートウェイのスナップショットを収集します。

サポートされるAPI コール	Audit Manager でこの API を使用して証拠を収集する方法
ec2_DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	仮想インターフェイスグループと のローカルゲートウェイルートテーブル間の関連付けの説明を収集します AWS アカウント。
ec2_DescribeLocalGateways	ローカルゲートウェイのスナップショットを収集します。
ec2_DescribeLocalGatewayVirtualInterfaces	ローカルゲートウェイの仮想インターフェースのスナップショットを収集します。
ec2_DescribeNatGateways	NAT ゲートウェイのスナップショットを収集します。
ec2_DescribeNetworkAcls	ネットワーク ACL のスナップショットを収集します。
ec2_DescribeRouteTables	ルートテーブルのスナップショットを収集します。
ec2_DescribeSecurityGroups	セキュリティグループのスナップショットを収集します。
ec2_DescribeSecurityGroupRules	1 つ以上のセキュリティグループルールのスナップショットを収集します。
ec2_DescribeTransitGateways	トランジットゲートウェイのスナップショットを収集します。
ec2_DescribeVolumes	VPC エンドポイントのスナップショットを収集します。
ec2_DescribeVpcs	VPC のスナップショットを収集します。

サポートされるAPI コール	Audit Manager でこの API を使用して証拠を収集する方法
ec2_DescribeVpcEndpoints	VPC エンドポイントのスナップショットを収集します。
ec2_DescribeVpcEndpointConnections	VPC エンドポイントサービスへの VPC エンドポイント接続のスナップショットを収集します。これには、承認保留中のエンドポイントも含まれます。
ec2_DescribeVpcEndpointServiceConfigurations	で VPC エンドポイントサービス設定のスナップショットを収集します AWS アカウント。
ec2_DescribeVpcPeeringConnections	VPN 接続のスナップショットを収集します。
ec2_DescribeVpnConnections	VPN 接続のスナップショットを収集します。
ec2_DescribeVpnGateways	仮想プライベートゲートウェイのスナップショットを収集します。
ec2_GetEbsDefaultKmsKeyId	現在のリージョンの AWS KMS key の EBS 暗号化のデフォルト AWS アカウント のスナップショットを収集します。
ec2_GetEbsEncryptionByDefault	現在のリージョンの AWS アカウント に対してデフォルトでの EBS 暗号化が有効になっているかどうかを示します。
ECS_DescribeClusters	ECS クラスターのスナップショットを収集します。
eks_DescribeAddonVersions	アドオンバージョンのスナップショットを収集します。
elasticache_DescribeCacheClusters	プロビジョニングされたクラスターのスナップショットを収集します。

サポートされるAPIコール	Audit Manager でこの API を使用して証拠を収集する方法
elasticache_DescribeServiceUpdates	Amazon のサービス更新のスナップショットを収集します ElastiCache。
elasticfilesystem_DescribeAccessPoints	内の Amazon EFS アクセスポイントのスナップショットを収集します AWS アカウント。
elasticfilesystem_DescribeFileSystems	Amazon EFS ファイルシステムのスナップショットを収集します。
elasticloadbalancingv2_DescribeLoadBalancers	のロードバランサーのスナップショットを収集します AWS アカウント。
elasticloadbalancingv2_DescribeSSLPolicies	SSL ネゴシエーションに使用するポリシーのスナップショットを収集します。
elasticloadbalancingv2_DescribeTargetGroups	ELB ターゲットグループのスナップショットを収集します。
elasticmapreduce_ListSecurityConfigurations	AWS アカウントで確認できるセキュリティ設定のリストを、その作成日時および名前とともに取得します。
events_ListConnections	内の Amazon EventBridge 接続のリストを取得します AWS アカウント。
events_ListEventBuses	デフォルトの EventBridge イベントバス AWS アカウント、カスタムイベントバス、パートナーイベントバスなど、 内の Amazon イベントバスのリストを取得します。
events_ListEventSources	AWS アカウントで共有されているパートナーイベントソースのリストを取得します。

サポートされるAPIコール	Audit Manager でこの API を使用して証拠を収集する方法
events_ListRules	Amazon EventBridge ルールのリストを取得します。
Firehose_ListDeliveryStreams	配信ストリームのリストを取得します。
fsx_DescribeFileSystems	AWS アカウントが所有するファイルシステムのスナップショットを収集します。
ガードデューティListDetectors	Amazon GuardDuty ディテクターリソースの `detectorIds` のリストを取得します。
iam_GenerateCredentialReport	AWS アカウントの認証情報レポートを生成します。
iam_GetAccountPasswordPolicy	AWS アカウントのパスワードポリシーのスナップショットを収集します。
iam_GetAccountSummary	AWS アカウント内での IAM エンティティの使用状況および IAM クォータのスナップショットを収集します。
iam_ListGroups	で使用可能なパスプレフィックスに関連付けられている IAM グループのリストを取得します AWS アカウント。
iam_ListOpenIDConnectProviders	AWS アカウントで定義されている IAM OpenID Connect (OIDC) プロバイダーリソースオブジェクトのリストを取得します。
iam_ListPolicies	AWS アカウントで使用できる管理ポリシーのリストを取得します。これには、独自の顧客定義の管理ポリシーおよび AWS マネージドポリシーが含まれます。
iam_ListRoles	で使用可能なパスプレフィックスに関連付けられている IAM ロールのリストを取得します AWS アカウント。

サポートされるAPI コール	Audit Manager でこの API を使用して証拠を収集する方法
iam_ListSAMLProviders	AWS アカウントの IAM で定義されている SAML プロバイダーリソースオブジェクトのリストを取得します。
iam_ListUsers	内の IAM ユーザーのリストを取得します AWS アカウント。
iam_ListVirtualMFADevices	AWS アカウント内で定義されている仮想 MFA デバイスのリストを取得します。
kafka_ListClusters	内の Amazon MSK クラスターのリストを取得します AWS アカウント。
kafka_ListKafkaVersions	AWS アカウント内にある Apache Kafka バージョンのオブジェクトのリストを取得します。
kinesis_ListStreams	Kinesis データストリームのリストを取得します。
kms_GetKeyPolicy	Audit Manager はこの API を使用して、 AWS アカウント内にある AWS KMS keys のキーポリシーのスナップショットを収集します。 この API をデータソースとして使用する場合は、特定の の名前を指定する必要はありません AWS KMS key。代わりに、Audit Managerは `ListKeys` オペレーションを使用してすべての KMS キーを一覧表示します。次に、Audit Manager は、一覧表示されているすべての KMS キーに対して `GetKeyPolicy` オペレーションを実行して、そのリソースの証拠を生成します。
kms_GetKeyRotationStatus	Audit Manager は、この API を使用して、 AWS KMS keys で に対して自動ローテーションが有効になっているかどうかのスナップショットを収集します AWS アカウント。 この API をデータソースとして使用する場合は、特定の の名前を指定する必要はありません AWS KMS key。代わりに、Audit Managerは `ListKeys` オペレーションを使用してすべての KMS キーを一覧表示します。次に、Audit Manager は、一覧表示されているすべての KMS キーに対して `GetKeyRotationStatus` オペレーションを実行して、そのリソースの証拠を生成します。

サポートされるAPI コール	Audit Manager でこの API を使用して証拠を収集する方法
kms_ListKeys	内の AWS KMS keys のリストを取得します AWS アカウント。
Lambda_ListFunctions	のバージョン固有の設定を使用して AWS アカウント、 内の Lambda 関数のリストを取得します。
rds_DescribeDBClusters	内の既存の Amazon Aurora DB クラスターとマルチ AZ DB クラスターのスナップショットを収集します AWS アカウント。
rds_DescribeDBInstances	AWS アカウント内のプロビジョニングされた RDS インスタンスのスナップショットを収集します。
rds_DescribeDbInstanceAutomatedBackups	内の現在削除されているインスタンスと削除されたインスタンスの両方のバックアップのスナップショットを収集します AWS アカウント。
rds_DescribeDbSecurityGroups	で DB のスナップショットを収集SecurityGroups します AWS アカウント。
redshift_DescribeClusters	AWS アカウント内のプロビジョニングされた Amazon Redshift クラスターのスナップショットを収集します。

サポートされるAPIコール	Audit Manager でこの API を使用して証拠を収集する方法
s3_GetBucketEncryption	S3 バケットのデフォルトの暗号化設定を示すスナップショットを収集します。 この API をデータソースとして使用する場合、特定の S3 バケットの名前を指定する必要はありません。代わりに、Audit Manager は`ListBuckets` オペレーションを使用してすべてのバケットを一覧表示します。一覧表示されているすべてのバケットに対して、Audit Manager は`GetBucketEncryption` オペレーションを実行して、そのリソースの証拠を生成します。 Audit Manager は、評価 AWS リージョン と同じ で作成されたバケットの暗号化ステータスのみを提供できます。複数の にまた AWS リージョンがるすべての S3 バケットの暗号化ステータスを確認する必要がある場合は AWS リージョン、S3 バケットがある各 で評価を作成することをお勧めします。
s3_ListBuckets	内の S3 バケットのリストを取得します AWS アカウント。
sagemaker_ListAlgorithms	内の機械学習アルゴリズムのリストを取得します AWS アカウント。
sagemaker_ListDomains	内のドメインのリストを取得します AWS アカウント。
sagemaker_ListEndpoints	のエンドポイントのリストを取得します AWS アカウント。
sagemaker_ListEndpointConfigs	のエンドポイント設定のリストを取得します AWS アカウント。
sagemaker_ListFlowDefinitions	のフロー定義のリストを取得します AWS アカウント。
sagemaker_ListHumanTaskUis	のヒューマンタスクインターフェイスのリストを取得します AWS アカウント。

サポートされるAPIコール	Audit Manager でこの API を使用して証拠を収集する方法
sagemaker_ListLabelingJobs	内のラベル付けジョブのリストを取得します AWS アカウント。
sagemaker_ListModels	内のモデルのリストを取得します AWS アカウント。
sagemaker_ListModelBiasJobDefinitions	でモデルバイアスジョブ定義のリストを取得します AWS アカウント。
sagemaker_ListModelCards	内のモデルカードのリストを取得します AWS アカウント。
sagemaker_ListModelQualityJobDefinitions	でモデル品質モニタリングジョブ定義のリストを取得します AWS アカウント。
sagemaker_ListMonitoringAlerts	特定のモニタリングスケジュールのアラートのリストを取得します。
sagemaker_ListMonitoringSchedules	内のすべてのモニタリングスケジュールのリストを取得します AWS アカウント。
sagemaker_ListTrainingJobs	のトレーニングジョブのリストを取得します AWS アカウント。
sagemaker_ListUserProfiles	でユーザープロファイルのリストを取得します AWS アカウント。
secretsmanager_ListSecrets	削除対象としてマークされたシークレットを含まない AWS アカウント、に保存されているシークレットのリストを取得します。
sns_ListTopics	の SNS トピックのリストを取得します AWS アカウント。

サポートされるAPIコール	Audit Manager でこの API を使用して証拠を収集する方法
sqs_ListQueues	内の SQS キューのリストを取得します AWS アカウント。
waf-regional_ListWebAcls	の WebACLSummary オブジェクトのリストを取得します AWS アカウント。
waf-regional_ListRules	のRuleSummaryオブジェクトのリストを取得します AWS アカウント。
waf_ListRuleGroups	のルールグループのRuleGroupSummaryオブジェクトのリストを取得します AWS アカウント。
waf_ListRules	のRuleSummaryオブジェクトのリストを取得します AWS アカウント。
waf_ListWebAcls	の WebACLSummary オブジェクトのリストを取得します AWS アカウント。

AWS License Manager 標準フレームワークで使用される API コール

AWS License Manager 標準フレームワークにおいて、Audit Manager は、証拠を収集するために `GetLicenseManagerSummary` と呼ばれるカスタムアクティビティを使用します。このアクティビティでは、次の 3 つのLicense Manager API を呼び出します。

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

返されたデータは証拠に変換され、評価の関連するコントロールにアタッチされます。

例

2 つのライセンス製品 (SQL Service 2017 と Oracle Database Enterprise Edition) を使用しているとします。まず、`GetLicenseManagerSummary`アクティビティは ListLicenseConfigurations API を呼び出し、アカウント内のライセンス設定の詳細を提供します。次に、 ListUsageForLicenseConfigurationと を呼び出して、ライセンス設定ごとにコンテキストデータを追加しますListAssociationsForLicenseConfiguration。最後に、ライセンス設定データを証拠に変

換し、フレームワークのそれぞれのコントロールにアタッチします (4.5 - SQL Server 2017 のカスタマーマネージドライセンスおよび 3.0.4 - Oracle Database Enterprise Edition のカスタマーマネージドライセンス)。

フレームワークのどのコントロールによってもカバーされていないライセンス製品を使用している場合、そのライセンス設定データは、次のコントロールの証拠としてアタッチされます: 5.0 - 他のライセンスのカスタマーマネージドライセンス。

追加リソース

- このデータソースタイプの証拠収集に関する問題については、「」を参照してください評価で AWS API コールの設定データの証拠が収集されていない。
- このデータソースタイプを使用してカスタムコントロールを作成するには、「」を参照してくださいでのカスタムコントロールの作成 AWS Audit Manager。
- カスタムコントロールを使用するカスタムフレームワークを作成するには、「」を参照してくださいでのカスタムフレームワークの作成 AWS Audit Manager。
- カスタムコントロールを既存のカスタムフレームワークに追加するには、「」を参照してくださいでのカスタムフレームワークの編集 AWS Audit Manager。

AWS CloudTrail でサポートされているイベント名 AWS Audit Manager

Audit Manager を使用して、監査の証拠として AWS CloudTrail 管理イベントとグローバルサービスイベントをキャプチャできます。カスタムコントロールを作成または編集するときに、証拠収集のデータソースマッピングとして 1 つ以上の CloudTrail イベント名を指定できます。Audit Manager は、選択したキーワードに基づいて CloudTrail ログをフィルタリングし、その結果をユーザーアクティビティの証拠としてインポートします。

> **Note**
>
> Audit Manager は、管理イベントとグローバルサービスイベントのみをキャプチャします。データイベントやインサイトイベントは証拠として利用できません。さまざまなタイプの CloudTrail イベントの詳細については、「 ユーザーガイド」の「 のCloudTrail 概念AWS CloudTrail 」を参照してください。

上記の例外として、以下の CloudTrail イベントは Audit Manager ではサポートされていません。

- kms_GenerateDataKey
- kms_Decrypt
- sts_AssumeRole
- kinesisvideo_GetDataEndpoint
- kinesisvideo_GetSignalingChannelEndpoint
- kinesisvideo_DescribeSignalingChannel
- kinesisvideo_DescribeStream

2023 年 5 月 11 日以降、Audit Manager は証拠収集のキーワードとして読み取り専用 CloudTrail イベントをサポートしなくなりました。合計3,135の読み取り専用キーワードを削除しました。顧客も AWS のサービス も API への読み取り呼び出しを行うため、読み取り専用イベントにはノイズが多くなります。その結果、読み取り専用キーワードによって、信頼性が低く、監査に適さない証拠が大量に収集されます。読み取り専用キーワードには`List`、、`Describe`、および `Get` API コール (Amazon S3 ListBucketsの場合は GetObjectおよび など) が含まれます。 Amazon S3 これらのキーワードのいずれかを証拠収集に使用していた場合、何もする必要はありません。これらのキーワードは Audit Manager コンソールと評価から自動的に削除されるため、これらのキーワードでは証拠は収集されなくなりました。

追加リソース

- このデータソースタイプの証拠収集に関する問題については、「」を参照してください私の評価では、 AWS CloudTrailからユーザーアクティビティの証拠が収集されていません。
- このデータソースタイプを使用してカスタムコントロールを作成するには、「」を参照してくださいでのカスタムコントロールの作成 AWS Audit Manager。
- カスタムコントロールを使用するカスタムフレームワークを作成するには、「」を参照してくださいでのカスタムフレームワークの作成 AWS Audit Manager。
- カスタムコントロールを既存のカスタムフレームワークに追加するには、「」を参照してくださいでのカスタムフレームワークの編集 AWS Audit Manager。

推奨設定 AWS Audit Manager を使用した のセットアップ

Audit Manager の使用を開始する前に、以下のセットアップタスクを完了することが重要です。

この章では、前提条件、アカウント設定、ユーザーアクセス許可、および推奨される機能と統合で Audit Manager を有効にして設定するために必要な手順について説明します。これらのタスクを完了すると、Audit Manager を使用する準備が整い、監査とコンプライアンスの作業の合理化を開始します。

目次

を設定するための前提条件 AWS Audit Manager

を使用する前に AWS Audit Manager、 AWS アカウント とユーザーのアクセス許可が適切に設定されていることを確認する必要があります。

このページでは、 AWS アカウント （ 必要に応じて) の作成、管理ユーザーの設定、Audit Manager へのアクセスと有効化に必要なアクセス許可の付与に必要な手順の概要を説明します。

タスク

1. にサインアップする AWS アカウント
2. 管理アクセスを持つユーザーを作成する
3. Audit Manager へのアクセスと有効化に必要な権限を追加する

> **Important**
>
> AWS と IAM を既にセットアップしている場合は、タスク 1 と 2 をスキップできます。ただし、タスク 3 を完了して、Audit Manager をセットアップするために必要なアクセス許可があることを確認する必要があります。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次のステップを実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセス IAM アイデンティティセンターディレクトリを設定するAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

Audit Manager へのアクセスと有効化に必要な権限を追加する

Audit Manager を有効にするには、ユーザーに必要なアクセス許可を付与する必要があります。Audit Manager へのフルアクセスを必要とするユーザーには、AWSAuditManagerAdministratorAccessマネージドポリシーを使用します。これは、 AWS で利用可能な マネージドポリシーであり AWS アカウント、Audit Manager 管理者に推奨されるポリシーです。

> **Tip**
>
> セキュリティのベストプラクティスとして、 管理ポリシーの使用を開始し、最小特権の AWS アクセス許可に移行することをお勧めします。 AWS 管理ポリシーは、多くの一般的なユースケースに対するアクセス許可を付与します。ただし、 AWS 管理ポリシーはすべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない可能性があることに注意してください。そのため、ユースケースに応じたカスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

アクセス権限を付与するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- のユーザーとグループ AWS IAM Identity Center：

アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。
- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。詳細については、「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

次のステップ

をセットアップ AWS アカウント し、必要なアクセス許可を付与したので、Audit Manager を有効にする準備が整いました。 step-by-step 手順については、「」を参照してくださいの有効化 AWS Audit Manager。

の有効化 AWS Audit Manager

Audit Manager の設定の前提条件を完了したので、 AWS 環境でサービスを有効にできます。

このページでは、Audit Manager コンソール、 (AWS CLI) 、 AWS Command Line Interface または Audit Manager API を使用して Audit Manager を有効にする方法について説明します。ニーズに最適な方法を選択し、対応する手順に従って Audit Manager を起動して実行します。

前提条件

で説明されているすべてのタスクを完了していることを確認してくださいを設定するための前提条件 AWS Audit Manager。

手順

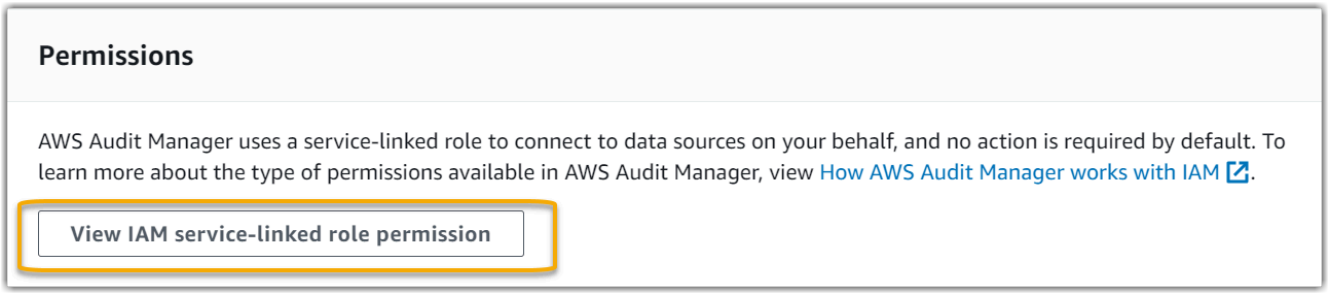
Audit Manager は、、Audit Manager API AWS Management Console、または AWS Command Line Interface () を使用して有効にできますAWS CLI。

Audit Manager console

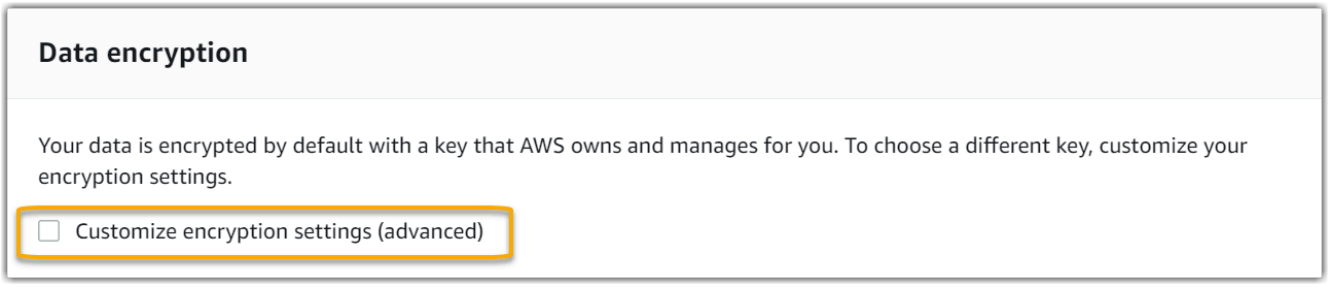
Audit Manager コンソールを使用してを有効にするには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. IAM アイデンティティの認証情報を使用してサインインします。
3. [Set up (セットアップ) AWS Audit Manager] を選択します。

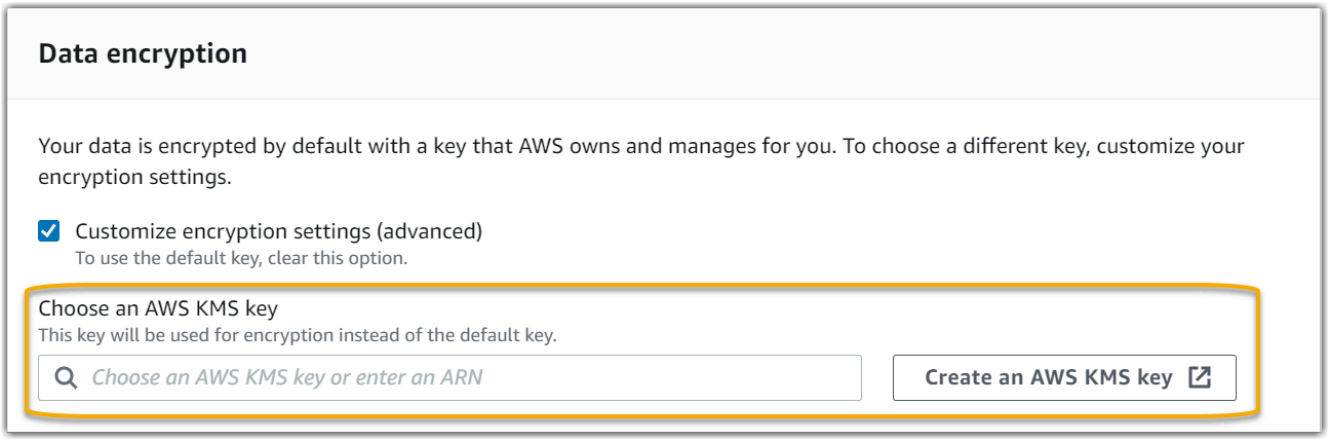
4. [許可] で、デフォルトではアクションは不要です。これは、Audit Manager がサービスリンクロールを使用して、ユーザーに代わってデータソースに接続するためです。必要に応じて、[IAM サービスリンクロールの許可を表示] を選択して、サービスにリンクされたロールを確認できます。



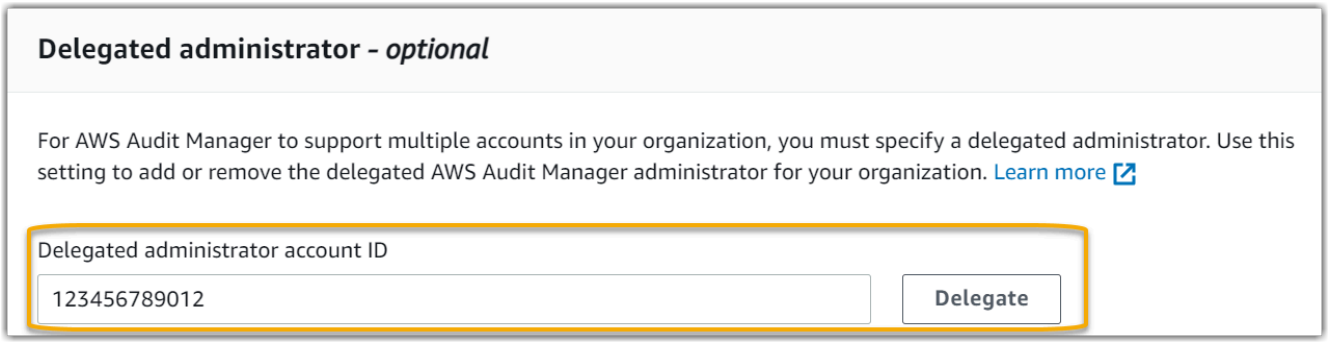
5. データ暗号化 では、Audit Manager がデータを安全に保存するための を作成および管理 AWS KMS key するためのデフォルトオプションが です。



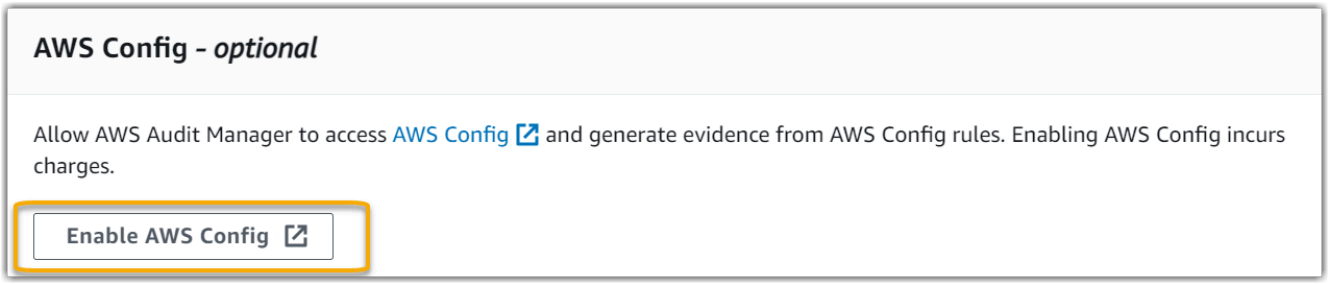
独自のカスタマーマネージドキーを使用して Audit Manager でデータを暗号化する場合は、[暗号化の設定をカスタマイズ (アドバンスト)] を選択します。その後、既存の KMS キーを選択するか、新しい KMS キーを作成できます。



6. (オプション) Audit Manager に複数のアカウントの評価を実行させる場合は、[委任された管理者 - オプション] で、委任された管理者アカウントを指定できます。詳細と推奨事項については、「有効化とセットアップ AWS Organizations （ オプション ）」を参照してください。

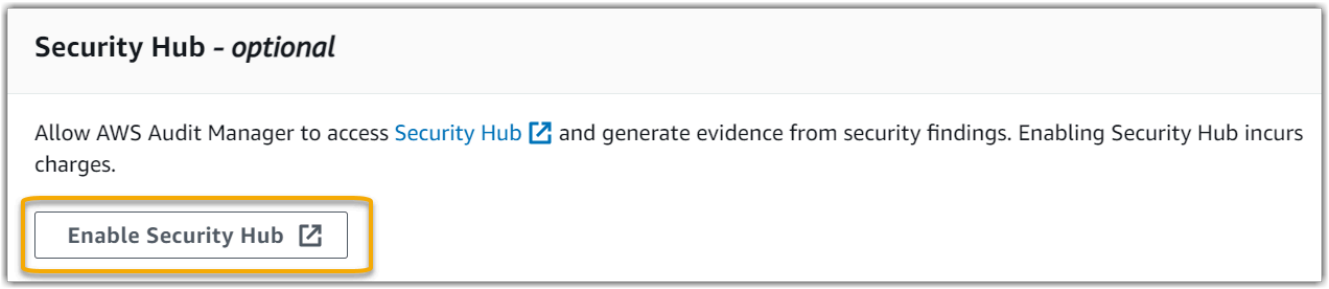


7. （ オプション) AWS Config - オプションの では、最適なエクスペリエンス AWS Config を実現するために を有効にすることをお勧めします。これにより、Audit Manager は AWS Config ルールを使用して証拠を生成できます。手順と推奨設定については、「」を参照してください有効化と設定 AWS Config (オプション)。



8. (オプション) [Security Hub - オプション]で、最適なエクスペリエンスを実現するために Security Hub を有効にすることをお勧めします。これにより、Audit Manager は Security

Hub チェックを使用して証拠を生成できます。手順と推奨設定については、「」を参照してください有効化と設定 AWS Security Hub (オプション)。



9. [Complete setup] (設定を完了) を選択して、設定プロセスを終了します。

AWS CLI

を使用して Audit Manager を有効にするには AWS CLI

コマンドラインで、以下の設定パラメータを使用して register-account コマンドを実行します。

- `--kms-key` (オプション) - このパラメータを使い、独自の顧客管理キーを使用して Audit Manager データを暗号化します。ここでオプションを指定しない場合、Audit Manager はユーザーに代わってデータを安全に保管するための AWS KMS key を作成および管理します。
- `--delegated-admin-account` (オプション) - このパラメータを使用して、Audit Manager のために 組織の委任された管理者アカウントを指定できます。ここでオプションを指定しない場合、委任管理者は登録されません。

入力例 (*###########*を独自の情報に置き換えてください):

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

出力例:

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

```
}
```

の詳細 AWS CLI と AWS CLI ツールのインストール手順については、「 AWS Command Line Interface ユーザーガイド」の以下を参照してください。

- AWS Command Line Interface ユーザーガイド
- のセットアップ AWS Command Line Interface

Audit Manager API

Audit Manager API を使用して Audit Manager を有効にするには

以下の設定パラメータを指定して RegisterAccountオペレーションを使用します。

- KMSkey (オプション) – このパラメータを使用して、独自の顧客管理キーを使用して Audit Manager データを暗号化します。ここでオプションを指定しない場合、Audit Manager はユーザーに代わってデータを安全に保管するための AWS KMS key を作成および管理します。
- delegatedAdminAccount (オプション) — このパラメータを使用して、Audit Manager の組織の委任管理者アカウントを指定します。指定しない場合、委任管理者は登録されません。

入力例 (############を独自の情報に置き換えてください):

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

出力例:

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

次のステップ

Audit Manager を有効にしたら、最適なエクスペリエンスを実現するために、いくつかの推奨機能と統合を設定することをお勧めします。詳細については、「の推奨機能 および AWS のサービス の有効化 AWS Audit Manager」を参照してください。

の推奨機能 および AWS のサービス の有効化 AWS Audit Manager

を有効にしたので AWS Audit Manager、サービスを最大限に活用するための推奨機能と統合をセットアップします。

重要ポイント

Audit Manager を最適に使用するには、次の機能を設定し、次の AWS のサービスを有効にすることをお勧めします。

タスク

- Audit Manager の推奨機能の設定
- 他の との推奨統合を設定する AWS のサービス
  - 有効化と設定 AWS Config (オプション)
  - 有効化と設定 AWS Security Hub (オプション)
  - 有効化とセットアップ AWS Organizations （ オプション ）

Audit Manager の推奨機能の設定

Audit Manager を有効にした後、エビデンスファインダー機能を有効にすることをお勧めします。

証拠ファインダー Audit Manager でエビデンスを検索する強力な方法を提供します。深くネストされたエビデンスフォルダをブラウズして探しているものを探す代わりに、エビデンスファインダーを使用してエビデンスをすばやく検索できます。委任された管理者として Evidence Manager を使用している場合は、組織内のすべてのメンバーアカウントで証拠を検索できます。

フィルターとグルーピングを組み合わせて使用することで、検索クエリの範囲を徐々に絞り込むことができます。例えば、システムの状態を大まかに把握したい場合は、広範囲にわたる検索を行い、評価、日付範囲、およびリソースコンプライアンスに基づいてフィルタリングします。特定のリソースを修復することが目的であれば、特定の統制 ID またはリソース ID の証拠を絞り込んで絞り込むこ

とができます。フィルターを定義したら、評価レポートを作成する前に、一致する検索結果をグループ化してプレビューできます。

他の との推奨統合を設定する AWS のサービス

Audit Manager で最適なエクスペリエンスを得るには、次の を有効にすることを強くお勧めします AWS のサービス。

- AWS Organizations – 組織を使用すると、複数のアカウントに対して Audit Manager の評価を実行し、委任された管理者アカウントに証拠を統合できます。
- AWS Security Hub および AWS Config – これらの を有効にすると AWS のサービス、Audit Manager 評価のコントロールのデータソースタイプとして使用できます。その後、Audit Manager はコンプライアンスチェックの結果をこれらのサービスから直接報告できます。

> **Important**
>
> AWS Config、Security Hub、および Organizations を有効にすることは、オプションの推奨事項です。ただし、これらのサービスを有効にする場合は、次の設定が必要です。

有効化と設定 AWS Config (オプション)

Audit Manager の多くのコントロールは、データソースタイプ AWS Config として を使用します。これらのコントロールをサポートするには、 AWS Config Audit Manager が有効になってい AWS リージョン る各 のすべてのアカウントで を有効にする必要があります。Audit Manager がデータソースタイプ AWS Config として を使用するコントロールの証拠を収集しようとし、関連する AWS Config ルールが有効になっていない場合、それらのコントロールの証拠は収集されません。

Audit Manager はお客様 AWS Config に代わって管理しません。以下の手順に従って設定 AWS Config を有効化および構成できます。

> **Important**
>
> 有効化はオプションの推奨事項 AWS Config です。ただし、有効にする場合は AWS Config、次の設定が必要です。

Audit Manager AWS Config と統合するタスク

- ステップ 1: を有効にする AWS Config
- ステップ 2: Audit Manager で使用する AWS Config 設定を構成する

ステップ 1: を有効にする AWS Config

AWS Config コンソールまたは API AWS Config を使用して を有効にできます。手順については、AWS Config デベロッパーガイドのAWS Configの開始方法を参照してください。

ステップ 2: Audit Manager で使用する AWS Config 設定を構成する

を有効にしたら AWS Config、監査に関連するコンプライアンス標準のAWS Config ルールも有効にするか、コンフォーマンスパックをデプロイしてください。この手順により、監査マネージャーが有効にした AWS Config ルールの検出結果を確実にインポートできるようになります。

AWS Config ルールを有効にしたら、そのルールのパラメータを確認することをお勧めします。次に、選択したコンプライアンスフレームワークの要件と照らし合わせてこれらのパラメータを検証する必要があります。必要に応じて、AWS Configでルールのパラメータを更新して、フレームワークの要件に合致するようにすることができます。これにより、評価によって特定のフレームワークに関する正しいコンプライアンスチェックの証拠が収集されるようになります。

例えば、CIS v1.2.0 の評価を作成するとします。このフレームワークには、1.4-アクセスキーが 90 日以内にローテーションされることを確認するコントロールがあります。では AWS Config、access-keys-rotatedルールにはデフォルト値が 90 日のmaxAccessKeyAgeパラメータがあります。その結果、このルールは統制要件と一致しています。デフォルト値を使用していない場合は、使用する値が CIS v1.2.0 の 90 日間の要件以上であることを確認してください。

各マネージドルールのデフォルトパラメータの詳細は、AWS Config ドキュメントに記載されています。ルールの設定方法については、「 AWS Config マネージドルールの使用」を参照してください。

有効化と設定 AWS Security Hub (オプション)

Audit Manager の多くのコントロールは、Security Hub をデータソースタイプとして使用しています。これらの制御をサポートするには、Audit Manager が有効になっている各リージョンのすべてのアカウントで Security Hub を有効にする必要があります。Audit Manager が Security Hub をデータソースタイプとして使用する統制の証拠を収集しようとしても、関連する Security Hub 標準が有効になっていない場合、それらの統制に関する証拠は収集されません。

Audit Manager は、ユーザーに代わって Security Hub を管理しません。以下の手順に従って Security Hub を有効にし、設定を構成できます。

> **Important**
>
> Security Hub を有効にすることはオプションの推奨事項です。ただし、Security Hub を有効にする場合は、次の設定が必要です。

Audit Manager AWS Security Hub と統合するタスク

- ステップ 1: を有効にする AWS Security Hub
- ステップ 2: Audit Manager で使用する Security Hub の設定を設定する
- ステップ 3: 組織の Organizations 設定を構成する

ステップ 1: を有効にする AWS Security Hub

Security Hub は、コンソールまたは API を使用して有効にすることができます。手順については、AWS Security Hub ユーザーガイドのタスク設定の構成 AWS Security Hubを参照してください。

ステップ 2: Audit Manager で使用する Security Hub の設定を設定する

Security Hub を有効にしたら、次も実行してください。

- リソース記録の有効化 AWS Config と設定 — Security Hub は、サービスにリンクされた AWS Config ルールを使用して、コントロールのセキュリティチェックのほとんどを実行します。これらのコントロールをサポートするには、有効な各標準で有効にしたコントロールに必要なリソースを記録するように、 を有効にして設定 AWS Config する必要があります。
- すべてのセキュリティ標準を有効にする – このステップにより、Audit Manager はサポートされているすべてのコンプライアンス標準の結果をインポートできます。
- Security Hub の [統合されたコントロールの検出結果] 設定を有効にする -この設定は、2023 年 2 月 23 日以降に Security Hub を有効にした場合、デフォルトで [有効] になっています。

> **Note**
>
> 統合された検出結果を有効にすると、Security Hub はセキュリティチェックごとに 1 つの結果を生成します (同じチェックが複数の標準で使用されている場合でも)。Security Hub 結果はそれぞれ、Audit Manager に 1 つの固有のリソース評価として収集されます。その結果、検出結果を統合すると、Audit Manager が Security Hub の検出結果に対して実施する固有リソース評価の合計が減少します。このため、統合された検出結果を使用すると、

多くの場合、Audit Manager の使用コストを削減できます。Security Hub をデータ ソース タイプとして使用する方法の詳細については、「AWS Security Hub でサポートされている コントロール AWS Audit Manager」を参照してください。Audit Manager の価格設定の詳細については、「AWS Audit Manager 料金」を参照してください。

ステップ 3: 組織の Organizations 設定を構成する

を使用して AWS Organizations おり、メンバーアカウントから Security Hub の証拠を収集する場合は、Security Hub で次の手順も実行する必要があります。

組織の Security Hub の設定を構成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. AWS Organizations 管理アカウントを使用して、アカウントを Security Hub の委任管理者として指定します。詳細については、AWS Security Hub ユーザーガイドの「Security Hub 管理者アカウントの指定」を参照してください。

   > **Note**
   >
   > Security Hub で指定する委任された管理者アカウントが、Audit Manager で指定したものと同じであることを確認してください。

3. Organizations の委任された管理者アカウントを使用して、設定、アカウントに移動し、すべてのアカウントを選択してから、[Auto-enroll] (自動登録) を選択してメンバーとして追加します。詳細については、AWS Security Hub ユーザーガイドの「組織からメンバーアカウントを有効にする」を参照してください。
4. 組織のすべてのメンバーアカウント AWS Config に対して を有効にします。詳細については、AWS Security Hub ユーザーガイドの「組織からメンバーアカウントを有効にする」を参照してください。
5. 組織のすべてのメンバーアカウントについて PCI DSS セキュリティ標準を有効にします。AWS CIS Foundations Benchmark 標準と AWS Foundational Best Practices 標準は、デフォルトで既に有効になっています。詳細については、AWS Security Hub ユーザーガイドの「セキュリティ標準の有効化」を参照してください。

有効化とセットアップ AWS Organizations （ オプション ）

Audit Manager は、 との統合を通じて複数のアカウントをサポートします AWS Organizations。Audit Manager は、複数のアカウントに対して評価を実行し、委任された管理者アカウントに証拠を統合できます。委任管理者は、組織を信頼ゾーンとして持つ Audit Manager リソースを作成および管理するための許可を持っています。管理アカウントのみが委任管理者を指定できます。

> **Important**
>
> 有効化はオプションの推奨事項 AWS Organizations です。ただし、 を有効にする場合は AWS Organizations、次の設定が必要です。

Audit Manager AWS Organizations と統合するタスク

- ステップ 1: 組織を作成または組織に参加する
- ステップ 2: 組織内のすべての機能を有効にする
- ステップ 3: Audit Manager の委任された管理者を指定する

ステップ 1: 組織を作成または組織に参加する

が組織に属していない場合 AWS アカウント は、組織を作成または参加できます。手順については、AWS Organizations ユーザーガイドの「組織の作成と管理」を参照してください。

ステップ 2: 組織内のすべての機能を有効にする

次に、組織内のすべての機能を有効にする必要があります。手順については、AWS Organizations ユーザーガイドの「組織内のすべての機能の有効化」を参照してください。

ステップ 3: Audit Manager の委任された管理者を指定する

組織管理アカウントを使用して Audit Manager を有効にしてから、委任された管理者を設定することをお勧めします。その後、委任された管理者アカウントを使用してログインし、評価を実行できます。ベストプラクティスとして、管理アカウントではなく、委任された管理者アカウントを使用してのみ評価を作成することをお勧めします。

Audit Manager を有効にした後に委任管理者を追加または変更するには、委任された管理者の追加「」および「」を参照してください委任管理者の変更。

次のステップ

推奨設定で Audit Manager をセットアップしたので、サービスの使用を開始する準備が整いました。

- 最初の評価を開始するには、「」を参照してください監査所有者向けチュートリアル: 評価の作成。
- 今後設定を更新するには、「」を参照してくださいAWS Audit Manager 設定の確認と設定。

の開始方法 AWS Audit Manager

このセクションの step-by-step チュートリアルでは、 を使用してタスクを実行する方法について説明します AWS Audit Manager。

> **Tip**
>
> 次のチュートリアルは、対象者別に分類されています。監査所有者または受任者としての役割に基づいて、適切なチュートリアルを選択してください。
>
> - 監査所有者は、評価の作成と管理を担当する Audit Manager のユーザーです。ビジネスの文脈では、監査所有者は、通常、ガバナンス、リスク管理、およびコンプライアンス (GRC) に精通しています。ただし、Audit Manager では、 SecOps または DevOps チームの個人が監査所有者のユーザーペルソナを引き受ける場合もあります。監査所有者は、特定のコントロールを確認し、証拠を検証するために、対象分野のエキスパート (受任者とも呼びます) にサポートを求めることができます。監査所有者には、評価を管理するために必要な許可が付与されている必要があります。
> - 受任者は、技術またはビジネスに関する専門知識を持つ対象分野のエキスパートです。これらの受任者は、Audit Manager の評価を所有または管理しませんが、それでも評価に貢献できます。受任者は、自らの専門分野に属するコントロールの証拠を検証するなどのタスクで監査所有者をサポートします。Audit Manager では、受任者の許可が制限されています。これは、監査所有者が委任するのが、評価全体ではなく、レビューする特定のコントロールセットであることによります。
>
> これらのペルソナおよびその他の Audit Manager の概念の詳細については、このガイドのAWS Audit Manager 概念と用語を理解する「」セクションdelegateのaudit owner「」および「」を参照してください。
> 各ペルソナに推奨される IAM 許可の詳細については、「 のユーザーペルソナに推奨されるポリシー AWS Audit Manager」を参照してください。

Audit Manager のチュートリアル

評価の作成

対象者: 監査所有者

概要: step-by-step 指示に従って最初の評価を作成し、すぐに起動して実行します。このチュートリアルでは、標準フレームワークを使用して評価を作成し、証拠の自動収集を開始する方法について説明します。

コントロールセットのレビュー

対象者: 受任者

概要: 自らの専門分野に属するコントロールの証拠をレビューすることを通じて、監査所有者をサポートします。コントロールセットとその関連証拠の確認、コメントの追加、証拠のアップロード、コントロールのステータスの更新について説明します。

監査所有者向けチュートリアル: 評価の作成

このチュートリアルでは、 の概要を説明します AWS Audit Manager。このチュートリアルでは、 を使用して評価を作成しますAWS Audit Manager サンプルフレームワーク。評価を作成して、そのフレームワークのコントロールに関する自動証拠収集の継続プロセスを開始します。

> **Note**
>
> AWS Audit Manager は、特定のコンプライアンスフレームワークおよび規制への準拠の検証に関連する証拠の収集を支援します。ただし、コンプライアンス自体を評価するものではありません。 AWS Audit Manager したがって、 によって収集された証拠には、監査に必要な AWS 使用状況に関するすべての情報が含まれていない場合があります。 AWS Audit Manager は、法律顧問やコンプライアンスの専門家に代わるものではありません。

前提条件

このチュートリアルを開始する前に、次の条件を満たしていることを確認してください。

- 推奨設定 AWS Audit Manager を使用した のセットアップ で説明されているすべての前提条件を満たしたこと。このチュートリアルを完了するには、 AWS アカウント と AWS Audit Manager コンソールを使用する必要があります。
- IAM アイデンティティには、 AWS Audit Managerで評価を作成および管理するための適切な許可が付与されます。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

- Audit Manager の用語と機能に精通していること。一般的な概要については、「とは AWS Audit Manager」および「AWS Audit Manager 概念と用語を理解する」を参照してください。

手順

タスク

- ステップ 1: 評価の詳細を指定する
- ステップ 2: 範囲内 AWS アカウント で を指定する
- ステップ 3: 監査所有者を指定する
- ステップ 4: 確認して作成する

ステップ 1: 評価の詳細を指定する

最初のステップでは、フレームワークを選択して、評価に関する基本的な情報を入力します。

評価の詳細を指定するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. [Launch] AWS Audit Manager (起動する) を選択します。
3. 画面上部の緑色のバナーで、フレームワーク で開始 を選択します。
4. 必要なフレームワークを選択してから、[Create assessment from framework (フレームワークから評価を作成)] を選択します。このチュートリアルでは、AWS Audit Manager サンプルフレームワーク を使用します。
5. [Assessment name (評価の名前)] で、評価の名前を入力します。
6. (オプション) [Assessment description (評価の説明)] で、評価の説明を入力します。
7. 評価レポートの宛先 で、評価レポートを保存する S3 バケットを選択します。
8. フレームワーク で、AWS Audit Manager サンプルフレームワークが選択されていることを確認します。
9. (オプション) タグ で、新しいタグを追加 を選択してタグを評価に関連付けます。タグごとにキーと値を指定できます。タグキーは必須であり、この評価を検索するときに検索条件として使用できます。
10. [次へ] をクリックします。

ステップ 2: 範囲内 AWS アカウント で を指定する

次に、評価の範囲に含める AWS アカウントを指定します。

AWS Audit Manager は と統合されているため AWS Organizations、複数のアカウントで Audit Manager の評価を実行し、証拠を委任された管理者アカウントに統合できます。Audit Manager で組織を有効にするには (まだ有効にしていない場合)、このガイドの設定のページで「有効化とセットアップ AWS Organizations （ オプション ）」を参照してください。

> **Note**
>
> Audit Manager は、評価の範囲内で最大 200 のアカウントをサポートできます。200 を超えるアカウントを含めると、評価の作成が失敗する可能性があります。

範囲内のアカウントを指定するには

1. でAWS アカウント、評価の範囲 AWS アカウント に含める を選択します。
   - Audit Manager で Organizations を有効にした場合、複数のアカウントが一覧表示されます。
   - Audit Manager で Organizations を有効にしなかった場合は、現在の アカウントのみが一覧表示されます。
2. [次へ] をクリックします。

ステップ 3: 監査所有者を指定する

このステップでは、評価の監査所有者を指定します。監査所有者とは、通常 GRC の職場にいる個人 SecOps、または Audit Manager の評価の管理を担当する DevOps チームのことです。AWSAuditManagerAdministratorAccess ポリシーを使用することをお勧めします。

監査所有者を指定するには

1. [Audit owners] (監査所有者) で、評価のための監査所有者を選択します。追加の監査所有者を検索するには、検索バーを使用して名前または で検索します AWS アカウント。
2. [次へ] をクリックします。

ステップ 4: 確認して作成する

評価に関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。完了したら、評価の作成を選択して、証拠の継続的な収集を開始します。

評価を作成した後、評価ステータスを [inactive (非アクティブ)] に変更するまで、証拠の収集が続行されます。または、コントロールのステータスを [inactive (非アクティブ)] に変更することで、特定のコントロールの証拠収集を停止できます。

> **Note**
>
> 自動証拠は、評価を作成してから 24 時間後に利用できます。Audit Manager は複数のデータソースから証拠を自動的に収集し、その証拠収集の頻度は証拠の種類に基づきます。詳細については、このガイドの「証拠収集の頻度」を参照してください。

追加リソース

このチュートリアルで概説する概念とツールについて、さらに学習を深めることをお勧めします。学習を深めるには、次のリソースをご利用ください。

- での評価の詳細の確認 AWS Audit Manager – 評価の詳細ページを紹介します。このページでは、評価のさまざまなコンポーネントを確認できます。
- での評価の管理 AWS Audit Manager – このチュートリアルに基づいて構築され、評価を管理するための概念とタスクに関する詳細情報を提供します。この章では、特に以下のトピックを確認することをお勧めします。
  - 別のフレームワークから評価を作成する方法
  - 評価で証拠を確認し、評価レポートを生成する方法
  - 評価のステータスを変更する方法または評価を削除する方法
- フレームワークライブラリを使用して でフレームワークを管理する AWS Audit Manager – フレームワークライブラリについて概説し、独自かつ特定のコンプライアンスニーズに合わせてカスタムフレームワークを作成する方法を説明します。
- コントロールライブラリを使用して でコントロールを管理する AWS Audit Manager – コントロールライブラリについて概説し、カスタムフレームワークで使用するカスタムコントロールを作成する方法を説明します。

- AWS Audit Manager 概念と用語を理解する – Audit Manager で使用される概念と用語の定義を提供します。
- 〔動画] を使用して証拠を収集し、監査データを管理する AWS Audit Manager – このチュートリアルで説明されている評価作成プロセスと、コントロールの確認や評価レポートの生成などのその他のタスクを示します。

受任者向けチュートリアル: コントロールセットの確認

このチュートリアルでは、 AWS Audit Managerで監査所有者によって共有されたコントロールセットをレビューする方法について説明します。

監査所有者は、Audit Manager を使用して評価を作成し、その評価のコントロールの証拠を収集します。コントロールセットの証拠を検証する際に、監査所有者に疑問が生じたり、監査所有者がサポートを必要としたりする場合があります。このような場合、監査所有者は、レビューのために対象分野のエキスパートにコントロールセットを委任できます。

受任者は、自らの専門分野に属するコントロールについて収集された証拠を監査所有者がレビューするのをサポートします。

前提条件

このチュートリアルを開始する前に、次の条件を満たしていることを確認してください。

- AWS アカウント がセットアップされます。このチュートリアルを完了するには、 AWS アカウント と Audit Manager コンソールの両方を使用する必要があります。詳細については、「推奨設定 AWS Audit Manager を使用した のセットアップ」を参照してください。
- Audit Manager の用語と機能に精通していること。Audit Manager の一般的な概要については、「とは AWS Audit Manager」および「AWS Audit Manager 概念と用語を理解する」を参照してください。

手順

タスク

- ステップ 1: 通知を確認する
- ステップ 2: コントロールセットと関連する証拠をレビューする
- ステップ 3。手動証拠を追加する (オプション)

- ステップ 4。コントロールのコメントを追加する (オプション)
- ステップ 5: コントロールを [reviewed(レビュー済み)] としてマークする (オプション)
- ステップ 6。レビュー済みコントロールセットを監査所有者に送信する

ステップ 1: 通知を確認する

まず、Audit Manager にサインインして通知にアクセスし、レビューのために委任されたコントロールセットを確認できます。

通知を確認するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Notifications (通知)] を選択します。
3. [Notifications (通知)] ページで、自分に委任されたコントロールセットのリストを確認します。通知の表には、次の情報が含まれます。

名前	説明
日付	コントロールセットが委任された日付。
[評価]	コントロールセットに関連付けられている評価の名前。評価の名前を選択して、評価の詳細のページを開くことができます。
コントロールセット	レビューのために委任されたコントロールセットの名前。
ソース	コントロールセットを委任したユーザーまたはロール。
説明	監査所有者から提供されたレビュー手順。

> **Tip**
>
> また、SNS トピックをサブスクライブして、レビューのためにコントロールセットが割り当てられたときに E メールによるアラートを受信することもできます。詳細については、「の通知 AWS Audit Manager」を参照してください。

ステップ 2: コントロールセットと関連する証拠をレビューする

次のステップでは、監査所有者から委任されたコントロールセットをレビューします。コントロールとその証拠を調べることにより、コントロールについて追加のアクションが必要かどうかを判断できます。その他のアクションには、コンプライアンスを実証するための追加の証拠を手動でアップロードしたり、そのコントロールに関するコメントを残したりすることが含まれます。

コントロールセットをレビューするには

1. [Notifications] (通知) ページから、自分に委任されたコントロールセットのリストを確認します。その後、レビュー対象を特定し、関連する評価の名前を選択します。
2. 評価の詳細のページの [Controls (コントロール)] タブで、[Control sets (コントロールセット)] の表が表示されるまで下方向にスクロールします。
3. [Controls grouped by control set (コントロールセット別にグループ化されたコントロール)] の列で、コントロールセットの名前を展開して、そのコントロールを表示します。その後、コントロールの名前を選択して、コントロールの詳細のページを開きます。
4. (オプション) コントロールのステータスを変更するには、[Update control status (コントロールのステータスを更新)] を選択します。レビューの進行中に、ステータスを「レビュー中」としてマークできます。
5. 証拠フォルダ 、詳細 、証拠ソース 、コメント 、変更ログ タブでコントロールに関する情報を確認します。 これらの各タブと、タブに含まれるデータを理解する方法については、「」を参照してくださいでの評価コントロールの確認 AWS Audit Manager。

コントロールの証拠をレビューするには

1. コントロールの詳細のページから、[Evidence folders (証拠フォルダ)] タブを選択します。
2. 証拠フォルダの表に移動します。この表には、そのコントロールの証拠を含むフォルダのリストが表示されます。これらのフォルダは、そのフォルダ内の証拠が収集された日付に基づいて編成され、名前が付けられます。
3. 証拠フォルダの名前を選択して開きます。ここから、その日に収集されたすべての証拠の概要を確認できます。この情報については、「」を参照してくださいでの証拠フォルダの確認 AWS Audit Manager。
4. 証拠フォルダの概要のページから、証拠の表に移動します。[Time (時間)] 列で、その時点で収集された証拠を開いてその詳細をレビューする項目を選択します。この情報については、「」を参照してくださいでの証拠の確認 AWS Audit Manager。

ステップ 3。手動証拠を追加する (オプション)

は多くのコントロールの証拠 AWS Audit Manager を自動的に収集しますが、場合によっては追加の証拠を提供する必要がある場合があります。このような場合は、そのコントロールへの準拠を示すのに役立つ独自の証拠を手動で追加できます。

コントロールに手動証拠を追加するには

手動証拠をコントロールに追加する方法はいくつかあります。Amazon S3 からファイルをインポートしたり、ブラウザからファイルをアップロードしたり、テキストレスポンスを入力したりできます。各メソッドの手順については、「」を参照してください[での手動証拠の追加 AWS Audit Manager](#)。

ステップ 4。コントロールのコメントを追加する (オプション)

レビューしたコントロールにコメントを追加できます。監査所有者は、これらのコメントを確認できます。例えば、コメントを残してステータスについての最新情報を提供し、そのコントロールに関する問題を是正したことを確認できます。

コントロールにコメントを追加するには

1. [Notifications] (通知) ページから、自分に委任されたコントロールセットのリストを確認します。コメントを残すコントロールセットを見つけて、関連する評価の名前を選択します。
2. [Controls (コントロール)] タブを選択し、[Control sets (コントロールセット)] の表が表示されるまでスクロールダウンして、コントロールの名前を選択して開きます。
3. [Comments (コメント)] タブを選択します。
4. [Send comments (コメントを送信)] で、テキストボックスにコメントを入力します。
5. コメントの送信 を選択してコメントを追加します。これで、このコントロールに関する他のコメントとともに、ページの [Previous comments (以前のコメント)] のセクションにコメントが表示されます。

ステップ 5: コントロールを [reviewed(レビュー済み)] としてマークする (オプション)

コントロールのステータスの変更はオプションです。しかし、そのコントロールのレビューを完了する際には、各コントロールのステータスを [Reviewed (レビュー済み)] に変更することをお勧めします。個々のコントロールのステータスにかかわらず、監査所有者にコントロールを送信できます。

コントロールを [reviewed (レビュー済み)] としてマークするには

1. [Notifications (通知)] ページから、自分に委任されたコントロールセットのリストを確認します。レビュー済みとしてマークするコントロールを含むコントロールセットを見つけます。その後、関連する評価の名前を選択して、評価の詳細のページを開きます。
2. 評価の詳細のページの [Controls (コントロール)] タブで、[Control sets (コントロールセット)] の表が表示されるまでスクロールダウンします。
3. [Controls grouped by control set (コントロールセット別にグループ化されたコントロール)] の列で、コントロールセットの名前を展開して、そのコントロールを表示します。コントロールの名前を選択して、コントロールの詳細のページを開きます。
4. [Update control status (コントロールのステータスを更新)] を選択し、ステータスを [Reviewed(レビュー済み)] に変更します。
5. 表示されるポップアップウィンドウで、[Update control status (コントロールのステータスを更新)] を選択して、コントロールのレビューが終了したことを確認します。

ステップ 6。レビュー済みコントロールセットを監査所有者に送信する

すべてのコントロールのレビューが完了したら、コントロールセットを監査所有者に送信して、レビューが完了したことを監査所有者に知らせます。

レビュー済みコントロールセットを監査所有者に送信するには

1. [Notifications (通知)] ページで、自分に割り当てられたコントロールセットのリストを確認します。監査所有者に送信するコントロールセットを見つけて、関連する評価の名前を選択します。
2. [Control sets (コントロールセット)] の表が表示されるまでスクロールダウンし、監査所有者に送信するコントロールセットを選択してから、[Submit for review (レビュー用に送信)] を選択します。
3. 表示されるポップアップウィンドウで、[Submit for review (レビュー用に送信)] を選択する前に、そのコントロールセットに関する概要レベルのコメントを追加できます。

コントロールを監査所有者に送信すると、監査所有者は残されたコメントを表示できます。

追加リソース

このチュートリアルで紹介されている概念については、引き続き詳細をご覧いただけます。推奨されるリソースは次のとおりです。

- での評価の詳細の確認 AWS Audit Manager - Audit Manager 評価のさまざまなコンポーネントを詳しく知ることができる評価の詳細ページを紹介します。
- での評価コントロールの確認 AWS Audit Manager および での証拠の確認 AWS Audit Manager - 評価のコントロールと証拠を理解するのに役立つ定義を提供します。
- AWS Audit Manager 概念と用語を理解する – Audit Manager で使用される概念と用語の定義を提供します。

Audit Manager ダッシュボードの使用

Audit Manager ダッシュボードを使用すると、アクティブな評価で非準拠の証拠を視覚化できます。これを使用することで、簡便かつ迅速に、評価をモニタリングしたり、最新情報を入手したり、問題をプロアクティブに是正したりできます。デフォルトでは、ダッシュボードは、すべてのアクティブな評価のトップダウンの集約ビューを提供します。このビューを使用すると、最初に膨大な量の個々の証拠をふるいにかけることなく、評価の問題を視覚的に特定できます。

ダッシュボードは、Audit Manager コンソールにサインインしたときに最初に表示される画面です。これには、最も関連性の高いデータと重要業績評価指標 (KPI) を表示する 2 つのウィジェットが含まれています。評価フィルターを使用すると、このデータを絞り込んで、特定の評価の KPI に焦点を当てることができます。そこから、コントロールドメインのグループを確認して、どのコントロールに非準拠の証拠が最も多くあるかを特定できます。その後、基礎となるコントロールを詳しく確認し、問題を調査して是正できます。

> **Note**
>
> 初めて Audit Manager を使用する場合、またはアクティブな評価がない場合、ダッシュボードにデータは表示されません。使用を開始するには、評価を作成します。これにより、継続的な証拠の収集が開始されます。24 時間後から、集約された証拠データがダッシュボードに表示され始めます。次のセクションを読んで、このデータを理解して解釈する方法を学ぶことができます。

このページでは、次のトピックについて説明します。

トピック

ダッシュボードの概念と用語

このセクションでは、Audit Manager ダッシュボードの使用を開始する前に知っておくべき重要事項について説明します。

許可と可視性

監査所有者と受任者は両方ともダッシュボードにアクセスできます。つまり、これらのペルソナの両方が、 のすべてのアクティブな評価のメトリクスと集計を表示できます AWS アカウント。同じ情報にアクセスできることで、チーム全員が同じ KPI と目標に集中できるようになります。

フィルター

Audit Manager は、ダッシュボード上のすべてのウィジェットに適用できるページレベルの the section called “評価フィルター” を提供します。

非準拠の証拠

ダッシュボードは、[non-compliant] (非準拠) と結論付けられたコンプライアンスチェックの証拠がある評価のコントロールを強調表示します。コンプライアンスチェックの証拠は、データソースタイプ AWS Security Hub として AWS Config または を使用するコントロールに関連しています。この証拠タイプについては、Audit Manager は、これらのサービスから直接コンプライアンスチェックの結果をレポートします。Security Hub が [Fail] (失敗) の結果をレポートした場合、または AWS Config が [Non-compliant] (非準拠) の結果をレポートした場合、Audit Manager は、該当の証拠を非準拠として分類します。

未判断の証拠

コンプライアンスチェックが利用できない、または適用できない場合、証拠は未判断となります。その結果、コンプライアンス評価を実行できません。これは、コントロールがデータソースタイプ AWS Security Hub として AWS Config または を使用しているが、それらのサービスを有効にしていない場合に当てはまります。これは、手動証拠、 AWS API コール、 などのコンプライアンスチェックをサポートしていないデータソースタイプをコントロールが使用する場合にも当てはまります AWS CloudTrail。

証拠のコンプライアンスチェックのステータスがコンソールで [not applicable] (該当なし) となっている場合、ダッシュボードでは [inconclusive] (未判断) として分類されます。

準拠の証拠

コンプライアンスチェックで問題が報告されなかった場合、証拠は [compliant] (準拠) です。これは、Security Hub が合格結果を報告した場合、または準拠結果を AWS Config 報告した場合も同様です。

コントロールドメイン

ダッシュボードには、コントロールドメインの概念が導入されています。コントロールドメインは、特定のフレームワークに固有ではないコントロールの一般的なカテゴリと考えることができます。コントロールドメインのグループ化は、ダッシュボードの最も強力な機能の 1 つで

す。Audit Manager は、非準拠の証拠がある評価のコントロールを強調表示し、コントロールドメインごとにグループ化します。この機能を使用することで、監査に向けて準備する際に、特定の対象ドメインの是正に集中的に取り組むことができます。

> **Note**
>
> コントロールドメインは、コントロールセットとは異なります。コントロールセットは、フレームワーク固有のコントロールのグループであり、通常は規制機関によって定義されます。例えば、PCI DSS フレームワークには、[Requirement 8: Identify and authenticate access to system components] (要件 8: システムコンポーネントへのアクセスを識別および認証する) という名前のコントロールセットがあります。このコントロールセットは、Identity and Access Management のコントロールドメインに分類されます。

データの結果整合性

ダッシュボードデータには結果整合性があります。つまり、ダッシュボードからデータを読み取るときに、最近完了した書き込みまたは更新操作の結果がすぐに反映されない場合があります。数時間が経過してから再度確認すると、ダッシュボードには最新のデータが反映されているはずです。

削除された評価および非アクティブな評価のデータ

ダッシュボードには、アクティブな評価のデータが表示されます。ダッシュボードを表示した同じ日に評価を削除するか、ステータスを非アクティブに変更すると、その評価のために含まれるデータは次のように含まれます。

- [Inactive assessments] (非アクティブな評価) – 非アクティブに変更する前に Audit Manager が評価のために証拠を収集した場合、その証拠データはその日のダッシュボードカウントに含まれます。
- [Deleted assessments] (削除された評価) – 削除前に Audit Manager が評価のために証拠を収集した場合、その証拠データはその日のダッシュボードカウントに含まれません。

ダッシュボードの要素

次のセクションでは、ダッシュボードのさまざまなコンポーネントについて説明します。

トピック

- 日次スナップショット
- コントロールドメイン別にグループ化された非準拠の証拠を持つコントロール

評価フィルター

評価フィルターを使用して、特定のアクティブな評価に焦点を当てることができます。

デフォルトでは、ダッシュボードにはすべてのアクティブな評価についての集計データが表示されます。特定の評価のデータを表示するには、評価フィルターを適用します。これは、ダッシュボード上のすべてのウィジェットに適用されるページレベルのフィルターです。

評価フィルターを適用するには、ダッシュボードの上部にあるドロップダウンリストから評価を選択します。このリストには、最大 10 個のアクティブな評価が表示されます。最近作成された評価が最初に表示されます。アクティブな評価が多数ある場合は、評価の名前を入力することで、目的の評価をすぐに見つけることができます。評価を選択すると、ダッシュボードにはその評価のデータのみが表示されます。

日次スナップショット

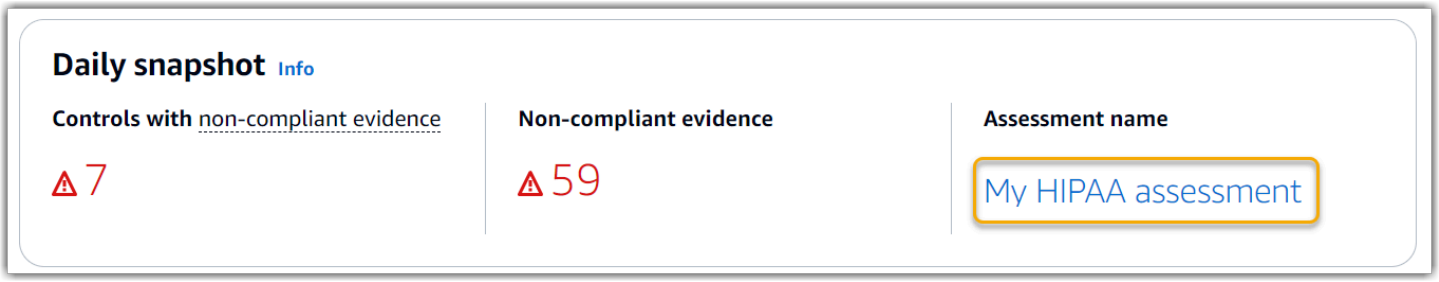
このウィジェットは、アクティブな評価に関する現在のコンプライアンスのステータスのスナップショットを表示します。

日次スナップショットは、ダッシュボードの上部にある日付に収集された最新のデータを反映しています。ダッシュボードの日付と時刻は協定世界時 (UTC) です。これらの数値は、このタイムスタンプに基づく 1 日あたりのカウントであることを理解することが重要です。現在までの合計ではありません。

デフォルトでは、日次スナップショットは、すべてのアクティブな評価について次のデータを表示します。

1. Controls with non-compliant evidence (非準拠の証拠を持つコントロール) - 非準拠の証拠に関連付けられているコントロールの総数。
2. 非準拠の証拠 - 非準拠の結果を含むコンプライアンスチェックの証拠の合計量。
3. Active assessments (アクティブな評価) - アクティブな評価の総数。これらの評価へのリンクを表示するには、この番号を選択してください。

日次スナップショットデータは、適用した the section called “評価フィルター” に基づいて変更されます。評価を指定すると、データにはその評価の 1 日あたりのカウントのみが反映されます。この場合、日次スナップショットには、指定した評価の名前が表示されます。評価を開くには、その名前を選択できます。

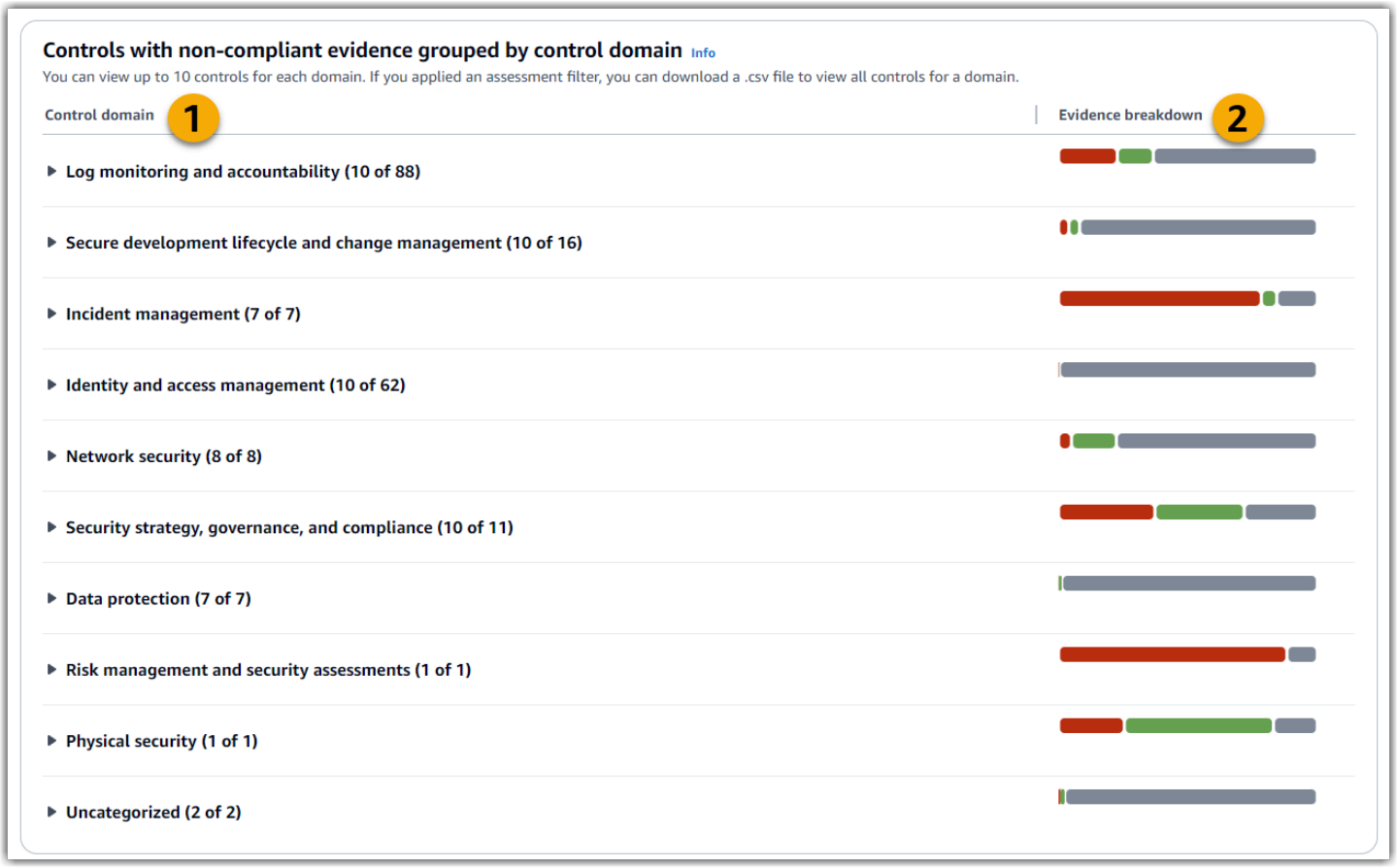


コントロールドメイン別にグループ化された非準拠の証拠を持つコントロール

このウィジェットを使用して、どのコントロールに非準拠の証拠が最も多くあるかを特定できます。

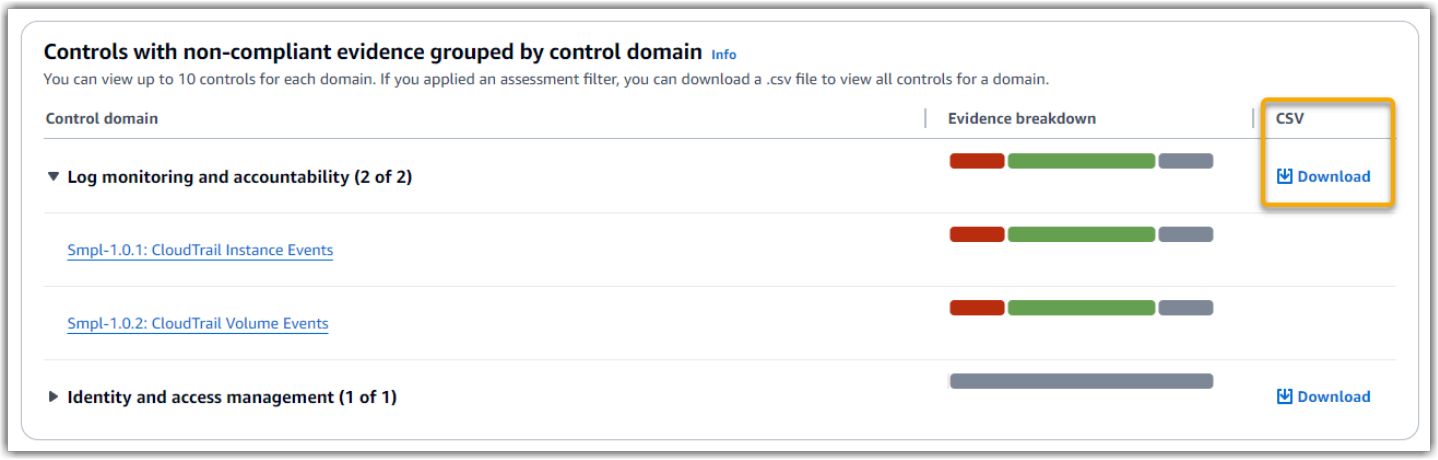
デフォルトでは、ウィジェットは、すべてのアクティブな評価について次のデータを表示します。

1. Control domain (コントロールドメイン) – アクティブな評価に関連付けられている control domains のリスト。
2. [Evidence breakdown] (証拠の内訳) – 証拠のコンプライアンスステータスの内訳を示す棒グラフ。



コントロールドメインを展開するには、名前の横にある矢印を選択します。展開すると、コンソールは、各ドメインについて最大 10 個のコントロールを表示します。これらのコントロールは、非準拠の証拠の総数が多い順にランク付けされます。

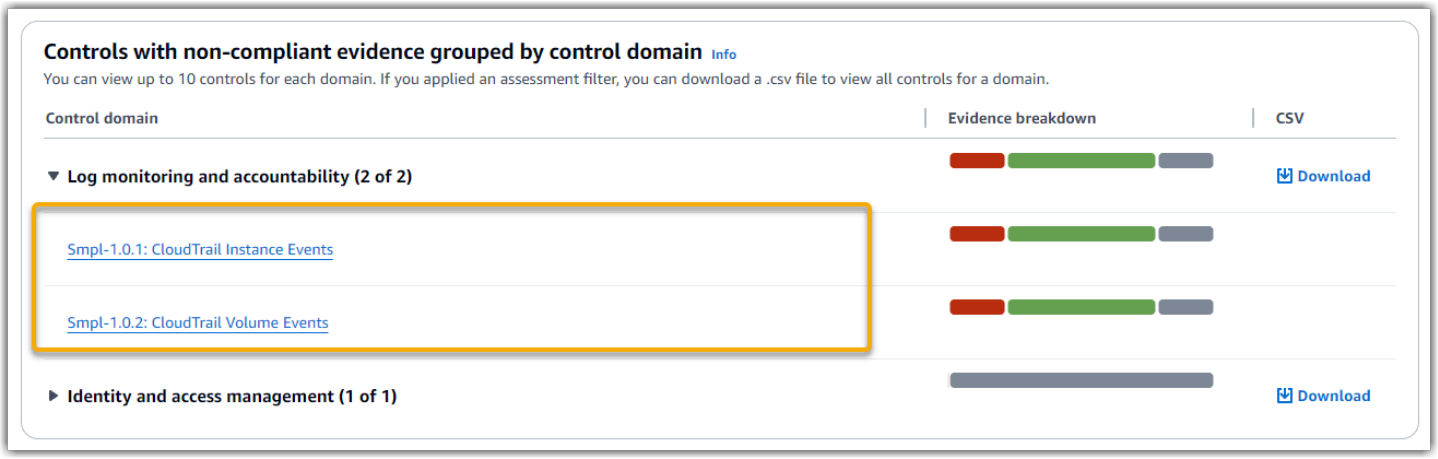
このウィジェットのデータは、適用する the section called “評価フィルター” に基づいて変化します。評価を指定すると、その評価のデータのみが表示されます。さらに、評価で使用可能なコントロールドメインごとに CSV ファイルをダウンロードすることもできます。



.csv ファイルには、非準拠の証拠に関連付けられているドメイン内のコントロールの詳細なリストが含まれています。次の例は、架空の値を持つ CSV データ列を示しています。

	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							

最後に、評価フィルターを適用すると、各ドメインの下のコントロール名にハイパーリンクが設定されます。任意のコントロールを選択して、指定した評価のコントロールの詳細のページを開きます。



Tip

コントロールの詳細のページを開始点として使用すると、ある詳細レベルから次の詳細レベルに移動できます。

1. コントロールの詳細ページ - このページでは、Audit Manager がそのコントロールのために収集した証拠の日次フォルダが証拠フォルダタブ一覧表示されます。詳細については、フォルダを選択してください。
2. 証拠フォルダ - 次に、 証拠フォルダの概要とそのフォルダ内の証拠のリストを確認できます。詳細については、個々の証拠項目を選択してください。
3. 個々の証拠 - 最後に、個々の証拠の詳細を詳しく確認できます。これは、最も詳細なレベルの証拠データです。

次のステップ

ダッシュボードを確認した後に実行できる次の手順は以下のとおりです。

- CSV ファイルのダウンロード – 焦点を当てる評価およびコントロールドメインを検索し、非準拠の証拠を含む関連コントロールの完全なリストをダウンロードします。
- コントロールをレビューする – 是正が必要なコントロールを特定したら、コントロールをレビューできます。
- レビューのためにコントロールを委任する – コントロールのレビューについてサポートが必要な場合は、レビューのためにコントロールセットを委任できます。
- 評価を編集する – アクティブな評価の範囲を変更する場合は、評価を編集できます。
- 評価のステータスを更新する – 評価の証拠の収集を停止する場合は、評価ステータスを非アクティブな に変更できます。

追加リソース

一般的な質問や問題に対する回答を見つけるには、このガイドダッシュボードに関する問題のトラブルシューティングのトラブルシューティングセクションの「」を参照してください。

での評価の管理 AWS Audit Manager

Audit Manager の評価は、コントロールのグループ化であるフレームワークに基づいています。フレームワークを開始点として使用して、そのフレームワークのコントロールについての証拠を収集する評価を作成できます。評価では、監査の範囲を定義することもできます。これには、証拠 AWS アカウント を収集する の指定が含まれます。

重要ポイント

フレームワークから評価を作成できます。どちらの場合も、Audit Manager が提供する標準フレームワークを使用できます。または、自分で構築したカスタムフレームワークから評価を作成することもできます。標準フレームワークには、特定のコンプライアンス標準または規制をサポートする構築済みのコントロールセットが含まれています。対照的に、カスタムフレームワークには、独自の要件に応じてカスタマイズおよびグループ化できるコントロールが含まれています。

評価を作成すると、継続的な証拠の収集が開始されます。監査の時期になると、ユーザーまたは代理人はこの証拠を確認してから、評価レポートに追加できます。

> **Note**
>
> AWS Audit Manager は、特定のコンプライアンス標準および規制への準拠の検証に関連する証拠の収集を支援します。ただし、コンプライアンス自体を評価するものではありません。AWS Audit Manager したがって、 によって収集された証拠には、監査に必要な AWS 使用状況に関するすべての情報が含まれていない場合があります。 AWS Audit Manager は、法律顧問やコンプライアンスの専門家に代わるものではありません。

追加リソース

Audit Manager で評価を作成および管理するには、ここで概説されている手順に従ってください。

- での評価の作成 AWS Audit Manager
- での評価の検索 AWS Audit Manager
- での評価の確認 AWS Audit Manager
  - での評価の詳細の確認 AWS Audit Manager

での評価の作成 AWS Audit Manager

このトピックは に基づいて構築されています監査所有者向けチュートリアル: 評価の作成。このページには、フレームワークから評価を作成する方法を示す詳細な手順が記載されています。次の手順に従って評価を作成し、継続的な証拠の収集を開始します。

前提条件

このチュートリアルを開始する前に、次の条件を満たしていることを確認してください。

- 推奨設定 AWS Audit Manager を使用した のセットアップ で説明されているすべての前提条件を満たしたこと。このチュートリアルを完了するには、 と Audit Manager コンソールを使用する必要があります AWS アカウント 。
- IAM アイデンティティには、Audit Manager で評価を作成および管理するための適切なアクセス許可があります。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

タスク

- ステップ 1: 評価の詳細を指定する
- ステップ 2: 範囲内 AWS アカウント で を指定する
- ステップ 3: 監査所有者を指定する
- ステップ 4: 確認して作成する

ステップ 1: 評価の詳細を指定する

フレームワークを選択し、評価のための基本的な情報を提供することから始めます。

評価の詳細を指定するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Assessments] (評価)、[Create assessment] (評価を作成) の順に選択します。
3. 名前 に、評価の名前を入力します。
4. (オプション) 説明 に、評価の説明を入力します。
5. 評価レポートの宛先 で、評価レポートを保存する S3 バケットを選択します。

> **Tip**
>
> 評価レポートのデフォルトの送信先は、評価設定 に基づいています。必要に応じて、複数の S3 バケットを作成して使用して、さまざまな評価の評価レポートを整理できます。

6. 「フレームワークの選択」で、評価を作成するフレームワークを選択します。検索バーを使用して、名前、またはコンプライアンス標準や規制によってフレームワークを検索することもできます。

> **Tip**
>
> フレームワークの詳細については、フレームワーク名を選択してフレームワークの詳細ページを参照してください。

7. (オプション) タグ で、新しいタグを追加 を選択してタグを評価に関連付けます。タグごとにキーと値を指定できます。タグキーは必須であり、この評価を検索するときに検索条件として使用できます。
8. [次へ] をクリックします。

> **Note**
>
> 評価が指定したフレームワークの正しいエビデンスを収集していることを確認することが重要です。証拠収集を開始する前に、選択したフレームワークの要件を確認することをお勧めします。次に、現在の AWS Config ルールパラメータに対してこれらの要件を検証します。ルールパラメータがフレームワークの要件と一致していることを確認するために、AWS Config でルールを更新できます。
> 例えば、CIS v1.2.0 の評価を作成するとします。このフレームワークには 1.9 - IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認と命名されたコントロールがあります。では AWS Config、iam-password-policyルールにはパスワードの長さを確認する`MinimumPasswordLength`パラメータがあります。このパラメータのデフォルト値は 14 文字です。その結果、このルールは統制要件と一致しています。デフォルトのパラメータ値を使用していない場合は、使用する値が CIS v1.2.0 の 14 文字要件以上であることを確認してください。各マネージドルールのデフォルトパラメータの詳細は、AWS Config ドキュメントに記載されています。

ステップ 2: 範囲内 AWS アカウント で を指定する

評価の範囲内 AWS アカウント に複数の を指定できます。Audit Manager は、 AWS Organizations との統合により複数のアカウントをサポートします。つまり、Audit Manager の評価は複数のアカウントで実行でき、収集された証拠は委任された管理者アカウントに統合されます。Audit Manager で

組織を有効にするには、有効化とセットアップ AWS Organizations （オプション） を参照してください。

> **Note**
>
> Audit Manager は、評価の範囲内で最大 200 のアカウントをサポートできます。200 を超えるアカウントを含めると、評価の作成が失敗する可能性があります。

スコープ AWS アカウント 内で を指定するには

1. でAWS アカウント、評価の範囲 AWS アカウント に含める を選択します。
   - Audit Manager で組織を有効にした場合は、複数のアカウントが表示されます。リストから 1 つ以上のアカウントを選択できます。または、アカウント名、ID、または E メールでアカウントを検索することもできます。
   - Audit Manager で Organizations を有効にしなかった場合 AWS アカウント は、現在の のみが表示されます。
2. [次へ] をクリックします。

> **Note**
>
> 範囲内のアカウントが組織から削除されると、Audit Manager は、それ以降、そのアカウントの証拠を収集しなくなります。ただし、アカウントは引き続き [AWS アカウント] タブの評価に表示されます。範囲内のアカウントのリストからアカウントを削除するには、評価を編集を実行します。削除されたアカウントは編集中にリストに表示されなくなります。また、そのアカウントが範囲に含まれていなくても変更を保存できます。

ステップ 3: 監査所有者を指定する

このステップでは、評価の監査所有者を指定します。監査所有者とは、通常 GRC の職場にいる個人 SecOps、または Audit Manager の評価の管理を担当する DevOps チームのことです。AWSAuditManagerAdministratorAccess ポリシーを使用することをお勧めします。

監査所有者を指定するには

1. [Audit owners] (監査所有者) で、現在の監査所有者のリストを確認します。[監査所有者] の列には、ユーザーの ID とロールが表示されます。AWS アカウント 列には、その監査所有者 AWS アカウント の が表示されます。
2. チェックボックスがオンになっている監査所有者は、評価に含まれます。監査所有者が自らを評価から削除するには、チェックボックスをオフにします。検索バーを使用して名前または AWS アカウントで検索すると、追加の監査所有者を検索できます。
3. 完了したら、[Next (次へ)] を選択します。

ステップ 4: 確認して作成する

評価に関する情報を確認します。ステップに関する情報を変更するには、[Edit (編集)] を選択します。完了したら、[Create assessment (評価を作成)] を選択します。

このアクションにより、評価のための継続的な証拠の収集が開始されます。評価を作成した後、評価ステータスを [inactive (非アクティブ)] に変更するまで、証拠の収集が続行されます。または、コントロールステータスを非アクティブな に変更することで、特定のコントロールの証拠収集を停止することもできます。

> **Note**
>
> 自動証拠は、評価が作成されてから 24 時間後に利用可能になります。Audit Manager は複数のデータ ソースから証拠を自動的に収集し、その証拠収集の頻度は証拠の種類に基づきます。詳細については、このガイドの「証拠収集の頻度」を参照してください。

次のステップ

後日評価を再確認するには、「」を参照してくださいでの評価の検索 AWS Audit Manager。以下の手順に従って評価を検索し、評価を表示、編集、または作業を続けることができます。

追加リソース

Audit Manager の問題を評価する解決策については、「」を参照してください評価と証拠収集の問題に関するトラブルシューティング。

での評価の検索 AWS Audit Manager

で評価を作成すると AWS Audit Manager、Audit Manager コンソールの評価ページで評価を確認できます。

このページから、評価に対してさまざまなアクションを実行できます。例えば、評価の詳細を表示したり、評価設定を編集したり、不要になった評価を削除したりできます。さらに、評価ページは、新しい評価を作成するための出発点として機能します。

Audit Manager API または () を使用して、評価をプログラムで AWS Command Line Interface 表示することもできますAWS CLI。

前提条件

次の手順では、以前に少なくとも 1 つの評価を作成していることを前提としています。評価をまだ作成していない場合、これらのステップを実行すると結果は表示されません。

IAM アイデンティティに、 で評価を表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して評価を表示できますAWS CLI。

Audit Manager console

Audit Manager コンソールで評価を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[変更を保存] を選択して、評価のリストを表示します。
3. 評価名を選択して、その評価の詳細を表示します。

AWS CLI

評価 (CLI) を見るには

Audit Manager で評価を見るには、list-assessments コマンドを実行します。--status サブコマンドを使用して、アクティブまたは非アクティブな評価を見ることができます。

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

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

API を使用して評価を表示するには

Audit Manager で評価を表示するには、 ListAssessmentsオペレーションを使用します。ステータス属性で、アクティブまたは非アクティブな評価を見ることができます。

詳細については、前述のリンクのいずれかを選択して、AWS Audit Manager API リファレンスの詳細をご覧ください。これには、言語固有の AWS SDK の 1 つで ListAssessments オペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

評価の内容を確認する準備ができたら、「」のステップに従いますでの評価の確認 AWS Audit Manager。このページでは、評価の詳細を説明し、表示される情報について説明します。

評価のページから、評価の編集、評価の削除、評価の作成を行うことができます。

追加リソース

Audit Manager の問題を評価する解決策については、「」を参照してください評価と証拠収集の問題に関するトラブルシューティング。

での評価の確認 AWS Audit Manager

Audit Manager で評価を作成した後は、いつでも評価を開いて確認できます。

重要ポイント

評価を検討する準備ができたら、詳細を徐々に深く掘り下げ、詳細度を高めて評価を確認できます。

1. 評価の詳細 – まず、評価の全体的な詳細を確認します。このページでは、評価名、説明、範囲、その他の詳細を確認できます。これにより、評価の概要が表示されます。
2. 評価コントロールの詳細 — 次に、各評価コントロールの詳細を確認して、評価について詳しく説明します。これにより、各コントロールの具体的な要件と目標を理解できます。
3. 証拠フォルダの詳細 – 評価コントロールごとに、特定のコントロールの証拠を含む対応する証拠フォルダを確認できます。これらのフォルダは、各コントロールに関連する証拠を整理します。
4. 証拠の詳細 – 最後に、さらにドリルダウンして、各フォルダ内の個々の証拠を確認します。これには、設定スナップショット、ユーザーアクティビティログ、コンプライアンスの検出結果、ドキュメントやスクリーンショットなどの手動でアップロードされた証拠などが含まれます。この証拠を確認すると、組織がコントロールの要件を満たしていることを理解するのに役立ちます。

これらのステップに従うことで、評価を徹底的に調べ、そのコンポーネントを理解し、組織のコンプライアンスの取り組みをサポートする証拠を確認できます。

追加リソース

Audit Manager で評価の確認を開始するには、ここで概説されている手順に従ってください。

- での評価の詳細の確認 AWS Audit Manager
- での評価コントロールの確認 AWS Audit Manager
- での証拠フォルダの確認 AWS Audit Manager
- での証拠の確認 AWS Audit Manager

での評価の詳細の確認 AWS Audit Manager

評価の詳細を確認する必要がある場合は、評価の詳細ページのいくつかのセクションに情報がまとめられています。これらのセクションは、タスクに関連する情報に簡単にアクセスして理解するのに役立ちます。

目次

- 評価レポートの選択のタブ
- AWS アカウント タブ
- AWS のサービス タブ
- 監査所有者のタブ
- [Tags (タグ)] タブ
- Changelog タブ

- 次のステップ
- 追加リソース

前提条件

次の手順では、以前に少なくとも 1 つの評価を作成していることを前提としています。評価をまだ作成していない場合、これらのステップを実行すると結果は表示されません。

IAM アイデンティティに、 で評価を表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

評価の詳細ページを開いて確認するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[変更を保存] を選択して、評価のリストを表示します。
3. 評価を開くには、その名前を選択します。
4. 以下の情報をリファレンスとして使用して、評価の詳細を確認します。

評価の詳細ページのセクション

- 評価の詳細セクション
- [コントロール] タブ
- 評価レポートの選択のタブ
- AWS アカウント タブ

- AWS のサービス タブ
- 監査所有者のタブ
- [Tags (タグ)] タブ
- Changelog タブ

評価の詳細セクション

評価の詳細セクションを使用して、評価の概要を表示できます。

評価の詳細セクションでは、次の情報を確認できます。

名前	説明
1. 説明	評価の説明。
2. コンプライアンスタイプ	評価がサポートするコンプライアンス標準または規制。
3. 評価レポートの宛先	Audit Manager が評価レポートを保存する S3 バケット。
4. 証拠の合計	この評価で収集された証拠項目の合計数。
5。評価レポートの選択	評価レポートに含めるように選択された証拠項目の数。
6。作成日	評価が作成された日付。
7。最終更新日	評価が最後に編集された日付。
8。[ステータス]	評価のステータス。 • アクティブ - 評価は現在証拠を収集しています。 • 非アクティブ - 評価は証拠を収集しなくなりました。

[コントロール] タブ

このタブを使用して、評価のコントロールに関する情報を表示できます。

コントロールステータスの概要 では、次の情報を確認できます。

名前	説明
コントロールの合計	この評価のコントロールの総数。
確認済み	監査所有者または代理人によってレビューされたコントロールの数。
レビュー中	現在レビュー中のコントロールの数。
無効	証拠をアクティブに収集しなくなったコントロールの数

コントロールセットテーブルでは、コントロールセット別にグループ化されたコントロールのリストを確認できます。各コントロールセットのコントロールを展開または折りたたむことができます。特定のコントロールを探している場合は、名前で検索することもできます。

この表では、次の情報を確認できます。

名前	説明
コントロールセット別にグループ化されたコントロール	コントロールセットの名前。
コントロールのステータス	コントロールのステータス。 • レビュー中 は、このコントロールのレビューが未完了であることを示します。このコントロールの証拠はまだ収集中であり、手動証拠を追加できます。これはデフォルトのステータスです。 • レビュー済み は、このコントロールの証拠のレビューが完了していることを示します。証拠はまだ収集中であり、手動証拠を追加できます。

名前	説明
	• 非アクティブは、このコントロールの自動証拠収集が停止していることを示します。手動証拠を追加することはできなくなりました。
に委任	レビューのために代理人に割り当てられた場合、このコントロールのレビューワー。
証拠の合計	このコントロールに対して収集された証拠項目の数。

評価レポートの選択のタブ

このタブを使用して、評価レポートに含まれる証拠を確認できます。証拠は証拠フォルダ別にグループ化され、証拠フォルダは作成日に基づいて整理されます。

これらのフォルダを参照して、評価レポートに含める証拠を選択できます。評価レポートに証拠を追加する方法については、「」を参照してください評価レポートへの証拠の追加。

このセクションでは、次の情報を確認できます。

名前	説明
証拠フォルダ	証拠フォルダの名前。フォルダ名は、証拠が収集された日付に基づいています。
選択した証拠	評価レポートに含まれるフォルダ内の証拠項目の数。
コントロール名	この証拠フォルダに関連付けられているコントロールの名前。

AWS アカウント タブ

このタブを使用して、評価の範囲内 AWS アカウント にある を表示できます。

このセクションでは、次の情報を確認できます。

名前	説明
アカウント ID	AWS アカウントの ID。

名前	説明
[アカウント名]	AWS アカウントの名前。
Email(メール)	AWS アカウントに関連付けられているメールアドレス。

AWS のサービス タブ

このタブは、評価に表示される場合と表示されない場合があります。

AWS のサービス タブが表示されない場合 (理想的な状態)

このタブが表示されない場合、Audit Manager は評価の対象となる AWS のサービス を管理しています。

Audit Manager は、評価コントロールとそのデータソースを調べ、この情報を対応する にマッピングすることで、この範囲を推測します AWS のサービス。評価の基盤となるデータソースが変更されるたびに、Audit Manager は必要に応じてスコープを自動的に更新して、正しい を反映します AWS のサービス。これにより、評価によって AWS 、環境内のすべての関連サービスに関する正確で包括的な証拠が収集されます。

AWS のサービス タブが表示されている場合

このタブが表示された場合、Audit Manager は評価の対象となる AWS のサービス を管理していません。

この場合、定義した範囲内のサービスに関する次の情報が表示されます。

名前	説明
AWS のサービス	AWS のサービスの名前。
カテゴリ	コンピューティングやデータベース などのサービスカテゴリ。
説明	AWS のサービスの説明。

Audit Manager は、この表のサービスのリソース評価を実行します。例えば、Amazon S3 がリストに表示されている場合、Audit Manager は S3 バケットに関する証拠を収集できます。収集される正確な証拠は、コントロールの によって決まりますdata source。例えば、データソースタイプが で

AWS Config、データソースマッピングが AWS Config ルール (など`s3-bucket-public-write-prohibited`) の場合、Audit Manager はそのルール評価の結果を証拠として収集します。詳細については、このガイドの「サービスの対象範囲とデータソースタイプにはどのような違いがありますか?」を参照してください。

評価が標準フレームワークからコンソールで作成された場合は、Audit Manager がお客様にサービスを選択して、フレームワークの要件に従ってデータソースをマッピングしました。標準フレームワークに手動コントロールのみが含まれている場合、 AWS のサービス は対象になりません。

> **Note**
>
> 次回、評価を編集したり、評価のカスタムコントロールのいずれかを変更したりすると、Audit Manager が対象範囲内のサービスの管理を引き継ぎます。この場合、AWS のサービスタブは評価から削除されます。

監査所有者のタブ

このタブを使用して、評価の監査所有者を確認できます。

このセクションでは、次の情報を確認できます。

名前	説明
監査所有者	監査所有者の名前。
AWS アカウント	監査所有者の AWS アカウント ID。

[Tags (タグ)] タブ

このタブを使用して、評価のタグを表示できます。これらのタグは、評価の作成に使用されたフレームワークから継承されます。Audit Manager のタグの詳細については、「AWS Audit Manager リソースのタグ付け」を参照してください。

このセクションでは、次の情報を確認できます。

名前	説明
キー	コンプライアンス標準、規制、カテゴリなど、タグのキー。

名前	説明
値	タグの値。

Changelog タブ

このタブを使用して、評価のユーザーアクティビティを表示できます。

このセクションでは、次の情報を確認できます。

名前	説明
日付	アクティビティの日付。
ユーザー	アクションを実行したユーザー。
[アクション]	作成された評価など、発生したアクション。
タイプ	評価など、変更されたオブジェクトタイプ。
リソース	評価の作成元のフレームワークなど、変更の影響を受けたリソース。

次のステップ

評価の内容を引き続き確認するには、「」の手順に従いますでの評価コントロールの確認 AWS Audit Manager。このページでは、評価コントロールの詳細について説明し、表示される情報について説明します。

追加リソース

- 評価の詳細ページで、評価を再作成するように求められます。
- 評価にコントロールまたはコントロールセットが表示されません
- 評価の対象となるサービスが表示されない

での評価コントロールの確認 AWS Audit Manager

評価でコントロールを確認する必要がある場合は、評価コントロールの詳細ページのいくつかのセクションに情報がまとめられています。これらのセクションは、タスクに関連する情報に簡単にアクセスして理解するのに役立ちます。

目次

前提条件

次の手順では、以前に少なくとも 1 つの評価を作成していることを前提としています。評価をまだ作成していない場合、これらのステップを実行すると結果は表示されません。

IAM アイデンティティに、 で評価を表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

評価コントロールの詳細ページを開いて確認するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、評価 を選択し、評価の名前を選択して開きます。
3. 評価のページから、[コントロール] タブを選択し、[コントロールセット] の表が表示されるまでスクロールダウンして、コントロールの名前を選択して開きます。
4. 以下の情報をリファレンスとして使用して、評価コントロールの詳細を確認します。

評価コントロールの詳細ページのセクション

コントロールの詳細セクション

コントロールの詳細セクションを使用して、評価コントロールの概要を表示できます。

このセクションでは、次の情報を確認できます。

名前	説明
説明	このコントロールについて提供される説明。
コントロールのステータス	コントロールのステータス。 • レビュー中 – コントロールはまだレビューされていません。このコントロールの証拠はまだ収集中であり、手動証拠を追加できます。これはデフォルトのステータスです。 • レビュー済み — このコントロールの証拠がレビューされます。証拠はまだ収集中であり、手動証拠を追加できます。 • 非アクティブ — このコントロールの自動証拠収集は停止されます。手動証拠を追加することはできなくなりました。

証拠フォルダタブ

このタブを使用して、このコントロールで収集された証拠を表示できます。毎日、フォルダに整理されます。ここから、次のアクションを実行することもできます。

- 証拠フォルダの確認 – 証拠フォルダの詳細を表示するには、ハイパーリンクが設定されたフォルダ名を選択します。

- 評価レポートに証拠フォルダを追加する – 証拠フォルダを含めるには、そのフォルダを選択し、評価レポートに追加 を選択します。
- 評価レポートから証拠フォルダを削除する – フォルダを除外するには、そのフォルダを選択し、評価レポートから削除を選択します。
- 手動証拠の追加 – 手順については、「」を参照してください[での手動証拠の追加 AWS Audit Manager]。

このセクションでは、次の情報を確認できます。

名前	説明
証拠フォルダ	証拠フォルダの名前。名前は、証拠が収集または手動で追加された日付に基づいています。
コンプライアンスチェック	証拠フォルダの問題の数。この数は、 AWS Security Hub、 AWS Config、またはその両方から直接報告されたセキュリティ問題の合計数を表します。 該当なし と表示されている場合は、Security Hub がないか、 AWS Config 有効になっていないか、証拠が別のデータソースタイプから取得されていることを示します。
証拠の合計	フォルダ内の証拠項目の合計数。
評価レポートの選択	評価レポートに含まれるフォルダ内の証拠項目の数。

> **Tip**
>
> 探している証拠フォルダが表示されない場合は、ドロップダウンフィルターを常時 に変更します。そうしないと、過去 7 日間のフォルダがデフォルトで表示されます。

[詳細] タブ

このセクションでは、次の情報を確認できます。

名前	説明
テスト情報	コントロールが意図したとおりに動作していることをテストするための推奨手順。
アクションプラン	コントロールを修正する必要がある場合に実行する推奨アクション。

証拠ソースタブ

このタブを使用して、評価コントロールが証拠を収集する場所を確認できます。証拠ソースには、次のいずれかを含めることができます。

名前	説明
一般的なコントロール	これらは、評価コントロールをサポートするために証拠を収集する一般的なコントロールです。 一般的なコントロールは、 が AWS 管理する基盤となるデータソースを使用して証拠を収集します。リストされているすべての一般的なコントロールについて、Audit Manager は、サポートされているすべてのコアコントロールに関連する証拠を収集します。共通コントロールを選択すると、関連するコアコントロールが表示されます。
コアコントロール	これらは、評価コントロールをサポートするために証拠を収集するコアコントロールです。 コアコントロールは、 が AWS 管理する定義済みのデータソースグループを使用して証拠を収集します。コアコントロールを選択すると、基盤となるデータソースが表示されます。
データソース	これらは、評価コントロールをサポートするために証拠を収集する個々のデータソースです。 • 名前 – データソースの名前。 • Type – 証拠のソースとなるデータソースのタイプ。

名前	説明
	• Audit Manager が証拠を収集する場合、タイプは AWS Security Hub、、AWS CloudTrail、または API AWS Configコール です。 AWS • 独自の証拠をアップロードする場合、タイプは手動 です。説明では、必要な手動証拠がファイルアップロードまたはテキスト応答であるかことが示されます。 • マッピング — 証拠の収集に使用される特定のキーワード。 • タイプが の場合AWS Config、マッピングは AWS Config ルール (などSNS_ENCRYPTED_KMS) です。 • タイプが の場合AWS Security Hub、マッピングは Security Hub コントロール (などEC2.1) です。 • タイプが AWS API コールの場合、マッピングは API コール (などkms_ListKeys) です。 • タイプが の場合AWS CloudTrail、マッピングは CloudTrailイベント (など) ですCreateAccessKey 。 • 頻度 — Audit Manager が AWS API コールデータソースの証拠を収集する頻度。

コメントのタブ

このタブでは、コントロールとその証拠に関するコメントを追加できます。以前のコメントのリストを表示することもできます。

- [コメントを送信] で、テキストを入力して [コメントを送信] を選択することにより、コントロールについてのコメントを追加できます。
- [以前のコメント] で、以前のコメントのリストを、コメントが作成された日付および関連するユーザー ID とともに表示できます。

Changelog タブ

このタブを使用して、評価コントロールのユーザーアクティビティを表示できます。 AWS CloudTrailの監査証跡ログと同じ情報を利用できます。Audit Manager で直接キャプチャされたユー

ザーアクティビティを使用すると、指定したコントロールについて、アクティビティの監査証跡を簡単にレビューできます。

このセクションでは、次の情報を確認できます。

名前	説明
日付	協定世界時 (UTC) で表されるアクティビティの日時。
ユーザー	アクティビティを実行したユーザーまたはロール。
[アクション]	作成された評価など、発生したアクション。
タイプ	評価など、変更されたオブジェクトタイプ。
リソース	評価の作成元のフレームワークなど、変更の影響を受けたリソース。

Audit Manager は、変更ログで次のユーザーアクティビティを追跡します。

- 評価の作成
- 評価の編集
- 評価の完了
- 評価の削除
- レビューのためのコントロールセットの委任
- レビュー済みコントロールセットの監査所有者への送信
- 手動証拠のアップロード
- コントロールステータスの更新
- 評価レポートの生成

次のステップ

評価を引き続き確認するには、「」の手順に従ってくださいでの証拠フォルダの確認 AWS Audit Manager。このページでは、証拠フォルダについて説明し、表示される情報を理解する方法について説明します。

追加リソース

- 評価にコントロールまたはコントロールセットが表示されません

での証拠フォルダの確認 AWS Audit Manager

評価が証拠を収集すると、Audit Manager は便宜上、証拠をフォルダに整理します。証拠フォルダを確認する必要がある場合は、情報がいくつかのセクションに分かれています。

目次

前提条件

次の手順では、以前に少なくとも 1 つの評価を作成していることを前提としています。評価をまだ作成していない場合、これらのステップを実行すると結果が表示されません。

IAM アイデンティティに、 で評価を表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

評価が自動証拠の収集を開始するまでに最大 24 時間かかることに注意してください。評価にまだ証拠がない場合、これらのステップを実行すると結果が表示されません。

手順

証拠フォルダを開いて確認するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。

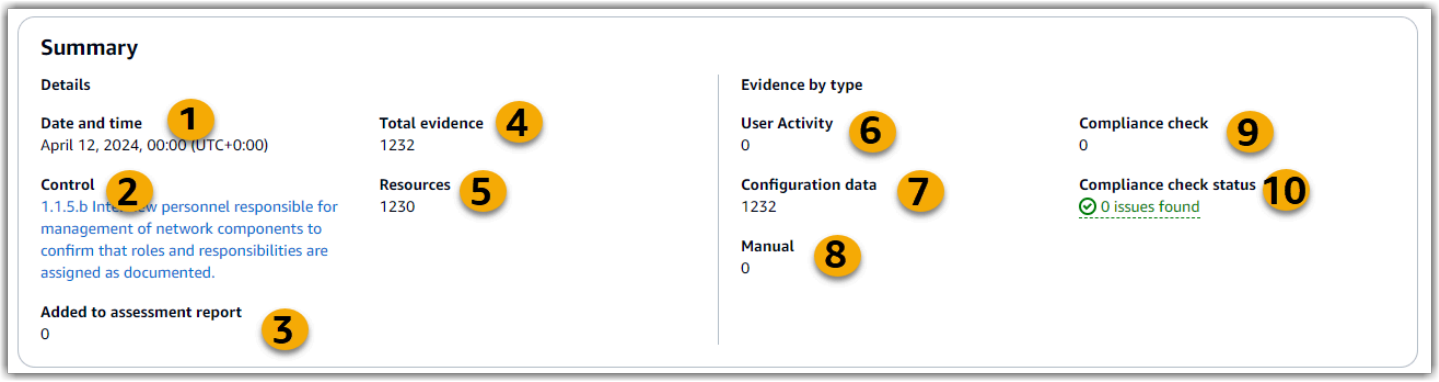
2. ナビゲーションペインで、評価 を選択し、評価を選択します。
3. 評価ページから、コントロールタブを選択し、コントロールテーブルまで下にスクロールし、評価コントロールを選択します。
4. 評価コントロールページから、証拠フォルダタブを選択します。
5. 証拠フォルダ テーブルで、証拠フォルダの名前を選択します。
6. 以下の情報をリファレンスとして使用して、証拠フォルダを確認します。

証拠フォルダページのセクション

- 証拠フォルダの概要
- 証拠の表

証拠フォルダの概要

ページの 概要セクションを使用して、証拠フォルダに証拠の概要を表示できます。さまざまな証拠タイプの詳細については、「証拠」を参照してください。



このセクションでは、次の情報を確認できます。

名前	説明
1. 日付および時間	証拠フォルダが作成された日時。これは協定世界時 (UTC) で表されます。
2. コントロール	証拠フォルダに関連するコントロールの名前。
3. 評価レポートに を追加	評価レポートに含めるように選択された証拠項目の数。
4. 証拠の合計	証拠フォルダ内の証拠項目の合計数。

名前	説明
5. リソース	このフォルダで証拠を収集したときに評価された AWS リソースの合計数。
6。ユーザーアクティビティ	ユーザーアクティビティカテゴリに該当する証拠項目の数。この証拠は AWS CloudTrail ログから収集されます。
7。設定データ	設定データカテゴリに該当する証拠項目の数。この証拠は、他のの設定スナップショットを取得する API コールから収集されますAWS のサービス。
8。手動	手動カテゴリに該当する証拠項目の数。この証拠は手動で追加されます。
9。コンプライアンスチェック	コンプライアンスチェックカテゴリに該当する証拠項目の数。この証拠は AWS Config、、 AWS Security Hub、またはその両方から収集されます。
10。コンプライアンスチェックのステータス	AWS Security Hub、 AWS Config、またはその両方から直接報告された問題の合計数。

証拠の表

証拠テーブルを使用して、証拠フォルダに含まれる証拠を確認できます。この表から、次のアクションを実行することもできます。

- 個々の証拠の確認 – 証拠の詳細を表示するには、時間列でハイパーリンクが設定された証拠名を選択します。
- 評価レポートに証拠を追加する – 証拠を含めるには、それを選択し、評価レポートに追加 を選択します。
- 評価レポートから証拠を削除する – 証拠を除外するには、その証拠を選択し、評価レポートから削除を選択します。
- 手動証拠の追加 – 手順については、「」を参照してくださいでの手動証拠の追加 AWS Audit Manager。

この表では、次の情報を確認できます。

名前	説明
Time (時間)	証拠が収集された日時を指定します。これは証拠の名前としても機能します。時刻は、協定世界時 (UTC) で表されます。
コンプライアンスチェック	コンプライアンスチェックカテゴリに該当する証拠の評価ステータス。 • Security Hub から収集された証拠については、合格または不合格の結果が Security Hub から直接報告されます。 • から収集された証拠については AWS Config、準拠または非準拠の結果が から直接報告されます AWS Config。 • 該当なしと表示されている場合は、 AWS Config または Security Hub が有効になっていないか、証拠が別のデータソースタイプから取得されていることを示します。
タイプ別の証拠	証拠のタイプ。 • コンプライアンスチェックの証拠は、 または から AWS Config 収集されます AWS Security Hub。 • ユーザーアクティビティの証拠は から収集されます AWS CloudTrail。 • 設定データの証拠は、他の への API コールから収集されます AWS のサービス。 • 手動証拠は、手動で追加する証拠です。
データソース	証拠が収集されるデータソース。
イベント名	証拠収集を呼び出したイベントの名前。
[イベントソース]	イベント AWS のサービス に関連する を識別するサービスプリンシパル。
リソース	証拠の収集時に評価されたリソースの数。
評価レポートの選択	証拠が評価レポートに含まれているかどうかを示します。

名前	説明
	• 証拠を含めるには、証拠を選択し、[評価レポートに追加] を選択します。 • 証拠を除外するには、証拠を選択し、[評価レポートから削除] を選択します。

次のステップ

フォルダ内の個々の証拠を調べる準備ができたら、「」のステップに従いますでの証拠の確認 AWS Audit Manager。このページでは、証拠の詳細と、そこに表示されている情報の解釈方法について説明します。

追加リソース

- Audit Manager で問題を証拠する解決策については、「」を参照してください評価と証拠収集の問題に関するトラブルシューティング。

での証拠の確認 AWS Audit Manager

特定の証拠を確認する必要がある場合は、このページの指示に従ってください。証拠の詳細は、いくつかのセクションに分かれています。

目次

前提条件

次の手順では、以前に少なくとも 1 つの評価を作成していることを前提としています。評価をまだ作成していない場合、これらのステップを実行すると結果が表示されません。

IAM アイデンティティに、 で評価を表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

評価が自動証拠の収集を開始するまでに最大 24 時間かかることに注意してください。評価にまだ証拠がない場合、これらのステップを実行すると結果が表示されません。

手順

証拠の詳細ページを開いて確認するには

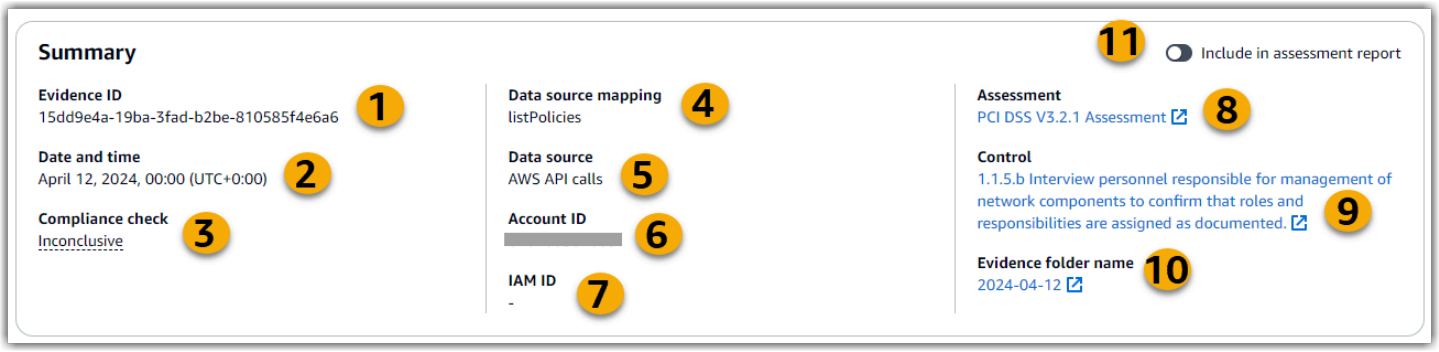
1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、評価 を選択し、評価を選択します。
3. 評価ページから、コントロールタブを選択し、コントロールテーブルまで下にスクロールし、コントロールを選択します。
4. コントロールのページから、[証拠フォルダ] タブを選択します。
5. 証拠フォルダ テーブルで、証拠フォルダの名前を選択します。
6. Time 列の下にある証拠名を選択して、証拠の詳細ページを開きます。
7. 以下の情報をリファレンスとして使用して、証拠の詳細を確認します。

証拠の詳細ページのセクション

- [概要]
- 属性
- 含まれるリソース

[概要]

概要セクションを使用して、証拠の概要を表示できます。



このセクションでは、次の情報を確認できます。

名前	説明
1. 証拠 ID	証拠の一意の識別子。
2。日付および時間	証拠が収集された日時。これは協定世界時 (UTC) で表されます。
3. コンプライアンスチェック	コンプライアンスチェックの証拠の評価ステータス。 • から収集された証拠の場合 AWS Security Hub、合格または不合格の結果は から直接報告されます AWS Security Hub。 • から収集された証拠については AWS Config、準拠または非準拠の結果が から直接報告されます AWS Config。 • 該当なしと表示されている場合は、2 つの要素のいずれかを示します。または AWS Security Hub AWS Config が有効になっていません。または、証拠は別のデータソースから取得されます。
4. データソースマッピング	証拠の収集に使用されたマッピングキーワード。
5. [Data source type]	証拠が収集されたデータソースのタイプ。
6。アカウント ID	証拠に関連付けられている AWS アカウント 。
7。IAM ID	該当する場合は、関連するユーザーまたはロール。
8。[評価]	証拠に関連付けられている評価の名前。
9。コントロール	証拠に関連付けられているコントロールの名前。
10。証拠フォルダ名	証拠を含む証拠フォルダの名前。

名前	説明
11。評価レポートに含める	評価レポートに証拠を含めたり除外したりできるスイッチ。

属性

属性テーブルを使用して、証拠属性の詳細を表示できます。

この表では、次の情報を確認できます。

名前	説明
属性名	属性のキー。
値	属性の値。場合によっては、JSON ファイルへのリンクに詳細情報が表示されます。

含まれるリソース

この証拠を生成するために評価されたリソースを確認するには、 リソースを含むテーブルを使用します。

このセクションでは、次の情報を確認できます。

名前	説明
ARN	リソースの Amazon リソースネーム (ARN)。ARN は、すべての証拠タイプで利用できるとは限りません。
リソースコンプライアンス	リソースの評価ステータス。 • から収集された証拠の場合 AWS Security Hub、合格または不合格の結果は Security Hub から直接報告されます。 • から収集された証拠については AWS Config、準拠または非準拠の結果が から直接報告されます AWS Config。

名前	説明
	• 該当なしが表示されている場合は、 AWS Config または Security Hub が有効になっていないか、証拠が別のデータソースから取得されていることを示します。
値	リソース評価に関する詳細情報。場合によっては、JSON ファイルへのリンクに詳細情報が表示されます。

追加リソース

- Audit Manager で問題を証拠する解決策については、「」を参照してください評価と証拠収集の問題に関するトラブルシューティング。

での評価の編集 AWS Audit Manager

で既存の評価を編集する必要がある場合があります AWS Audit Manager。監査の範囲が変更され、評価 AWS アカウント に含まれる の更新が必要になった可能性があります。または、人事の変更により、評価に割り当てられた監査所有者のリストを修正する必要がある場合があります。このような場合は、証拠収集を中断することなく、アクティブな評価を編集し、必要な調整を行うことができます。

次のページでは、評価の詳細の編集、範囲内 AWS アカウント の の変更、監査所有者の更新、変更の確認と保存の手順の概要を説明します。

前提条件

次の手順では、以前に少なくとも 1 つの評価を作成し、それがアクティブ状態であることを前提としています。

IAM アイデンティティに、 で評価を編集するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

タスク

- ステップ 1: 評価の詳細を編集する
- ステップ 2: 範囲内 AWS アカウント で を編集する
- ステップ 3: 監査所有者を編集する
- ステップ 4: 確認して保存する

ステップ 1: 評価の詳細を編集する

評価の詳細を編集するには、次の手順に従います。

評価を編集するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[評価] を選択します。
3. 評価を選択して、[編集] を選択します。
4. 「評価の詳細の編集」で、必要に応じて評価の詳細を編集します。
5. [次へ] をクリックします。

ステップ 2: 範囲内 AWS アカウント で を編集する

このステップでは、評価に含めるアカウントを変更できます。Audit Manager は、評価の範囲内で最大 200 のアカウントをサポートできます。

範囲内 AWS アカウント で を編集するには

1. を追加するには AWS アカウント、アカウント名の横にあるチェックボックスをオンにします。
2. を削除するには AWS アカウント、アカウント名の横にあるチェックボックスをオフにします。
3. [次へ] をクリックします。

> **Note**
>
> Audit Manager の委任管理者を編集するには、「」を参照してください委任管理者の変更。

ステップ 3: 監査所有者を編集する

このステップでは、評価に含める監査所有者を変更できます。

監査所有者を編集するには

1. 監査所有者を追加するには、アカウント名の横にあるチェックボックスをオンにします。
2. 監査所有者を削除するには、アカウント名の横にあるチェックボックスをオフにします。
3. [次へ] をクリックします。

ステップ 4: 確認して保存する

評価に関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。終了したら、[変更を保存] を選択して編集内容を確認します。

編集が完了すると、評価の変更は翌日の 00:00 (UTC) に有効になります。

次のステップ

特定の評価コントロールの証拠を収集する必要がなくなった場合は、そのコントロールのステータスを変更できます。手順については、「での評価コントロールのステータスの変更 AWS Audit Manager」を参照してください。

評価全体の証拠を収集する必要がなくなったら、評価ステータスを非アクティブに変更できます。手順については、「で評価のステータスを非アクティブに変更する AWS Audit Manager」を参照してください。

追加リソース

- Audit Manager の問題を評価する解決策については、「」を参照してください評価と証拠収集の問題に関するトラブルシューティング。
- 対象範囲内のサービスを編集できなくなる理由については、このガイドのトラブルシューティングセクションの評価の範囲内のサービスを編集できません「」を参照してください。

での手動証拠の追加 AWS Audit Manager

Audit Manager は、多くのコントロールの証拠を自動的に収集できます。ただし、一部のコントロールでは、自動的に収集できない証拠が必要になる場合があります。このような場合は、独自の証拠を手動で追加できます。

次の例を考えます。

- 一部のコントロールは、物理記録 (署名など)、またはクラウドで生成されないイベント (観察やインタビューなど) の提供に関連しています。このような場合は、証拠としてファイルを手動で追加できます。例えば、コントロールで組織構造に関する情報が必要である場合は、手動証拠として会社の組織図のコピーをアップロードできます。
- 一部のコントロールは、ベンダーのリスク評価に関する質問を表します。リスク評価の質問には、証拠として文書 (組織図など)が必要となる場合があります。または、単純なテキスト回答 (役職のリストなど) のみが必要な場合もあります。後者の場合、質問に応答し、応答を手動証拠として保存できます。

手動アップロード機能を使用して、複数の環境からの証拠を管理することもできます。会社がハイブリッドクラウドモデルまたはマルチクラウドモデルを使用している場合は、オンプレミス環境、クラウドでホストされている環境、または SaaS アプリケーションから証拠をアップロードできます。これにより、証拠を Audit Manager 評価の構造内に保存することで (その出所に関係なく) 証拠を整理でき、証拠の各部分は特定のコントロールにマッピングされます。

重要ポイント

Audit Manager で評価に手動証拠を追加する場合は、3 つの方法から選択できます。

1. Amazon S3 からのファイルのインポート - この方法は、ドキュメント、レポート、または Audit Manager によって自動的に収集できないその他のアーティファクトなど、証拠ファイルが S3 バケットに保存されている場合に最適です。これらのファイルを S3 から直接インポートすることで、この手動証拠を自動的に収集した証拠とシームレスに統合できます。
2. ブラウザからファイルをアップロードする - コンピュータまたはネットワークに証拠ファイルがローカルに保存されている場合は、この方法を使用して Audit Manager に手動でアップロードできます。このアプローチは、スキャンされたドキュメントやイメージなどの、 AWS 環境内でデジタル形式で利用できない物理レコードを含める必要がある場合に特に役立ちます。
3. 証拠として自由形式のテキストを追加する - 場合によっては、提供する必要がある証拠はファイルの形式ではなく、テキストのレスポンスや説明の形式です。この方法では、自由形式のテキストを Audit Manager に直接入力できます。これは、ベンダーのリスク評価の質問に応答するときに特に役立ちます。

追加リソース

- 評価コントロールに手動証拠を追加する方法については、以下のリソースを参照してください。一度に使用できるメソッドは 1 つだけであることに注意してください。
  - Amazon S3 からの手動証拠ファイルのインポート
  - ブラウザからの手動証拠ファイルのアップロード
  - 手動証拠としての自由形式のテキストレスポンスの入力
- 使用できるファイル形式については、「」を参照してください手動証拠にサポートされているファイル形式。
- Audit Manager のさまざまなタイプの証拠の詳細については、このガイドevidenceの「概念と用語」セクションの「」を参照してください。
- トラブルシューティングのサポートについては、「」を参照してくださいコントロールに手動証拠をアップロードできません。

Amazon S3 からの手動証拠ファイルのインポート

Amazon S3 バケットから評価に証拠ファイルを手動でインポートできます。これにより、自動的に収集された証拠に追加のサポート資料を補足できます。

前提条件

- 単一の手動証拠ファイルにサポートされる最大サイズは 100 MB です。
- のいずれかを使用する必要があります手動証拠にサポートされているファイル形式。
- 各 AWS アカウント は、毎日最大 100 個の証拠ファイルをコントロールに手動でアップロードできます。この 1 日あたりのクォータを超えると、そのコントロールについては追加の手動アップロードが失敗します。単一のコントロールに手動証拠を大量にアップロードする必要がある場合は、証拠を数日にわたってバッチでアップロードします。
- コントロールが 非アクティブの場合、そのコントロールに手動証拠は追加できません。手動証拠を追加するには、まずコントロールステータスをレビュー対象またはレビュー対象のいずれかに変更する必要があります。
- IAM アイデンティティに、 で評価を管理するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用してファイルをインポートできますAWS CLI。

AWS console

Audit Manager コンソールで S3 からファイルをインポートするには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、「評価」を選択し、「評価」を選択します。
3. コントロールタブを選択し、下にスクロールしてコントロールセットを選択し、コントロールを選択します。
4. [証拠フォルダ] タブで、[手動証拠を追加] を選択してから、[S3 からファイルをインポート] を選択します。
5. 次のページで、証拠の S3 URI を入力します。S3 URI は、Amazon S3 コンソールのオブジェクトに移動し、[Copy S3 URI (S3 URI をコピー)] を選択します。
6. [Upload (アップロード)] を選択します。

AWS CLI

次の手順では、*placeholder text*を独自の情報に置き換えます。

で S3 からファイルをインポートするには AWS CLI

1. `list-assessments` コマンドを実行して評価のリストを表示します。

```
aws auditmanager list-assessments
```

回答から証拠をアップロードする評価を検索して、評価 ID をメモします。

2. `get-assessment` コマンドを実行して、ステップ 1 の評価 ID を指定します。

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

回答から証拠をアップロードするコントロールセットとコントロールを検索して、その ID をメモします。

3. 次のパラメータを使用して、batch-import-evidence-to-assessment-control コマンドを実行します。

   - --assessment-id— ステップ 1 の評価 ID を使用します。
   - --control-set-id—ステップ 2 のコントロールセット ID を使用します。
   - --control-id— ステップ 2 のコントロール ID を使用します。
   - --manual-evidence — 手動証拠タイプとして s3ResourcePath を使用し、証拠の S3 URI を指定します。S3 URI は、Amazon S3 コンソールのオブジェクトに移動し、[S3 URI をコピー] を選択します。

```
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://
DOC-EXAMPLE-BUCKET/EXAMPLE-FILE.extension
```

Audit Manager API

API を使用して S3 からファイルをインポートするには

1. ListAssessments 操作を呼び出し、評価のリストを表示します。回答から証拠をアップロードする評価を検索して、評価 ID をメモします。
2. GetAssessment 操作を呼び出し、ステップ 1 の評価 ID を指定します。回答から証拠をアップロードするコントロールセットとコントロールを検索して、その ID をメモします。
3. 以下のパラメータで BatchImportEvidenceToAssessmentControl 操作を呼び出します。

   - assessmentId— ステップ 1 の評価 ID を使用します。
   - controlSetId—ステップ 2 のコントロールセット ID を使用します。
   - controlId— ステップ 2 のコントロール ID を使用します。
   - manualEvidence — 手動証拠タイプとして s3ResourcePath を使用し、証拠の S3 URI を指定します。S3 URI は、Amazon S3 コンソールのオブジェクトに移動し、[S3 URI をコピー] を選択します。

詳細については、前の手順のリンクのいずれかを選択して、 AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

評価の証拠を追加および確認したら、評価レポートを生成できます。詳細については、「での評価レポートの準備 AWS Audit Manager」を参照してください。

追加リソース

使用できるファイル形式については、「」を参照してください手動証拠にサポートされているファイル形式。

ブラウザからの手動証拠ファイルのアップロード

証拠ファイルは、ブラウザから Audit Manager の評価に手動でアップロードできます。これにより、自動的に収集された証拠に追加のサポート資料を補足できます。

前提条件

- 単一の手動証拠ファイルにサポートされる最大サイズは 100 MB です。
- のいずれかを使用する必要があります手動証拠にサポートされているファイル形式。
- 各 AWS アカウント は、毎日最大 100 個の証拠ファイルをコントロールに手動でアップロードできます。この 1 日あたりのクォータを超えると、そのコントロールについては追加の手動アップロードが失敗します。単一のコントロールに手動証拠を大量にアップロードする必要がある場合は、証拠を数日にわたってバッチでアップロードします。
- コントロールが 非アクティブの場合、そのコントロールに手動証拠は追加できません。手動証拠を追加するには、まずコントロールステータスをレビュー対象またはレビュー対象のいずれかに変更する必要があります。
- IAM アイデンティティに、 で評価を管理するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用してファイルをアップロードできますAWS CLI。

AWS console

Audit Manager コンソールでブラウザからファイルをアップロードするには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、「評価」を選択し、「評価」を選択します。
3. コントロールタブで、コントロールセットまで下にスクロールし、コントロールを選択します。
4. 証拠フォルダ タブから、手動証拠を追加 を選択します。
5. ブラウザ からファイルをアップロード を選択します。
6. アップロードするファイルを選択します。
7. [Upload (アップロード)] を選択します。

AWS CLI

次の手順では、*placeholder text*を独自の情報に置き換えます。

でブラウザからファイルをアップロードするには AWS CLI

1. `list-assessments` コマンドを実行して評価のリストを表示します。

```
aws auditmanager list-assessments
```

   回答から証拠をアップロードする評価を検索して、評価 ID をメモします。

2. `get-assessment` コマンドを実行して、ステップ 1 の評価 ID を指定します。

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   回答から証拠をアップロードするコントロールセットとコントロールを検索して、その ID をメモします。

3. get-evidence-file-upload-url コマンドを実行して、アップロードするファイルを指定します。

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

回答で指定された URL と evidenceFileName をメモします。

4. ステップ 3 で指定した URL で、ブラウザからファイルをアップロードします。このアクションにより、ファイルが Amazon S3 にアップロードされ、評価コントロールに添付できるオブジェクトとして保存されます。次のステップでは、evidenceFileName パラメータを使用して新しく作成したオブジェクトを参照します。

> **Note**
>
> 署名付き URL を使用してファイルをアップロードすると、Audit Manager は によるサーバー側の暗号化を使用してデータを保護し、保存します AWS Key Management Service。これをサポートするには、署名付き URL を使用してファイルをアップロードするときに、リクエスト内の x-amz-server-side-encryption ヘッダーを使用する必要があります。
> Audit Manager データ暗号化設定の構成の設定 AWS KMS key でカスタマー管理 を使用している場合は、リクエストに x-amz-server-side-encryption-aws-kms-key-idヘッダーも含めてください。x-amz-server-side-encryption-aws-kms-key-idヘッダーがリクエストにない場合、Amazon S3 は AWS マネージドキーを使用すると見なします。
> 詳細については、Amazon Simple Storage Service ユーザーガイドのAWS Key Management Service 「キーによるサーバー側の暗号化 (SSE-KMS) を使用したデータの保護」を参照してください。

5. 次のパラメータを使用して、batch-import-evidence-to-assessment-control コマンドを実行します。

- --assessment-id— ステップ 1 の評価 ID を使用します。
- --control-set-id—ステップ 2 のコントロールセット ID を使用します。
- --control-id— ステップ 2 のコントロール ID を使用します。
- --manual-evidence—手動による証拠タイプとして evidenceFileName 使用して、ステップ 3 から証拠ファイル名を指定します。

```
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

API を使用してブラウザからファイルをアップロードするには

1. ListAssessments 操作を呼び出します。回答から証拠をアップロードする評価を検索して、評価 ID をメモします。
2. GetAssessment 操作を呼び出して、ステップ 1 から assessmentId を指定します。回答から証拠をアップロードするコントロールセットとコントロールを検索して、その ID をメモします。
3. GetEvidenceFileUploadUrl 操作を呼び出して、アップロードする fileName を指定します。回答で指定された URL と evidenceFileName をメモします。
4. ステップ 3 で指定した URL で、ブラウザからファイルをアップロードします。このアクションにより、ファイルが Amazon S3 にアップロードされ、評価コントロールに添付できるオブジェクトとして保存されます。次のステップでは、evidenceFileName パラメータを使用して新しく作成したオブジェクトを参照します。

> **Note**
>
> 署名付き URL を使用してファイルをアップロードすると、Audit Manager は による サーバー側の暗号化を使用してデータを保護し、保存します AWS Key Management Service。これをサポートするには、署名付き URL を使用してファイルをアップロードするときに、リクエスト内の x-amz-server-side-encryption ヘッダーを使用する必要があります。
> Audit Manager データ暗号化設定の構成の設定 AWS KMS key でカスタマー管理 を使用している場合は、リクエストに x-amz-server-side-encryption-aws-kms-key-idヘッダーも含めてください。x-amz-server-side-encryption-aws-kms-key-idヘッダーがリクエストにない場合、Amazon S3 は AWS マネージドキーを使用すると見なします。

詳細については、Amazon Simple Storage Service ユーザーガイドのAWS Key Management Service 「キーによるサーバー側の暗号化 (SSE-KMS) を使用したデータの保護」を参照してください。

5. 以下のパラメータで BatchImportEvidenceToAssessmentControl 操作を呼び出します。

   - assessmentId— ステップ 1 の評価 ID を使用します。
   - controlSetId—ステップ 2 のコントロールセット ID を使用します。
   - controlId— ステップ 2 のコントロール ID を使用します。
   - manualEvidence—手動による証拠タイプとして evidenceFileName 使用して、ステップ 3 から証拠ファイル名を指定します。

詳細については、前の手順のリンクのいずれかを選択して、 AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

評価の証拠を収集して確認したら、評価レポートを生成できます。詳細については、「での評価レポートの準備 AWS Audit Manager」を参照してください。

追加リソース

使用できるファイル形式については、「」を参照してください手動証拠にサポートされているファイル形式。

手動証拠としての自由形式のテキストレスポンスの入力

自由形式のテキストを入力し、そのテキストを証拠として保存することで、評価コントロールに関する追加のコンテキストとサポート情報を提供できます。これにより、自動証拠収集ではキャプチャされない詳細を手動で文書化できます。

例えば、Audit Manager を使用して、ベンダーリスク評価アンケートの質問を表すカスタムコントロールを作成できます。この場合、各コントロールの名前は、組織のセキュリティおよびコンプライアンス体制に関する情報を尋ねる特定の質問です。特定のベンダーリスク評価の質問に対する回答を記録するには、テキストレスポンスを入力し、コントロールの手動証拠として保存できます。

前提条件

- コントロールが 非アクティブの場合、そのコントロールに手動証拠は追加できません。手動証拠を追加するには、まずコントロールステータスをレビュー対象またはレビュー対象のいずれかに変更する必要があります。
- IAM アイデンティティに、 で評価を管理するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用してテキストレスポンスを入力できますAWS CLI。

AWS console

Audit Manager コンソールでテキストレスポンスを入力するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、「評価」を選択し、「評価」を選択します。
3. コントロールタブを選択し、下にスクロールしてコントロールセットを選択し、コントロールを選択します。
4. 証拠フォルダ タブから、手動証拠の追加 を選択します。
5. Enter text response を選択します。
6. 表示されるポップアップウィンドウに、プレーンテキスト形式で回答を入力してください。
7. [Confirm (確認)] を選択します。

AWS CLI

次の手順では、*placeholder text*を独自の情報に置き換えます。

にテキストレスポンスを入力するには AWS CLI

1. `list-assessments` コマンドを実行します。

```
aws auditmanager list-assessments
```

回答から証拠をアップロードする評価を検索して、評価 ID をメモします。

2. get-assessment コマンドを実行して、ステップ 1 の評価 ID を指定します。

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

回答で、証拠のアップロード先のコントロールセットとコントロールを検索し、その ID をメモします。

3. 次のパラメータを使用して、batch-import-evidence-to-assessment-control コマンドを実行します。

- --assessment-id— ステップ 1 の評価 ID を使用します。
- --control-set-id—ステップ 2 のコントロールセット ID を使用します。
- --control-id— ステップ 2 のコントロール ID を使用します。
- --manual-evidence— 手動証拠タイプとして textResponse を使用して、手動証拠として保存するテキストを入力します。

```
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

API を使用してテキストレスポンスを入力するには

1. ListAssessments 操作を呼び出します。回答から証拠をアップロードする評価を検索して、評価 ID をメモします。
2. GetAssessment 操作を呼び出して、ステップ 1 から assessmentId を指定します。回答で、証拠のアップロード先のコントロールセットとコントロールを検索し、その ID をメモします。

3. 以下のパラメータで BatchImportEvidenceToAssessmentControl 操作を呼び出します。

   - assessmentId— ステップ 1 の評価 ID を使用します。
   - controlSetId—ステップ 2 のコントロールセット ID を使用します。
   - controlId— ステップ 2 のコントロール ID を使用します。
   - manualEvidence— 手動証拠タイプとして textResponse を使用して、手動証拠として保存するテキストを入力します。

   詳細については、前の手順のリンクのいずれかを選択して、 AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

評価の証拠を収集して確認したら、評価レポートを生成できます。詳細については、「での評価レポートの準備 AWS Audit Manager」を参照してください。

手動証拠にサポートされているファイル形式

次の表に手動証拠としてアップロードできるファイルの種類をリスト表示して、説明します。各ファイルタイプに、表にはサポートされているファイル拡張子もリスト表示されます。

ファイルタイプ	説明	サポートされているファイル拡張子
圧縮またはアーカイブ	GNU Zip 圧縮アーカイブおよび ZIP 圧縮アーカイブ	.gz, .zip
ドキュメント	PDF、Microsoft Office ファイルなどの一般的なドキュメントファイル	.doc, .docx, .pdf, .ppt, .pptx, .xls, .xlsx
イメージ	イメージファイルとグラフィックファイル	.jpeg, .jpg, .png, .svg

ファイルタイプ	説明	サポートされているファイル拡張子
テキスト	プレーンテキスト文書やマークアップ言語ファイルなど、その他の非バイナリテキストファイル	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

追加リソース

評価コントロールに独自の証拠を追加するさまざまな方法については、以下のページを参照してください。

- Amazon S3 からの手動証拠ファイルのインポート
- ブラウザからの手動証拠ファイルのアップロード
- 手動証拠としての自由形式のテキストレスポンスの入力

での評価レポートの準備 AWS Audit Manager

評価の証拠を収集して確認したら、評価レポートを生成できます。評価レポートは、評価を要約し、関連する証拠を含む整理されたフォルダのセットへのリンクを提供します。

重要ポイント

新しく収集された証拠は、評価レポートに自動的には表示されません。つまり、レポートに含める証拠を制御できます。含める証拠を選択したら、最終評価レポートを生成して監査人と共有できます。

評価レポートを生成すると、評価レポートの宛先として選択した S3 バケットに格納されます。Audit Manager のダウンロードセンターから評価レポートをダウンロードすることもできます。

追加リソース

評価レポートとその管理方法の詳細については、次のリソースを参照してください。

- 評価レポートへの証拠の追加
- 評価レポートから証拠を削除する
- 評価レポートの生成

- 評価レポートのダウンロード
- 評価レポートのナビゲーションとその内容の探索
- 評価レポートの検証
- 評価レポートの削除
- 証拠ファインダーの検索結果から評価レポートを生成する
- デフォルトの評価レポートの送信先の設定
- 評価レポートの問題のトラブルシューティング

評価レポートへの証拠の追加

評価レポートを作成する前に、評価レポートに少なくとも 1 つの証拠を追加する必要があります。証拠フォルダ全体を追加するか、フォルダ内から特定の証拠項目を追加できます。

手順

評価レポートに証拠を含めるには、次の手順に従います。

評価レポートへ証拠を追加するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、「評価」を選択し、「評価」を選択します。
3. コントロール タブで、コントロールセット テーブルまで下にスクロールし、評価レポートに含める証拠を含むコントロールを選択します。
4. 評価レポートに証拠を追加する方法を選択します。

    a. 証拠フォルダ全体を追加するには、[証拠フォルダ] までスクロールダウンし、追加するフォルダを選択してから、[評価レポートに追加] を選択します。

> **Tip**
>
> 探しているフォルダが見つからない場合は、ドロップダウンフィルターを[常時] に変更します。そうしないと、過去 7 日間のフォルダがデフォルトで表示されます。[評価レポートに追加] がグレーアウトされる場合は、証拠フォルダは既に評価レポートに追加されています。

b. 特定の証拠を追加するには、証拠フォルダを選択してその内容を開きます。リストから 1 つまたは複数の項目を選択してから、[評価レポートに追加] を選択します。

> **Tip**
>
> [評価レポートに追加] がグレーアウトされている場合は、証拠の横にあるチェックボックスが選択されていることを確認してから、再試行します。

5. 証拠を評価レポートに追加すると、緑の成功バナーが表示されます。[評価レポートに証拠を表示] を選択すると、評価レポートに含まれる証拠が表示されます。
   - または、評価に戻って、[評価レポート選択] タブを選択することで、評価レポートに含まれる証拠を表示できます。

次のステップ

評価レポートから証拠を削除する必要がある場合は、「」を参照してください評価レポートから証拠を削除する。

評価レポートを生成する準備ができたら、「」を参照してください評価レポートの生成。

追加リソース

一般的な質問や問題に対する回答を見つけるには、このガイドの評価レポートの問題のトラブルシューティング「トラブルシューティング」セクションの「」を参照してください。

評価レポートから証拠を削除する

評価レポートから証拠を削除する必要がある場合は、次の手順に従います。証拠フォルダ全体を削除、またはフォルダ内から特定の証拠項目を削除できます。

手順

評価レポートから証拠を削除するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[評価] を選択してから、評価の名前を選択して開きます。

3. [コントロール] タブで、[コントロールセット] 表までスクロールダウンし、コントロールの名前を選択して開きます。
4. 評価レポートから証拠を削除する方法を選択します。

   a. 証拠フォルダ全体を削除するには、証拠フォルダまでスクロールダウンし、削除するフォルダを選択してから、[評価レポートから削除] を選択します。

   > **Tip**
   >
   > 探しているフォルダが見つからない場合は、ドロップダウンフィルターを[常時] に変更します。そうしないと、過去 7 日間のフォルダがデフォルトで表示されます。[評価レポートから削除] がグレーアウトされている場合は、証拠フォルダは評価レポートから既に削除されています。

   b. 特定の証拠を削除するには、証拠フォルダを選択してその内容を開きます。リストから 1 つまたは複数の項目を選択してから、[評価レポートから削除] を選択します。

   > **Tip**
   >
   > [評価レポートから削除] がグレーアウトされている場合は、証拠の横にあるチェックボックスが選択されていることを確認してから、再試行します。

5. 証拠を評価レポートに追加すると、緑の成功バナーが表示されます。[評価レポートに証拠を表示] を選択すると、評価レポートに含まれる証拠が表示されます。
   - または、評価に戻って、[評価レポート選択] タブを選択することで、評価レポートに含まれる証拠を表示できます。

次のステップ

評価レポートを生成する準備ができたら、「」を参照してください評価レポートの生成。

追加リソース

一般的な質問や問題に対する回答を見つけるには、このガイドの評価レポートの問題のトラブルシューティング「トラブルシューティング」セクションの「」を参照してください。

評価レポートの生成

評価レポートを生成する準備ができたら、次のステップに従います。

前提条件

評価レポートを作成する前に、評価レポートに少なくとも 1 つの証拠を追加する必要があります。証拠フォルダ全体を追加、またはフォルダ内から各証拠項目を追加できます。

評価レポートが正常に作成されたことを確認するには、評価レポートの送信先設定のヒント をレビューします。

手順

評価レポートを生成するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Assessments (評価)] を選択します。
3. 評価レポートを生成する評価の名前を選択します。
4. [Assessment report selection (評価レポートの選択)] タブを選択してから、[Generate assessment report (評価レポートを生成)] を選択します。

   > **Tip**
   >
   > [評価レポートを生成] がグレーアウトされている場合は、証拠がまだ評価レポートに追加されなかったということです。

5. ポップアップウィンドウに評価レポートの名前と説明を入力し、評価レポートの詳細を確認します。
6. [評価レポートを生成] を選択して、評価レポートが生成されるまで数分待ちます。
7. Audit Manager コンソールの[ダウンロードセンター] ページから評価レポートを検索してダウンロードします。
   - または、評価レポートの送信先の S3 バケットに移動して、そこから評価レポートをダウンロードすることもできます。

次のステップ

評価を生成したら、以下の詳細を確認できます。

- 評価レポートを検索してダウンロード — ダウンロードセンターまたは Amazon S3 から評価レポートをダウンロードする方法について説明します。
- 評価レポートを検索 — 評価レポートをナビゲートして、その内容を調べる方法について説明します。
- 評価レポートの検証 — ValidateAssessmentReportIntegrity API オペレーションを使用して評価レポートを検証する方法について説明します。
- 不要な評価レポートを削除 — ダウンロードセンターまたは Amazon S3 から不要なレポートを削除する方法について説明します。
- 証拠ファインダーから評価レポートを生成する – 証拠ファインダーの検索結果から評価レポートを生成する方法について説明します。

追加リソース

一般的な質問や問題に対する回答を見つけるには、このガイドの評価レポートの問題のトラブルシューティング「トラブルシューティング」セクションの「」を参照してください。

での評価コントロールのステータスの変更 AWS Audit Manager

アクティブな評価内で評価コントロールのステータスを変更できます。コントロールのステータスを更新すると、その進行状況を追跡し、いつ確認したかを示すことができ、評価を整理し、 を維持できます up-to-date。

前提条件

次の手順では、以前に評価を作成し、その現在のステータスがアクティブであることを前提としています。

IAM アイデンティティに、 で評価を管理するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して、評価コントロールのステータスを更新できますAWS CLI。

> **Note**
>
> コントロールステータスのレビュー済みへの変更は、最終的な操作です。コントロールのステータスを [レビュー済み] に設定すると、そのコントロールのステータスを変更したり、以前のステータスに戻すことはできなくなります。

Audit Manager console

Audit Manager コンソールで評価コントロールのステータスを変更するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[評価] を選択します。
3. 評価を開くには、その名前を選択します。
4. 評価のページから、[コントロール] タブを選択し、[コントロールセット] の表が表示されるまでスクロールダウンして、コントロールの名前を選択して開きます。
5. ページの右上にあるコントロールステータスの更新を選択し、ステータスを選択します。

ステータス	説明
レビュー中	コントロールをまだ確認していない場合は、このステータスを選択します。
確認済み	このコントロールの証拠の確認が完了し、証拠の収集または追加を継続する場合は、このステータスを選択します。
無効	このコントロールの自動証拠収集を停止する場合は、このステータスを選択します。

6. コントロールステータスの更新を選択して、選択を確認します。

AWS CLI

で評価コントロールのステータスを変更するには AWS CLI

1. list-assessments コマンドを実行します。

```
aws auditmanager list-assessments
```

回答は評価のリストを返します。更新するコントロールを含む評価を見つけ、評価 ID を書き留めます。

2. get-assessment コマンドを実行し、ステップ 1 の評価 ID を指定します。

   次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
```

   レスポンスで、更新するコントロールを見つけ、コントロール ID とそのコントロールセット ID を書き留めます。

3. update-assessment-control コマンドを実行し、次のパラメータを指定します。

   - `--assessment-id` – コントロールが属する評価。
   - `--control-set-id` – コントロールが属するコントロールセット。
   - `--control-id` - 更新するコントロール。
   - `--control-status` – この値を UNDER_REVIEW、REVIEWED、または に設定しますINACTIVE。

   次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager update-assessment-control --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --
control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
```

Audit Manager API

API を使用して評価コントロールのステータスを変更するには

1. ListAssessments 操作を使用します。

   レスポンスで、更新するコントロールを含む評価を見つけ、評価 ID を書き留めます。

2. GetAssessment オペレーションを使用して、ステップ 1 の評価 ID を指定します。

レスポンスで、更新するコントロールを見つけ、コントロール ID とそのコントロールセット ID を書き留めます。

3. UpdateAssessmentControl オペレーションを使用して、次のパラメータを指定します。

   - assessmentId – コントロールが属する評価。
   - controlSetId – コントロールが属するコントロールセット。
   - controlId - 更新するコントロール。
   - controlStatus – この値を UNDER_REVIEW、REVIEWED、または に設定しますINACTIVE。

これらの API オペレーションの詳細については、前の手順のリンクのいずれかを選択して、AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

評価のステータスを変更する準備ができたら、「」を参照してくださいで評価のステータスを非アクティブに変更する AWS Audit Manager。

で評価のステータスを非アクティブに変更する AWS Audit Manager

評価のための証拠収集が不要になったら、評価のステータスを非アクティブに変更できます。評価のステータスが非アクティブに変わると、評価による証拠収集が停止します。停止後、その評価の料金は発生しなくなります。

証拠収集を停止することに加えて、Audit Manager は、非アクティブな評価内にあるコントロールに次の変更を加えます。

- すべてのコントロールセットが [レビュー済み] ステータスに変わります。
- [レビュー中] のすべてのコントロールが [レビュー済み] ステータスに変わります。
- 非アクティブな評価の受任者は、それ以降、そのコントロールとコントロールセットを表示または編集できなくなります。

前提条件

次の手順では、以前に評価を作成し、その現在のステータスがアクティブであることを前提としています。

IAM アイデンティティに、 で評価を管理するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して評価ステータスを更新できますAWS CLI。

> **Warning**
>
> このアクションを元に戻すことはできません。慎重に続行し、評価を非アクティブとしてマークすることを確認することをお勧めします。評価が非アクティブの場合、その内容への読み取り専用のアクセス権のみです。これは、以前に収集した証拠を引き続き確認し、評価レポートを生成できることを意味します。ただし、非アクティブな評価の編集、コメントの追加、手動証拠のアップロードはできません。

Audit Manager console

Audit Manager コンソールで評価ステータスを非アクティブに変更するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[評価] を選択します。
3. 評価を開くには、その名前を選択します。
4. ページの右上にある [評価ステータスを更新] を選択してから、[非アクティブ] を選択します。
5. ポップアップウィンドウで [ステータスを更新] を選択して、ステータスを非アクティブに変更することを確認します。

評価とそのコントロールの変更は、約 1 分後に有効になります。

AWS CLI

で評価ステータスを非アクティブに変更するには AWS CLI

1. まず、更新する評価を特定します。そのために、list-assessments コマンドを実行します。

```
aws auditmanager list-assessments
```

回答は評価のリストを返します。非アクティブ化する評価を検索して、評価 ID をメモします。

2. 次に、 update-assessment-status コマンドを実行し、次のパラメータを指定します。

- `--assessment-id`—このパラメータを使用して、非アクティブにする評価を指定します。
- `--status` – この値を `INACTIVE` に設定します。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
```

評価とそのコントロールの変更は、約 1 分後に有効になります。

Audit Manager API

API を使用して評価ステータスを非アクティブに変更するには

1. ListAssessments オペレーションを使用して、非アクティブ化する評価を検索し、評価 ID を書き留めます。
2. UpdateAssessmentStatus オペレーションを使用して、次のパラメータを指定します。

- AssessmentID — このパラメータを使用して、非アクティブ化する評価を指定します。
- ステータス — この値を `INACTIVE` に設定します。

評価とそのコントロールの変更は、約 1 分後に有効になります。

これらの API オペレーションの詳細については、前の手順のリンクのいずれかを選択して、AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS

SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

非アクティブな評価が不要になったことを確認したら、評価を削除して Audit Manager 環境をクリーンアップできます。手順については、「での評価の削除 AWS Audit Manager」を参照してください。

での評価の削除 AWS Audit Manager

評価が不要になった場合は、Audit Manager 環境から削除できます。これにより、ワークスペースをクリーンアップし、現在のタスクと優先順位に関連する評価に集中できます。

> **Tip**
>
> コストの削減を目的としている場合は、評価のステータスを削除するのではなく、非アクティブに変更することを検討してください。このアクションにより証拠の収集が停止し、評価が読み取り専用の状態になります。この状態では、以前に収集された証拠を確認できます。非アクティブな評価で、料金が発生することはありません。

前提条件

次の手順では、以前に評価を作成していることを前提としています。

IAM アイデンティティに、 で評価を削除するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して評価を削除できますAWS CLI。

> **Warning**
>
> このアクションにより、評価と収集されたすべての証拠が完全に削除されます。削除したデータを復元することはできません。そのため、評価の削除は確認の上、慎重に行ってください。

Audit Manager console

Audit Manager コンソールで評価を削除するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[評価] を選択します。
3. 削除する評価を選択し、[削除] を選択します。

AWS CLI

で評価を削除するには AWS CLI

1. まず、削除する評価を特定します。そのために、list-assessments コマンドを実行します。

   ```
   aws auditmanager list-assessments
   ```

   回答は評価のリストを返します。削除する評価を検索して、評価 ID をメモします。
2. 次に、delete-assessment コマンドを使用して、削除する評価の `--assessment-id` を指定します。

   次の例では、次の *placeholder text* を独自の情報に置き換えます。

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

Audit Manager API

API を使用して評価を削除するには

1. ListAssessments オペレーションを使用して、削除する評価を検索します。

回答の、評価 ID をメモします。

2. DeleteAssessment オペレーションを使用して、削除する評価の assessmentId を指定します。

これらの API 操作の詳細については、前述のリンクのいずれかを選択して「AWS Audit Manager API リファレンス」をご覧ください。これには言語固有の AWS SDK の 1 つでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

追加リソース

Audit Manager のデータ保持の詳細については、「」を参照してくださいAudit Manager のデータの削除。

での委任 AWS Audit Manager

で評価プロセスを進めると AWS Audit Manager、収集した証拠を確認および検証するために対象分野の専門家からのサポートが必要になる場合があります。そこで、委任の概念が登場します。

重要ポイント

委任により、監査所有者は特定のコントロールセットを受任者に割り当てることができます。受任者は、関連分野の専門知識を持つ個人です。委任機能を使用することで、各コントロールの証拠が適切な担当者によって徹底的に評価されるようにできます。これにより、レビュープロセスを合理化し、評価の全体的な精度と信頼性を高めることができます。技術的証拠の解釈、コンプライアンス要件の明確化、特定のドメインに関するより深いインサイトの取得に関するガイダンスが必要な場合でも、委任により対象分野の専門家と効果的にコラボレーションできます。

大まかに言うと、委任プロセスは次のとおりです。

1. 監査所有者は、評価でコントロールセットを選択し、レビューのためにそれを委任します。
2. 受任者は、これらのコントロールとその証拠を確認し、終了時にコントロールセットを監査所有者に送信します。
3. 監査所有者は、レビューが完了した旨の通知を受け取り、レビューされたコントロールに受任者からの備考がないかを確認します。

> **Note**
>
> は、監査所有者でも、異なる の代理人でも AWS アカウント かまいません AWS リージョン。

追加リソース

この章の以下のセクションでは、 で委任タスクを管理する方法について詳しく説明します AWS Audit Manager。

- 監査所有者向けのさまざまな委任タスクを理解する
  - でレビューするコントロールセットの委任 AWS Audit Manager
  - で送信した委任の検索と確認 AWS Audit Manager

監査所有者向けのさまざまな委任タスクを理解する

の監査所有者は AWS Audit Manager、評価を管理し、組織内のコンプライアンスを確保する責任があります。ガバナンス、リスク、コンプライアンスに関する専門知識はありますが、特定の技術的証拠やコントロールを確認および解釈するために、対象分野の専門家から質問を受けたり、サポートを必要としたりすることがあります。ここでは、Audit Manager の委任機能が役立ちます。

重要ポイント

委任を作成すると、評価内のコントロールセットを、関連分野の専門知識や技術的な専門知識を持つ他の Audit Manager ユーザー (代理人 と呼ばれる) に割り当てることができます。これらの代理人は、割り当てられたコントロールセットの確認、収集された証拠の分析、必要に応じてコメントや追加の証拠の提供、個々のコントロールのステータスの更新を行うことができます。

委任プロセスでは、組織内の総合的な専門知識を活用することで、コントロールのレビューと検証を効率化します。これにより、最も資格のある担当者によって各コントロールが徹底的に評価され、評価の精度と信頼性が向上します。

追加リソース

以下のセクションでは、監査所有者としての委任の管理に関連するさまざまなタスクについて説明します。これには、コントロールセットの委任、委任のステータスの追跡、完了した委任の管理の方法が含まれます。委任を効果的に使用することで、対象分野の専門家と協力して専門知識を活用し、Audit Manager 内で包括的で十分な情報に基づいた監査プロセスを維持できます。

- でレビューするコントロールセットの委任 AWS Audit Manager
- で送信した委任の検索と確認 AWS Audit Manager
- で完了した委任の削除 AWS Audit Manager

でレビューするコントロールセットの委任 AWS Audit Manager

対象分野の専門家からのサポートが必要な場合は、サポートする を選択し AWS アカウント 、レビューのためにコントロールセットを委任できます。

前提条件

IAM アイデンティティに、 で委任を作成するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

次の手順のいずれかを使用して、コントロールセットを委任できます。

評価ページからのコントロールセットの委任

評価ページからコントロールセットを委任するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Assessment] (評価) を選択します。
3. 委任するコントロールセットを含む評価の名前を選択します。
4. 評価ページから、[Controls] (コントロール) タブを選択します。これにより、コントロールステータスの概要と評価のコントロールのリストが表示されます。
5. コントロールセットを選択し、[Delegate control set] (コントロールセットを委任) を選択します。
6. [Delegate selection] (委任の選択) の下に、ユーザーとロールのリストが表示されます。ユーザーまたはロールを選択するか、検索バーを使用してそれらを探します。
7. [Delegation details] (委任の詳細) で、コントロールセット名と評価名を確認します。
8. (オプション) [Comments] (コメント) で、受任者がレビュータスクを実行するのに役立つ手順を含むコメントを追加します。コメントに機密情報を含めないでください。
9. [Delegate control set] (コントロールセットを委任) を選択します。
10. 緑の成功バナーは、コントロールセットの委任が成功したことを示します。[View delegation] (委任を表示) を選択して、委任リクエストを表示します。 AWS Audit Manager コンソールの左側のナビゲーションペインで委任を選択すると、いつでも委任を表示することもできます。

委任のページからのコントロールセットの委任

委任のページからコントロールセットを委任するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Delegations] (委任) を選択します。
3. 委任のページから、[Create delegation] (委任を作成) を選択します。
4. [Choose assessment and control set] (評価とコントロールセットを選択) で、委任する評価とコントロールセットを指定します。
5. [Delegate selection] (委任の選択) の下に、ユーザーとロールのリストが表示されます。ユーザーまたはロールを選択するか、検索バーを使用してそれらを探します。
6. (オプション) [Comments] (コメント) で、受任者がレビュータスクを実行するのに役立つ手順を含むコメントを追加します。コメントに機密情報を含めないでください。
7. [Create delegation] (委任を作成) を選択します。
8. 緑の成功バナーは、コントロールセットの委任が成功したことを示します。[View delegation] (委任を表示) を選択して、委任リクエストを表示します。 AWS Audit Manager コンソールの左側のナビゲーションペインで委任を選択すると、いつでも委任を表示することもできます。

レビュー用にコントロールセットを委任すると、代理人は通知を受け取り、コントロールセットのレビューを開始できます。受任者が従うこのプロセスは 代理人のさまざまな委任タスクを理解する に記載されています。

次のステップ

後日委任を再確認するには、「」を参照してくださいで送信した委任の検索と確認 AWS Audit Manager。

で送信した委任の検索と確認 AWS Audit Manager

Audit Manager の左側のナビゲーションペインで委任を選択すると、いつでも委任のリストにアクセスできます。委任ページには、アクティブな委任と完了した委任のリストが含まれています。

委任が完了すると、Audit Manager に通知が送信されます。代理人からコメント付きのコメントを受け取る場合もあります。次の手順では、委任が完了した後に Audit Manager で委任を確認する方法と、委任によって残された可能性のあるコメントを表示する方法について説明します。

前提条件

IAM アイデンティティに、 で委任を表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

以前に作成した委任を検索して確認するには、次の手順に従います。

完了済みの委任を表示し、コメントを確認するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Delegations] (委任) を選択します。
3. 委任ページを確認します。このページには、次の情報を含むテーブルが含まれています。

名前	説明
に委任	コントロールセットを AWS アカウント 委任した 。
日付	コントロールセットを委任した日付。
[ステータス]	委任の現在のステータス。
[評価]	評価の詳細ページへのリンクを含む評価の名前。
コントロールセット	レビューのために委任されたコントロールセットの名前。

4. 受任者がレビューして送信した評価とコントロールセットを見つけ、評価の名前を選択して開きます。
5. 評価の詳細のページの [Controls] (コントロール) タブで、[Control sets] (コントロールセット) の表が表示されるまで下方向にスクロールします。
6. コントロールセット でグループ化されたコントロール で、委任したコントロールセットの名前を見つけます。
7. コントロールセットの名前を展開してコントロールを表示し、コントロールの名前を選択してコントロールの詳細ページを開きます。

8. [Comments] (コメント) タブを選択して、その特定のコントロールについて受任者によって追加された備考を表示します。
9. コントロールセットのレビューが完了したことを確認したら、コントロールセットを選択し、「コントロールセットのレビューを完了」を選択します。

> **Important**
>
> Audit Manager は継続的に証拠を収集します。その結果、受任者がコントロールのレビューを完了した後に、追加の新しい証拠が収集される可能性があります。
> 評価レポートでレビュー済みの証拠のみを使用する場合は、[control reviewed] (レビュー済みコントロール) のタイムスタンプを参照して、証拠がいつレビューされたかを判断できます。このタイムスタンプは、コントロールの詳細ページの Changelog タブ にあります。その後、このタイムスタンプを使用して、評価レポートに追加する証拠を特定できます。

次のステップ

委任が完了し、不要になった委任を削除するには、「」を参照してくださいで完了した委任の削除 AWS Audit Manager。

で完了した委任の削除 AWS Audit Manager

委任を作成したが、後でそのコントロールセットをレビューするためのサポートが不要になる場合があります。この場合、Audit Manager でアクティブな委任を削除できます。委任ページに表示されなくなった完了した委任を削除することもできます。

前提条件

IAM アイデンティティに、 で委任を削除するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

委任を削除するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Delegations] (委任) を選択します。
3. [Delegations] (委任) ページで、キャンセルする委任を選択してから、[Remove delegation] (委任を削除) を選択します。
4. 表示されるポップアップウィンドウで、[Delete] (削除) を選択して選択内容を確認します。

代理人のさまざまな委任タスクを理解する

の代理人は AWS Audit Manager、評価プロセス中に監査所有者をサポートする上で重要な役割を果たします。監査所有者は評価を管理し、全体的なコンプライアンスを確保する責任がありますが、専門分野外の特定の技術的証拠のレビューと解釈について、対象分野の専門家からの支援が必要になる場合があります。このようなシナリオでは、知識とスキルが重要になります。

重要ポイント

委任機能を使用すると、監査所有者は、特定のコントロールセットをレビュー用に割り当て、専門的なビジネスまたは技術の専門知識を活用できます。この共同アプローチは、評価の精度と信頼性を高めるだけでなく、レビュープロセスを合理化し、監査所有者が中核的な責任に集中できるようにすると同時に、専門知識が最も価値のある分野に集中できるようにします。

委任されたユーザーは、割り当てられたコントロールセットに関連する証拠をレビューするリクエストを監査所有者から受け取る場合があります。コントロールセットとそれに関連する証拠のレビュー、コメントの追加、追加の証拠のアップロード、およびレビューする各コントロールのステータスの更新を行うことを通じて、監査所有者をサポートできます。

> **Note**
>
> 監査所有者は、評価全体ではなく、レビューする特定のコントロールセットを委任します。その結果、代表者による評価へのアクセスが制限されます。受任者は、証拠のレビュー、コメントの追加、手動証拠のアップロード、コントロールセット内の各コントロールについてのコントロールステータスの更新を行うことができます。Audit Manager のロールと許可の

詳細については、「 のユーザーペルソナに推奨されるポリシー AWS Audit Manager」を参照してください。

追加リソース

以下のセクションでは、委任の管理に関連するタスクの詳細について説明します。これには、受信した委任リクエストの表示、割り当てられたコントロールセットの確認、コメントと追加の証拠の提供、レビューしたコントロールを監査所有者に送信する方法が含まれます。

- 受信した委任リクエストの通知の表示
- 委任されたコントロールセットとそれに関連する証拠のレビュー
- コントロールセットのレビュー中にコントロールに関するコメントを追加する
- でレビューされたコントロールのマーク AWS Audit Manager
- レビュー済みコントロールセットの監査所有者への送信

受信した委任リクエストの通知の表示

監査所有者がコントロールセットのレビューについてサポートをリクエストすると、委任されたコントロールセットを知らせる通知が届きます。

前提条件

IAM アイデンティティに、 で通知を表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

通知を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Notifications] (通知) を選択します。
3. [Notifications] (通知) ページで、レビューのために自分に委任されたコントロールセットのリストを確認します。表には、次の情報が含まれます。

名前	説明
日付	コントロールセットが委任された日付。
[評価]	コントロールセットに関連付けられている評価の名前。
コントロールセット	コントロールセットの名前。
ソース	コントロールセットを委任したユーザーまたはロール。
説明	監査所有者から提供される指示。

> **Tip**
>
> また、SNS トピックをサブスクライブして、レビューのためにコントロールセットが委任されたときに E メールによるアラートを受信することもできます。詳細については、「の通知 AWS Audit Manager」を参照してください。

次のステップ

委任されたコントロールの確認を開始する準備ができたら、「」を参照してください委任されたコントロールセットとそれに関連する証拠のレビュー。

委任されたコントロールセットとそれに関連する証拠のレビュー

監査所有者から委任されたコントロールセットをレビューすることで、監査所有者をサポートできます。

これらのコントロールとそれに関連する証拠を調べて、追加のアクションが必要かどうかを判断できます。このような追加のアクションには、コンプライアンスを実証するために追加の証拠を手動でアップロードしたり、実行した是正手順の詳細を示すコメントを残したりすることが含まれる場合があります。

前提条件

IAM アイデンティティに、 でコントロールセットを表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS

Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

コントロールセットをレビューするには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Notifications] (通知) を選択します。
3. 通知ページには、委任されたコントロールセットのリストが表示されます。レビューするコントロールセットを特定し、関連する評価の名前を選択して、評価の詳細のページを開きます。
4. 評価の詳細のページの [Controls (コントロール)] タブで、[Control sets (コントロールセット)] の表が表示されるまでスクロールダウンします。
5. [Controls grouped by control set (コントロールセット別にグループ化されたコントロール)] の列で、コントロールセットの名前を展開して、そのコントロールを表示します。
6. コントロールの名前を選択して、コントロールの詳細のページを開きます。
7. (オプション) コントロールのステータスを変更するには、[Update control status (コントロールのステータスを更新)] を選択します。レビュー中、ステータスを [Under Review (レビュー中)] としてマークできます。
8. 証拠フォルダ 、詳細 、データソース 、コメント 、変更ログ タブでコントロールに関する情報を確認します。

   - これらの各タブと、タブに含まれるデータを理解する方法については、「」を参照してくださいでの評価コントロールの確認 AWS Audit Manager。

コントロールの証拠をレビューするには

1. コントロールの詳細のページから、[Evidence folders (証拠フォルダ)] タブを選択します。
2. 証拠フォルダテーブルに移動して、そのコントロールの証拠を含むフォルダのリストを表示します。これらのフォルダは、証拠が収集された日付に基づいて編成され、名前が付けられます。
3. 証拠フォルダの名前を選択して開きます。その後、その日に収集されたすべての証拠の概要を確認できます。

   - この概要には、、 AWS Security Hub AWS Configまたはその両方から直接報告されたコンプライアンスチェックの問題の総数が含まれます。

- この情報の詳細については、「」を参照してくださいでの証拠フォルダの確認 AWS Audit Manager。

4. 証拠フォルダの概要のページから、証拠の表に移動します。Time 列で、開く証拠を選択します。
5. 証拠の詳細を確認します。

- この情報の詳細については、「」を参照してくださいでの証拠の確認 AWS Audit Manager。

次のステップ

場合によっては、コンプライアンスを実証するために追加の証拠を提供する必要があります。このような場合、証拠を手動でアップロードできます。手順については、「での手動証拠の追加 AWS Audit Manager」を参照してください。

委任された 1 つ以上のコントロールに関するコメントを残す場合は、「」を参照してくださいコントロールセットのレビュー中にコントロールに関するコメントを追加する。

コントロールセットのレビュー中にコントロールに関するコメントを追加する

レビューしたコントロールにコメントを追加できます。監査所有者は、これらのコメントを確認できます。

前提条件

IAM アイデンティティに、 の評価コントロールにコメントを追加するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

コントロールにコメントを追加するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Notifications] (通知) を選択します。
3. [Notifications] (通知) ページで、自分に委任されたコントロールセットのリストを確認します。

4. コメントを残したいコントロールを含むコントロールセットを見つけ、関連する評価の名前を選択して評価を開きます。
5. [Controls (コントロール)] タブを選択し、[Control sets (コントロールセット)] の表が表示されるまでスクロールダウンして、コントロールの名前を選択して開きます。
6. [Comments (コメント)] タブを選択します。
7. [Send comments (コメントを送信)] で、テキストボックスにコメントを入力します。
8. コメントを追加するには、[Submit comment (コメントを送信)] を選択します。コメントは、ページの前のコメントセクションと、このコントロールに関するその他のコメントの下に表示されます。

次のステップ

コントロールの確認が完了したら、「」の手順に従いますでレビューされたコントロールのマーク AWS Audit Manager。

でレビューされたコントロールのマーク AWS Audit Manager

コントロールセット内の個々のコントロールのステータスを更新することで、レビューの進行状況を示すことができます。

コントロールステータスの変更はオプションです。しかし、そのコントロールのレビューを完了する際には、各コントロールのステータスを [Reviewed] (レビュー済み) に変更することをお勧めします。個々のコントロールのステータスにかかわらず、監査所有者にコントロールを送信できます。

前提条件

IAM アイデンティティに、 で評価コントロールのステータスを更新するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

コントロールを [reviewed] (レビュー済み) としてマークするには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。

2. 左側のナビゲーションペインで、[Notifications] (通知) を選択します。
3. [Notifications] (通知) ページで、自分に委任されたコントロールセットのリストを確認します。
4. レビュー済みとしてマークするコントロールセットを見つけ、関連する評価の名前を選択して評価を開きます。
5. 評価の詳細のページの [Controls (コントロール)] タブで、[Control sets (コントロールセット)] の表が表示されるまでスクロールダウンします。
6. [Controls grouped by control set (コントロールセット別にグループ化されたコントロール)] の列で、コントロールセットの名前を展開して、そのコントロールを表示します。
7. コントロールの名前を選択して、コントロールの詳細のページを開きます。
8. [Update control status (コントロールのステータスを更新)] を選択し、ステータスを [Reviewed(レビュー済み)] に変更します。
9. 表示されるポップアップウィンドウで、[Update control status (コントロールのステータスを更新)] を選択して、コントロールのレビューが終了したことを確認します。

次のステップ

委任プロセスを完了するには、「」を参照してくださいレビュー済みコントロールセットの監査所有者への送信。

レビュー済みコントロールセットの監査所有者への送信

コントロールセットの確認、コメントや追加の証拠の追加、個々のコントロールのステータスの更新が完了したら、レビューされたコントロールセットを監査所有者に返送するという重要なステップに到達します。レビュー済みコントロールセットを送信すると、委任されたタスクの完了がマークされ、監査所有者はインサイトとレコメンデーションを全体的な評価に組み込むことができます。

前提条件

IAM アイデンティティに、レビューされたコントロールセットを の監査所有者に返送するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、 AWS Audit Managerへの完全な管理者アクセス権を許可すると ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

コントロールセットを監査所有者に送信するには、次の手順に従います。

レビュー済みコントロールセットを監査所有者に送信するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Notifications] (通知) を選択します。
3. 自分に委任されたコントロールセットのリストを確認します。監査所有者に送信するコントロールセットを見つけて、関連する評価の名前を選択します。
4. [Control sets] (コントロールセット) の表が表示されるまで下方向にスクロールし、監査所有者に送信するコントロールセットを選択してから、[Submit for review] (レビューのために送信) を選択します。
5. 表示されるポップアップウィンドウで、[Submit for review] (レビューのために送信) を選択する前に、コメントを追加できます。

評価レポート

評価レポートには、評価のために収集された証拠のうち、選択された証拠の要約が記載されます。また、各証拠の詳細が記載された PDF ファイルへのリンクも含まれています。評価レポートの具体的な内容、構成、および命名ルールは、レポート生成時点で選択したパラメータによって異なります。

評価レポートは、監査に関連する証拠を選択して編集するのに役立ちます。ただし、証拠そのものの適合性は評価しません。代わりに、Audit Manager は、選択された証拠の詳細を監査人と共有できる出力として提供するだけです。

目次

評価レポートのフォルダ構造を理解する

評価レポートをダウンロードしたら、Audit Manager は zip フォルダを作成します。これには、評価レポートと関連する証拠ファイルがネストされたサブフォルダに格納されます。

フォルダは次のような構造になっています。

- 評価フォルダ (例:myAssessmentName-a1b2c3d4) — ルートフォルダ。
  - 評価レポートフォルダ (例: reportName-a1b2c3d4e5f6g7) – AssessmentReportSummary.pdf、 digest.txt、README.txt ファイルがあるサブフォルダ。
    - エビデンス・バイ・コントロール・フォルダ (例:controlName-a1b2c3d4e5f6g) — 証拠ファイルを関連するコントロールごとにグループ化するサブフォルダ。
      - データソース別証拠フォルダ (例:CloudTrail,Security Hub) — 証拠ファイルをデータソースタイプ別にグループ化するサブフォルダ。
        - 日付別証拠フォルダ (例:2022-07-01) — 証拠ファイルを証拠収集日ごとにグループ化するサブフォルダ。
          - 証拠ファイル — 個々の証拠に関する詳細を含むファイル。

評価レポートのナビゲーション

まず、zip フォルダを開き、1 レベル下の評価レポートフォルダに移動します。ここには、評価レポートの PDF と README.txt ファイルがあります。

README.txt ファイルを見れば、zip フォルダの構造と内容を理解できます。また、各ファイルの命名ルールに関する参照情報も記載されています。この情報は、特定のアイテムを探している場合に、サブフォルダまたは証拠ファイルに直接移動するのに役立ちます。

それ以外の場合、証拠を参照して必要な情報を見つけるには、評価レポートの PDF を開いてください。これにより、レポートの概要と、レポートの作成元となった評価の概要が表示されます。

概要を読んだ後、目次 (TOC) を使用してレポートを調べます。目次内のハイパーリンクが設定されたコントロールを選択すると、そのコントロールの概要に直接移動できます。

コントロールの証拠の詳細をレビューする準備ができたら、ハイパーリンクが設定された証拠名を選択してレビューできます。自動証拠については、ハイパーリンクが設定された名前をクリックすると、その証拠の詳細が記載された新しい PDF ファイルが開きます。手動証拠については、ハイパーリンクをクリックすると、手動証拠を含む S3 バケットに移動します。

> **Tip**
>
> コントロールと証拠を参照する際、各ページ上部のパンくずリストナビゲーションには、評価レポートにおける現在の場所が表示されます。ハイパーリンクが設定された TOC を選択して、いつでも TOC に戻ることができます。

評価レポートのセクションの確認

次のセクションには、評価レポートの各セクションに関する情報が記載されています。

> **Note**
>
> 次のセクションのデータ属性の横にハイフン (-) が表示されている場合は、その属性の値が null であるか、値が存在しないことを示しています。

カバーページ

カバーページには、評価レポートの名前が含まれています。また、レポートが生成された日時と、評価レポートを生成したユーザーのアカウント ID も表示されます。

カバーページの形式は以下のとおりです。Audit Manager は、*########*をレポートに関連する情報に置き換えます。

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

概要ページ

概要ページは、レポート自体の概要と、レポートの生成元である評価の概要の 2 つのパートで構成されます。

レポートの概要

このセクションでは、評価レポートを要約します。

名前	説明
レポート名	レポートの名前。
説明	監査所有者がレポートを生成するときに入力する説明。
生成された日付	レポートが生成された日付。時刻は、協定世界時 (UTC) で表されます。
含まれるコントロールの合計	レポートに含まれ、証拠を収集したコントロールの数。これは、評価におけるコントロールの総数のサブセットです。
AWS アカウント 含まれている	レポート AWS アカウント に含まれ、証拠を収集した の数。これは、 AWS アカウント 評価の の合計数のサブセットです。
評価レポートの選択	レポートに含めるために選択された証拠項目の数。これには、レポートで見つかったコンプライアンスチェックの問題の総数が含まれます。

評価の概要

このセクションでは、レポートに関連する評価を要約します。

名前	説明
評価名	レポートが生成された評価の名前。
[ステータス]	レポートが生成された時点の評価のステータス。
評価対象リージョン	評価 AWS リージョン が作成された 。
AWS アカウント 範囲内	評価の範囲内 AWS アカウント にある のリスト。
フレームワーク名	評価が作成されたフレームワークの名前。
監査所有者	評価の監査所有者のユーザーまたはロール。
最終更新日	評価が最後に更新された日付。時間は UTC 表記です。

目次ページ

目次には、評価レポートのすべてのコンテンツが表示されます。コンテンツは、評価に含まれるコントロールセットに基づいてグループ化および編成されます。コントロールは、それぞれのコントロールセットの下にリストされます。

目次で任意の項目を選択すると、レポートのそのセクションに直接移動できます。コントロールセット、または個々のコントロールのいずれでも選択可能です。

コントロールのページ

コントロールのページは、コントロール自体の概要と、コントロールに対して収集された証拠の概要の 2 つの部分があります。

コントロールの概要

このセクションでは、次の情報を紹介します。

名前	説明
コントロール名	コントロールの名前。
説明	コントロールの説明。
コントロールセット	コントロールが属するコントロールセットの名前。
テスト情報	このコントロールに推奨されるテスト手順。
アクションプラン	コントロールが満たされない場合に実行する推奨アクション。
評価レポートの選択	評価レポートに含まれていた、このコントロールに関連する証拠項目の数。このコントロールの証拠に対して検出されたコンプライアンスチェックの問題の数。

収集した証拠

このセクションには、コントロールのために収集された証拠が表示されます。証拠はフォルダごとにグループ化され、証拠の収集日によって整理され、名前が付けられます。各証拠フォルダ名の横に、そのフォルダに対するコンプライアンスチェックの問題の総数が表示されます。

各証拠フォルダ名の下には、ハイパーリンクが設定された証拠名のリストがあります。

- 自動証拠名は、証拠収集のタイムスタンプで始まり、サービスコード、イベント名 (最大 20 文字)、アカウント ID、および 12 文字の一意の ID が続きます。

  例：`21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  自動証拠については、設定されたハイパーリンク名をクリックすると、概要と詳細が記載された新しい PDF ファイルが開きます。
- 手動証拠名は証拠のアップロードタイムスタンプで始まり、その後に `manual` ラベル、アカウント ID、12 文字の一意 ID が続きます。また、ファイル名の最初の 10 文字とファイル拡張子 (最大 10 文字) も含まれます。

  例：`00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  手動証拠については、設定されたハイパーリンク名をクリックすると、その証拠を含む S3 バケットに移動します。

各証拠名の横には、その項目のコンプライアンスチェックの結果が表示されます。

- AWS Security Hub または から収集された自動証拠については AWS Config、準拠 、非準拠 、または判定不能 の結果が報告されます。
- AWS CloudTrail および API コールから収集された自動証拠、およびすべての手動証拠については、判定不能の結果が表示されます。

証拠の概要ページ

証拠の概要ページには、次の情報が含まれています。

名前	説明
ID	証拠の一意の識別子。
収集日	証拠が作成またはアップロードされた日付。
説明	アカウント ID とデータソースタイプを含む証拠の説明。
評価名	レポートが生成された評価の名前。

名前	説明
フレームワーク名	評価が作成されたフレームワークの名前。
コントロール名	証拠がサポートするコントロールの名前。
コントロールセット名	関連するコントロールが属するコントロールセットの名前。
コントロールの説明	証拠がサポートするコントロールの説明。
テスト情報	コントロールの推奨テスト手順。
アクションプラン	コントロールが満たされない場合に実行する推奨アクション。
AWS リージョン	証拠に関連付けられているリージョンの名前。
IAM ID	証拠に関連付けられているユーザーまたはロールの ARN。
AWS アカウント	証拠に関連付けられている AWS アカウント ID。
AWS のサービス	証拠に関連付けられている AWS のサービス の名前。
イベント名	証拠イベントの名前。
イベント時間	証拠イベントが発生した時刻。
データソース	証拠が収集またはアップロードされた場所。データソースタイプは、 AWS Config、Security Hub、 AWS API コール CloudTrail、または手動のいずれかです。
タイプ別の証拠	証拠のカテゴリ • コンプライアンスチェックの証拠は、 AWS Config または Security Hub から収集されます。 • ユーザーアクティビティの証拠は CloudTrail ログから収集されます。 • 設定データの証拠は、他の のスナップショットから収集されます AWS のサービス。 • 手動の証拠は、手動でアップロードした証拠です。

名前	説明
コンプライアンスチェックのステータス	コンプライアンスチェックカテゴリに該当する証拠の評価ステータス。 • AWS Security Hub または から収集された自動証拠の場合 AWS Config、準拠 、非準拠 、または判定不能 の結果が報告されます。 • AWS CloudTrail および API コールから収集された自動証拠、およびすべての手動証拠については、判定不能の結果が表示されます。

証拠の詳細ページ

証拠の詳細ページには、証拠の名前と証拠の詳細の表が表示されます。この表では、証拠の各要素の詳細な内訳を確認して、データを理解し、それが正しいことを検証できます。証拠の詳細ページの内容は、証拠のデータソースによって異なります。

> **Tip**
>
> 証拠の詳細を参照する際、各ページ上部のパンくずナビゲーションには、現在の場所が表示されます。ハイパーリンクが設定された証拠の概要の名前を選択して、いつでも証拠の概要に戻ることができます。

評価レポートの検証

評価レポートを生成すると、Audit Manager は `digest.txt` レポート ファイルの checksum を生成します。このファイルを使用してレポートの整合性を検証し、レポートの作成後に証拠が変更されていないことを確認できます。このファイルには、レポートアーカイブの一部が変更されると無効になる署名とハッシュを含む JSON オブジェクトが含まれています。

評価レポートの整合性を検証するには、Audit Manager が提供する ValidateAssessmentReportIntegrity API を使用します。

追加リソース

一般的な質問や問題に対する回答を見つけるには、このガイドの評価レポートの問題のトラブルシューティング「トラブルシューティング」セクションの「」を参照してください。

証拠ファインダー

証拠ファインダーは、Audit Manager で証拠を検索するための強力な手段です。検索する際に、深くネストされた証拠フォルダを閲覧する代わりに、証拠ファインダーを使用して証拠をすばやく検索できるようになりました。委任された管理者として Evidence Manager を使用している場合は、組織内のすべてのメンバーアカウントで証拠を検索できます。

フィルターとグルーピングを組み合わせて使用することで、検索クエリの範囲を徐々に絞り込むことができます。例えば、システムの状態を大まかに把握したい場合は、広範囲にわたる検索を行い、評価、日付範囲、およびリソースコンプライアンスに基づいてフィルタリングします。特定のリソースを修復することが目的であれば、特定の統制 ID またはリソース ID の証拠を絞り込んで絞り込むことができます。フィルターを定義したら、評価レポートを作成する前に、一致する検索結果をグループ化してプレビューできます。

エビデンスファインダーを使用するには、Audit Manager の設定からこの機能を有効にする必要があります。

重要ポイント

証拠ファインダーが Lake と CloudTrailどのように連携するかを理解する

証拠ファインダーは AWS CloudTrail Lake のクエリ機能とストレージ機能を使用します。証拠ファインダーの使用を開始する前に、 CloudTrail Lake の仕組みについてもう少し理解しておくと役に立ちます。

CloudTrail Lake は、強力な SQL クエリをサポートする単一の検索可能なイベントデータストアにデータを集約します。つまり、組織全体のデータをカスタムの時間範囲内で検索できるということです。証拠ファインダーを使用すると、この検索機能をAudit Manager コンソールで直接使用できます。

証拠ファインダーの有効化をリクエストすると、Audit Manager がユーザーに代わってイベントデータストアを作成します。証拠ファインダーを有効にすると、今後の Audit Manager の証拠はすべてイベントデータストアに取り込まれ、証拠ファインダーの検索クエリに使用できるようになります。証拠ファインダーを有効にすると、新しく作成されたイベントデータストアに、過去 2 年分の証拠データがバックフィルされます。委任管理者として証拠ファインダーを有効にすると、組織内のすべてのメンバーアカウントのデータがバックフィルされます。

バックフィルされたものか新しいものかを問わず、すべての証拠データはイベントデータストアに 2 年間保持されます。デフォルトの保持期間は、いつでも変更できます。手順については、「AWS CloudTrail ユーザーガイド」の「イベントデータストアの更新」を参照してください。イベントデータは、イベントデータストアに最大 7 年間 (2,555 日) 保持できます。

> **Note**
>
> 新しい証拠データがイベントデータストアに追加されると、データストレージと取り込みに対して CloudTrail レイク料金が発生します。
> CloudTrail Lake クエリの場合、支払いはそのままです。これは、証拠ファインダーで検索クエリを実行するたびに、スキャンされたデータに対して料金が請求されることを意味します。
> CloudTrail Lake の料金の詳細については、AWS CloudTrail 「 の料金」を参照してください。

次のステップ

開始するには、Audit Manager の設定から証拠ファインダーを有効にします。手順については、「証拠ファインダーの有効化」を参照してください。

追加リソース

- 証拠ファインダーでの証拠の検索
- 証拠ファインダーでの結果の表示
- 証拠ファインダーのフィルターとグループ化のオプション
- 証拠ファインダーのユースケースの例
- 証拠ファインダーの問題のトラブルシューティング

証拠ファインダーでの証拠の検索

証拠ファインダーを使用すると、ターゲットを絞った検索を実行し、関連する証拠をすばやく表示してレビューできます。

このページでは、評価、日付範囲、リソースコンプライアンスステータス、その他の属性などの基準で検索をフィルタリングする方法について説明します。これらのフィルターを適用すると、検索範囲

は必要な証拠だけに絞り込まれます。結果を特定のフィールド別にグループ化して、パターンをより適切に分析することもできます。

前提条件

Audit Manager の設定で証拠ファインダーを有効にする手順を完了していることを確認してください。手順については、「証拠ファインダーの有効化」を参照してください。

さらに、証拠ファインダーで検索クエリを実行するアクセス許可があることを確認してください。使用できるアクセス許可ポリシーの例については、「」を参照してくださいユーザーがエビデンスファインダーで検索クエリを実行できるようにします。

手順

Audit Manager コンソールで証拠を検索するには、次の手順に従います。

1. 検索クエリを実行する
2. 進行中の検索クエリを停止する (オプション)
3. 検索クエリのフィルターを編集する (オプション)

> **Note**
>
> CloudTrail API を使用して証拠データをクエリすることもできます。詳細については、 API リファレンスStartQueryの「」を参照してください。 AWS CloudTrail を使用する場合は AWS CLI、「 ユーザーガイド」の「クエリを開始するAWS CloudTrail 」を参照してください。

検索クエリの実行

証拠ファインダーで検索クエリを実行するには、次の手順に従います。

証拠を検索するには

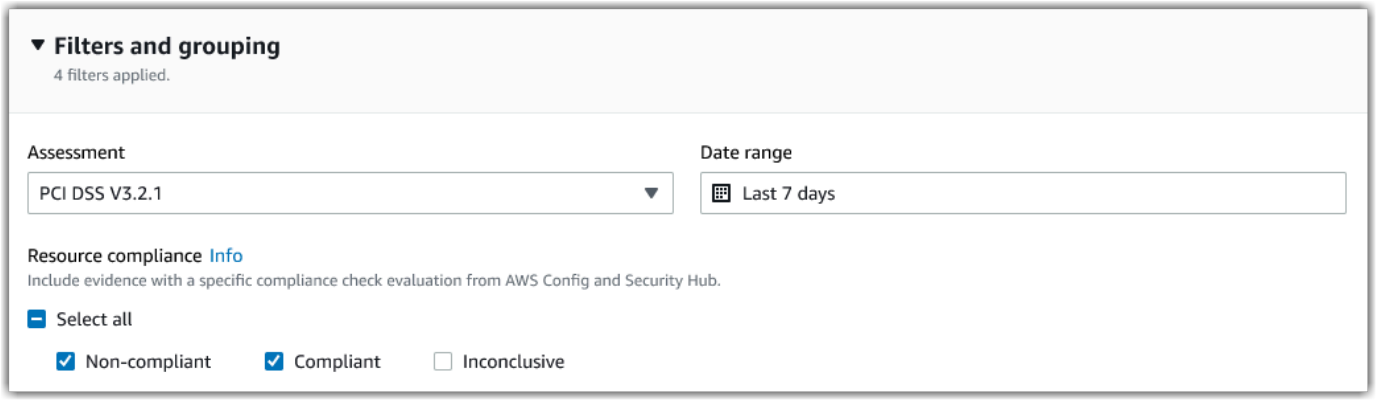
1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[証拠ファインダー] を選択します。

3. 次に、フィルターを適用して検索範囲を絞り込みます。

   a. 評価では、評価を選択します。

   b. 日付範囲では、範囲を選択します。

   c. リソースコンプライアンスでは、評価ステータスを選択します。

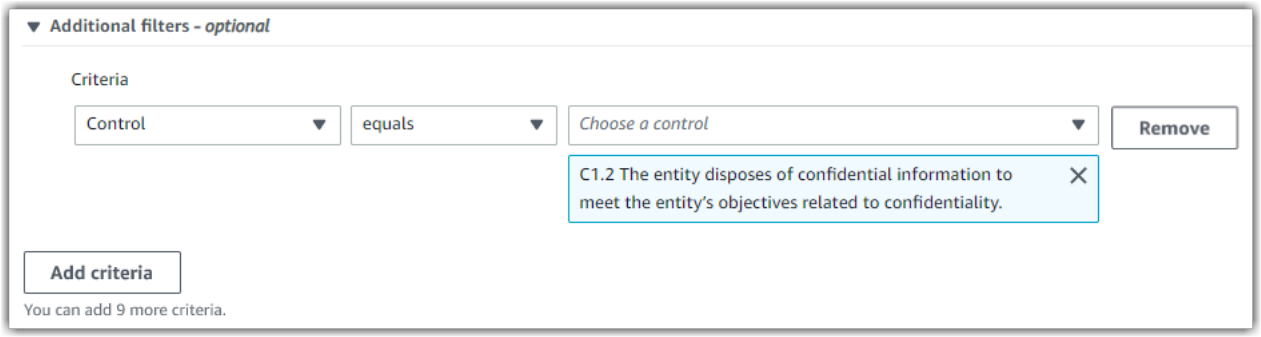


4. (オプション) 検索をさらに絞り込むには、その他のフィルター - オプションを選択します。

   a. 基準を追加を選択し、基準を選択してから、その基準の 1 つまたは複数の値を選択します。

   b. 同じ方法で、さらに多くのフィルターの作成を続けます。

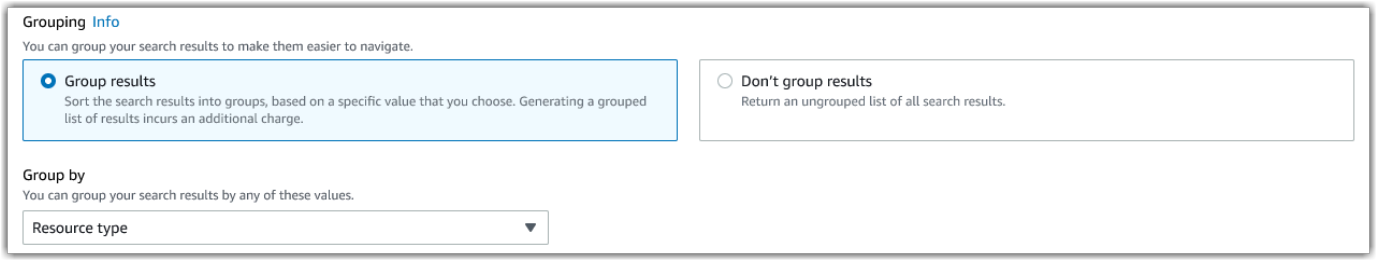
   c. 不要なフィルターを削除するには、削除を選択します。



5. グループ化で、検索結果をグループ化するかどうかを指定します。

   a. 結果をグループ化する場合は、結果をグループ化するための値を選択します。

   b. 結果をグループ化したくない場合は、ステップ 6 に進みます。



6. [検索] を選択します。

所有する証拠データの量によっては、検索に数分かかる場合があります。検索中は、証拠ファインダーから自由に離れることができます。検索結果の準備が整うと、フラッシュバーが通知します。

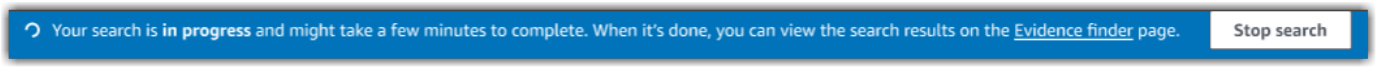
検索クエリの停止

何らかの理由で検索クエリを停止する場合は、以下の手順に従います。

> **Note**
>
> 検索クエリを停止しても、料金が発生する可能性があります。検索クエリを停止する前にスキャンされた証拠データの量に対して料金が発生します。停止すると、返された部分的な結果を確認できます。

進行中の検索クエリを停止するには

1. 画面上部にある青い進行状況フラッシュバーで、検索を停止を選択します。



2. (オプション) 検索クエリを停止する前に返された部分的な結果を確認します。

   a. 証拠ファインダーページを開いている場合は、結果の一部が画面に表示されます。

   b. 証拠ファインダーから離れた場合は、緑色の確認フラッシュバーで部分的な結果を表示を選択します。

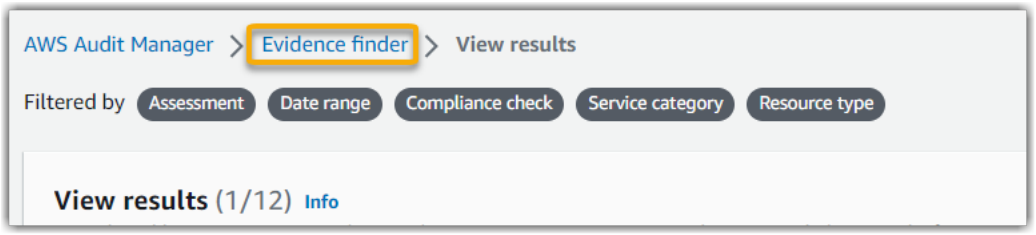
検索フィルターの編集

以下の手順に従って最新の検索クエリに戻り、必要に応じてフィルターを調整します。

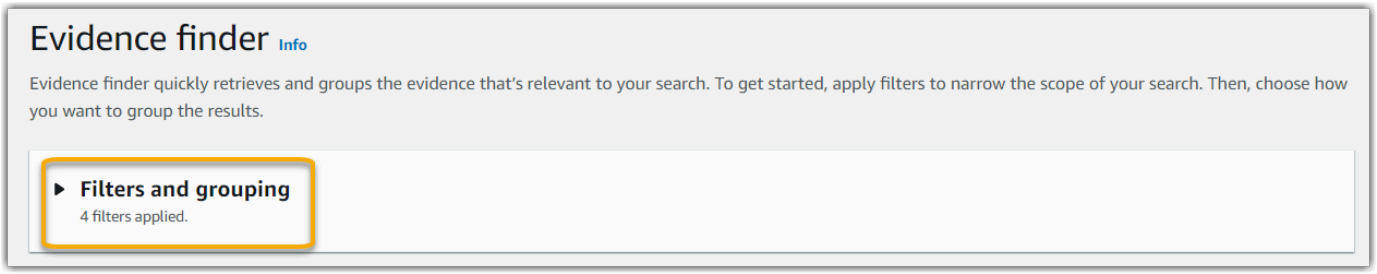
> **Note**
>
> フィルターを編集して検索を選択すると、新しい検索クエリが開始されます。

最近の検索クエリを編集するには

1. 結果を表示ページのパンくずリストナビゲーションメニューから証拠ファインダーを選択します。



2. フィルターとグループ化を選択してフィルターの選択肢を広げます。



3. 次に、フィルターを編集するか、新しい検索を開始します。

   a. フィルターを編集するには、現在のフィルターとグループ選択を調整または削除します。

   b. 最初からやり直すには、フィルターを解除を選択し、選択したフィルターとグループ化の選択を適用します。

4. 終了したら、検索を選択します。

次のステップ

検索が終了すると、検索基準に一致した結果を表示できます。手順については、「証拠ファインダーでの結果の表示」を参照してください。

追加リソース

- 証拠ファインダーのフィルターとグループ化のオプション.
- 証拠ファインダーのユースケースの例.
- 証拠ファインダーの問題のトラブルシューティング.

証拠ファインダーでの結果の表示

検索が終了すると、検索基準に一致した結果を表示できます。

証拠収集中に複数のリソースが評価される場合がありますので、ご注意ください。その結果、証拠には、関連するリソースが 1 つ以上含まれることがあります。証拠ファインダーでは、結果はリソースレベルで表示され、リソースごとに 1 行ずつ表示されます。ページを離れることなく、各リソースの概要をプレビューできます。

検索結果を確認したら、その証拠を含む評価レポートを生成できます。検索結果をカンマ区切り値 (CSV) ファイルにエクスポートすることもできます。

> **Important**
>
> 検索結果の調査が終了するまで、証拠ファインダーを開いたままにしておくことをお勧めします。結果表示表から移動すると、検索結果は破棄されます。必要に応じて、https://console.aws.amazon.com/cloudtrail/ の CloudTrail コンソールで最近の結果を表示できます。

ここでは、検索クエリの結果が 7 日間保存されます。ただし、 CloudTrail コンソールの検索結果から評価レポートを生成することはできません。

前提条件

次の手順は、証拠ファインダーで検索を実行するためのステップにすでに従っていることを前提としています。

手順

証拠ファインダーで検索結果を表示するには、次の手順に従います。

タスク

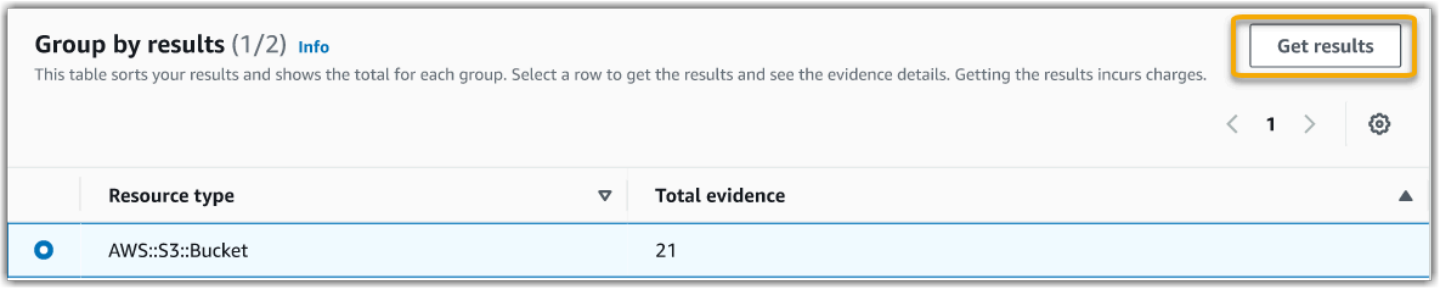
- Step 1. グループ化された結果の表示
- Step 2. 検索結果の表示
  - 表示設定の管理
  - リソース概要のプレビュー

Step 1. グループ化された結果の表示

結果をグループ化した場合は、証拠を詳しく調べる前にそのグループを確認できます。

> **Note**
>
> 結果をグループ化しなかった場合、証拠ファインダーには結果によるグループ化表が表示されません。代わりに、結果表示表に直接移動します。

結果によるグループ化表を使用すると、一致する証拠の範囲と、それが特定のディメンションにどのように分布しているかを確認できます。結果は選択した値によってグループ化されます。例えば、リソースタイプ でグループ化した場合、テーブルには AWS リソースタイプのリストが表示されます。証拠の合計列には、リソースタイプごとに一致する結果の数が表示されます。



グループの結果を取得するには

1. 結果によるグループ化 の表から、取得したい結果の行を選択します。
2. 結果を取得を選択します。新しい検索クエリが開始され、結果表示表にリダイレクトされ、そのグループの結果を確認できます。

Step 2. 検索結果の表示

結果表示表には検索結果が表示されます。ここから、表示設定とプレビューリソースの概要を管理できます。

表示設定の管理

表示設定によって、結果ページに表示される内容がコントロールされます。

表示設定を管理するには

1. 結果表示表の上部にある設定アイコン (#) を選択します。
2. 必要に応じて、以下の設定を確認して変更します。

設定	説明
表示可能なテーブル列を選択する	トグルオプションを使用して、表示する列を変更します。
ページサイズ	ラジオボタンを選択して、各ページに表示される結果の数を指定します。
[Wrap text] (テキストの折り返し)	読みやすくするために、長いテキスト行をラップするチェックボックスをオンにします。

3. 設定を保存するには確認を選択します。

リソース概要のプレビュー

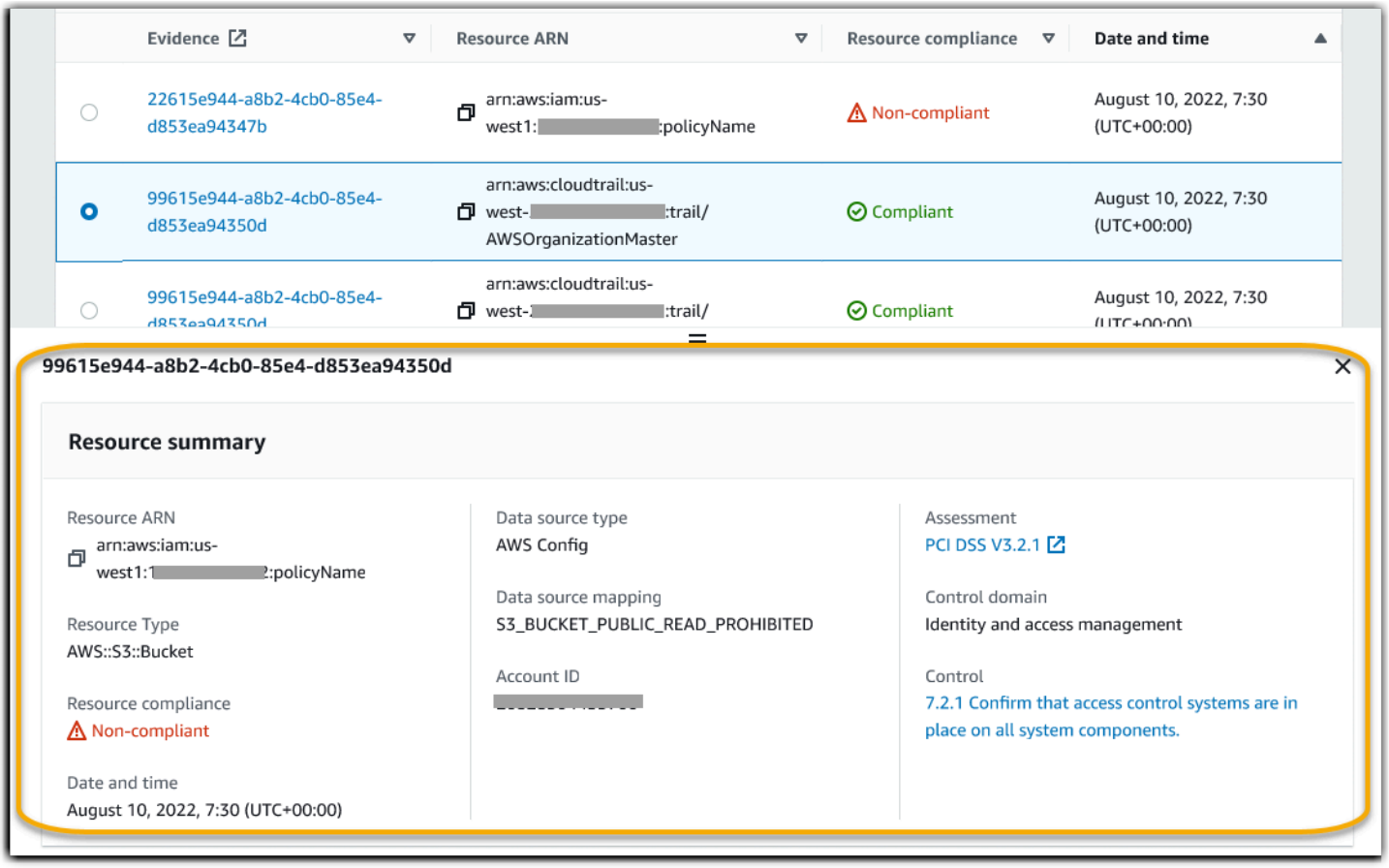
関連リソースをプレビューして、検索クエリに一致した証拠を探すことができます。これにより、検索クエリが意図した結果を返したのか、フィルターを調整して検索クエリを再実行する必要があるのかを判断できます。

証拠には、関連するリソースが 1 つ以上含まれている可能性がありますので、ご注意ください。証拠ファインダーは、リソースレベル (リソースごとに 1 行) で結果を表示します。

> **Note**
>
> 証拠ファインダーは、自動証拠と手動証拠の結果を返します。ただし、自動証拠をプレビューできるのは、自動証拠の詳細のみです。これは、Audit Manager が手動証拠のリソース評価を実行しないためです。その結果、リソースの概要は利用できません。
> 手動証拠に関する詳細を表示するには、証拠名を選択して証拠詳細ページを開きます。証拠ファインダーの結果から評価レポートを生成すると、手動証拠の詳細が評価レポートに含まれます。

リソースの概要をプレビューするには

1. 結果の横にあるラジオボタンを選択します。現在のページにリソース概要パネルが開きます。
2. (オプション) 関連する証拠の詳細を確認するには、証拠名を選択します。
3. (オプション) 水平線 (=) を使用して、リソースサマリーペインをドラッグしてサイズを変更します。
4. (x) を選択してリソースサマリーペインを閉じます。



次のステップ

検索結果を確認したら、検索結果から評価レポートを生成したり、CSV ファイルとしてエクスポートしたりできます。手順については、「証拠ファインダーから検索結果をエクスポートする」を参照してください。

追加リソース

- 証拠ファインダーのフィルターとグループ化のオプション
- 証拠ファインダーのユースケースの例
- 証拠ファインダーの問題のトラブルシューティング

証拠ファインダーから検索結果をエクスポートする

検索結果を確認したら、その結果に基づいて評価レポートを生成できます。または、証拠ファインダーの検索結果を CSV ファイルにエクスポートすることもできます。

前提条件

次の手順では、すでに手順に従って検索を実行し、証拠ファインダーで検索結果を確認していることを前提としています。

手順

目次

検索結果から評価レポートを生成する

検索結果に満足したら、評価レポートを生成できます。

検索結果から評価レポートを生成するには

1. 結果表示表の上部にある評価レポートを生成を選択します。
2. 評価レポートの名前と説明を入力し、評価レポートの詳細を確認します。
3. [Generate assessment report] (評価レポートを生成) を選択します。

評価レポートが生成されるまでには数分かかります。この間、証拠ファインダーから離れることができます。レポートの準備が整うと、緑色の完了通知が表示されます。その後、Audit Manager ダウンロードセンターにアクセスして、評価レポートをダウンロードできます。

> **Note**
>
> Audit Manager は、検索結果の証拠のみを使用して 1 回限りのレポートを生成します。このレポートには、手動で評価ページからレポートに追加された証拠は含まれていません。
> 評価レポートに含めることができる証拠の量には制限があります。詳細については、「証拠ファインダーの問題のトラブルシューティング」を参照してください。

検索結果を CSV ファイルにエクスポートする

証拠ファインダーの検索結果のポータブルバージョンが必要になる場合があります。その場合は、検索結果を CSV ファイルにエクスポートできます。

検索結果をエクスポートすると、CSV ファイルは Audit Manager ダウンロードセンターで 7 日間使用できます。CSV ファイルのコピーは、エクスポート先と呼ばれるご希望の S3 バケットにも配信されます。CSV ファイルは、削除するまでこのバケットに残ります。

Audit Manager は CloudTrail Lake の機能を使用して、証拠ファインダーから CSV ファイルをエクスポートおよび配信します。CSV エクスポートプロセスの仕組みは、以下の要素によって定義されます。

- 検索結果はすべて CSV ファイルに含まれます。特定の検索結果のみを含める場合は、検索フィルターを編集することをお勧めします。これにより、エクスポートしたい証拠だけをターゲットにするように結果を絞り込むことができます。
- CSV ファイルは圧縮された GZIP 形式でエクスポートされます。デフォルトの CSV ファイル名は`queryID/result.csv.gz`です。`queryID`は検索クエリの ID です。
- CSV エクスポートの最大ファイルサイズは 1 TB です。1 TB を超えるデータをエクスポートする場合、結果は複数のファイルに分割されます。各 CSV ファイルには`result_`*`number`*`.csv.gz`という名前が付けられます。取得できる CSV ファイルの数は、検索結果の合計サイズによって異なります。例えば、2 TB のデータをエクスポートすると、`result_1.csv.gz`と`result_2.csv.gz`の 2 つのクエリ結果のファイルが作成されます。
- CSV ファイルに加えて、JSON 署名ファイルが S3 バケットに配信されます。このファイルは、CSV ファイル内の情報が正確であることを確認するためのチェックサムとして機能します。詳細については、「 AWS CloudTrail デベロッパーガイド」のCloudTrail 「ファイル構造に署名する」を参照してください。クエリ結果が配信後に変更、削除、または変更されていないかどうかを判断するには、 CloudTrail クエリ結果の整合性検証を使用できます。手順については、「AWS CloudTrail 開発者ガイド」の「保存したクエリ結果の検証」を参照してください。

> **Note**
>
> 現在、証拠ファインダーのプレビューや CSV エクスポートには、手動証拠のテキストレスポンスは含まれていません。テキストレスポンスデータを表示するには、証拠ファインダーの結果から手動証拠名を選択し、証拠詳細ページを開きます。Audit Manager コンソールの外部でテキストレスポンスデータを表示する必要がある場合は、証拠ファインダーの結果か

ら評価レポートを生成することをお勧めします。テキストレスポンスを含め、手動証拠の詳細はすべて評価レポートに含まれます。

結果を初めてエクスポートする場合

検索結果を初めてエクスポートするには、以下の手順に従います。この手順では、今後のすべてのエクスポートに対してデフォルトのエクスポート先を指定するオプションを提供します。デフォルトのエクスポート先を今すぐ保存したくない場合は、エクスポート先の設定を更新することで後で保存できます。

> **Important**
>
> 開始する前に、エクスポート先として使用できる S3 バケットがあることを確認します。既存の S3 バケットを使用するか、Amazon S3 で新しいバケットを作成することができます。さらに、S3 バケットには、 がエクスポートファイルを CloudTrail 書き込むために必要なアクセス許可ポリシーが必要です。具体的には、バケットポリシーに `s3:PutObject`アクションとバケット ARN が含まれ、サービスプリンシパル CloudTrail としてリストされている必要があります。使用できるアクセス権限ポリシーの例を提供しています。このポリシーを S3 バケットにアタッチする方法については、「Amazon S3 コンソールを使用してバケットポリシーを追加する」を参照してください。
> その他のヒントについては、「」を参照してくださいエクスポート先の設定に関するヒント。CSV ファイルのエクスポート中に問題が発生した場合は、「」を参照してくださいcsv-exports。

検索結果をエクスポートするには (初回実行時)

1. 結果表示 表の上部にあるCSV をエクスポートを選択します。
2. ファイルのエクスポート先の S3 バケットを指定します。

   - Browse S3 を選択し、バケットのリストから選択します。
   - または、**`s3://bucketname/prefix`** 形式でバケット URI を入力できます。

> **Tip**
>
> エクスポート先のバケットを整理しておくために、CSV エクスポート用のオプションフォルダを作成できます。そのためには、[リソース URI] ボックス (例: **/**

evidenceFinderExports) の値にスラッシュ (**/**) とプレフィックスを追加します。Audit Manager は CSV ファイルをバケットに追加するときにこのプレフィックスを含め、Amazon S3 はプレフィックスで指定されたパスを生成します。Amazon S3 でのプレフィックスの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 コンソールのオブジェクトを整理する」を参照してください。

3. (オプション) このバケットをデフォルトのエクスポート先として保存したくない場合は、証拠ファインダー設定でこのバケットをデフォルトのエクスポート先として保存するというチェックボックスを解除します。
4. [エクスポート] をクリックします。

エクスポート先を保存した後で結果をエクスポートする

デフォルトの S3 バケットをデフォルトのエクスポート先として保存したら、次の手順に従って次に進むことができます。

検索結果をエクスポートするには (デフォルトのエクスポート先を保存した後に)

1. 結果表示 表の上部にあるCSV をエクスポートを選択します。
2. 表示されるプロンプトで、エクスポートされたファイルが保存されるデフォルトの S3 バケットを確認します。
   a. (オプション) このバケットを引き続き使用してこのメッセージを非表示にするには、「今後通知しない」ボックスをチェックしてください。
   b. (オプション) このバケットを変更するには、手順に従ってエクスポート先の設定を更新してください。
3. [確認] を選択します。

エクスポートするデータの量によっては、エクスポートプロセスが完了するまでに数分かかることがあります。エクスポート中は、証拠ファインダーから別の場所に移動できます。証拠ファインダーから離れると、検索は停止し、検索結果はコンソール内で破棄されます。ただし、CSV エクスポートプロセスはバックグラウンドで継続されます。CSV ファイルには、クエリに一致した検索結果がすべて含まれます。

結果をエクスポートした後の表示

CSV ファイルを検索してステータスを確認するには、Audit Manager に移動しますAudit Manager のダウンロードセンター。エクスポートしたファイルの準備ができたら、ダウンロードセンターから CSV ファイルをダウンロードできます。

エクスポート先の S3 バケットから CSV ファイルを検索してダウンロードすることもできます。

Amazon S3 コンソールで CSV ファイルと署名ファイルを検索するには

1. Amazon S3 コンソールを開きます。
2. CSV ファイルをエクスポートしたときに指定したエクスポート先バケットを選択します。
3. CSV ファイルおよび署名ファイルが見つかるまでオブジェクト階層内を移動します。CSV ファイルの拡張子は.csv.gzで、署名ファイルの拡張子は.jsonです。

次の例のように、オブジェクト階層を移動することになりますが、エクスポート先のバケット名、アカウント ID、日付、およびクエリ ID は異なります。

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

追加リソース

- 証拠ファインダーの問題のトラブルシューティング
- エビデンスファインダーのデフォルトのエクスポート先の設定

証拠ファインダーのフィルターとグループ化のオプション

このページには、証拠ファインダーで使用できるフィルターとグループ化オプションのリストが表示されます。

フィルターリファレンス

次のフィルターを使用して、評価、コントロール、 などの特定の基準に一致する証拠を検索できます AWS のサービス。

トピック

必須フィルター

これらのフィルターを使用して、評価における高レベルでの証拠の概要を開始します。

フィルター名	説明	メモ
[評価]	特定の評価の証拠を返します。	1 つの評価のみでフィルタリングできます。
日付範囲	特定の期間の証拠を返します。	また、相対範囲を使用して今日の日付を基準とした相対範囲を定義することもできます (例: **`Last 30 days`**)。 または、絶対範囲を使用して特定の日付範囲を指定することもできます (例: **`June 27th - July 4th`**)。
リソースコンプライアンス	特定のコンプライアンスチェック評価を含むリソースを返します。	Audit Manager は、 AWS Config と Security Hub をデータソースタイプとして使用するコントロールのコンプライアンスチェックの証拠を収集します。証拠収集中に複数のリソースが評価される場合があります。その結果、1 つのコンプライアンスチェックエビデンスに 1 つ以上のリソースが含まれる可能性があります。このフィルターを使用して、リソースレベルでコンプライアンスステータスを調べることができます。

フィルター名	説明	メモ
		次のオプションのいずれかを選択します (複数可)。 • 非準拠 — このフィルターは、コンプライアンスチェックの問題があるリソースを検索します。これは、Security Hub が失敗結果を報告した場合、または が非準拠結果を AWS Config 報告した場合に発生します。 • 準拠 — このフィルターは、コンプライアンスチェックの問題がないリソースを検索します。これは、Security Hub が合格結果を報告した場合、または が準拠結果を AWS Config 報告した場合に発生します。 • 未判断 — このフィルターは、コンプライアンスチェックが利用できない、または適用できないリソースを検索します。これは、リソースが基になるデータソースタイプとして AWS Config または Security Hub を使用しているが、それらのサービスが有効になっていない場合に発生します。これは、リソースがコンプライアンスチェック (手動証拠、 AWS API コール、 など) をサポートしていない基盤となるデータソースタイプを使用している場合にも発生します CloudTrail。

追加フィルター (オプション)

これらのフィルターを使用して、検索クエリの範囲を絞り込みます。例えば、Amazon S3 に関連するすべての証拠を表示するには、サービスを使用します。リソースタイプを使うと S3 バケットだけに集中できます。または、リソース ARN を使用して特定の S3 バケットをターゲットにします。

次の 1 つ以上の基準を使用して追加のフィルターを作成できます。

基準名	説明	この基準はいつ使用するか
アカウント ID	でドリルダウンします AWS アカウント。	この基準を使用して、特定の AWS アカウントに関連する証拠を検索してください。
コントロール	コントロール名別にドリルダウンします。	この基準を使用して、特定のコントロールに関連する証拠を検索してください。
コントロールドメイン	コントロールドメイン別にドリルダウンします。	この基準を使用して、監査に向けて準備する際に、特定の対象領域に集中します。標準フレームワークから作成された評価を問い合わせる場合は、コントロールドメインでフィルタリングできます。 コントロールドメインの例としては、ID とアクセスの管理、ロギングと監視、ネットワーク管理などがあります。
[Data source type]	データソースのタイプ別にドリルダウンします。	この基準を使用して、特定のデータソースに集中します。 値を`Manual`に設定すると、手動でアップロードした証拠を検索できます。それ以外の場合は、自動証拠をその出所 (`AWS Config`、`CloudTrail` 、`Security Hub`、`AWS API calls`など) に基づいてフィルタリングできます。
イベント名	イベント名でドリルダウンします。	この基準を使用して、証拠に関連する特定のイベントに焦点を当てます。イベントは、 AWS アカウントでのアクティビティのレコードです。 例えば、アクセス権限の設定に使用される IAM `AttachRolePolicy` オペレーションなどの API コールの名前を検索できます。または、ユーザーがアカウントにサインイン CloudTrail したときに によってログに記録される`ConsoleLogin` イベントなどの CloudTrail キーワードを検索します。
リソース ARN	Amazon リソースネーム (ARN)でドリルダウンします。	この基準を使用して、特定の AWS リソースに関連する証拠を検索してください。

基準名	説明	この基準はいつ使用するか
リソースタイプ	リソースタイプ別にドリルダウンします。	この基準を使用して、Amazon EC2 インスタンスや S3 バケットなど、評価対象のリソースのタイプに集中します。
サービス	AWS のサービス 名前でドリルダウンします。	この基準を使用して、Amazon EC2 AWS のサービス、Amazon S3、 など、特定の に関連する証拠を検索します AWS Config。
サービスのカテゴリ	AWS のサービス カテゴリ別にドリルダウンします。	この基準を使用して、 の特定のカテゴリに焦点を当てます AWS のサービス。 例としては、セキュリティ、ID とコンプライアンス、データベース、ストレージなどがあります。

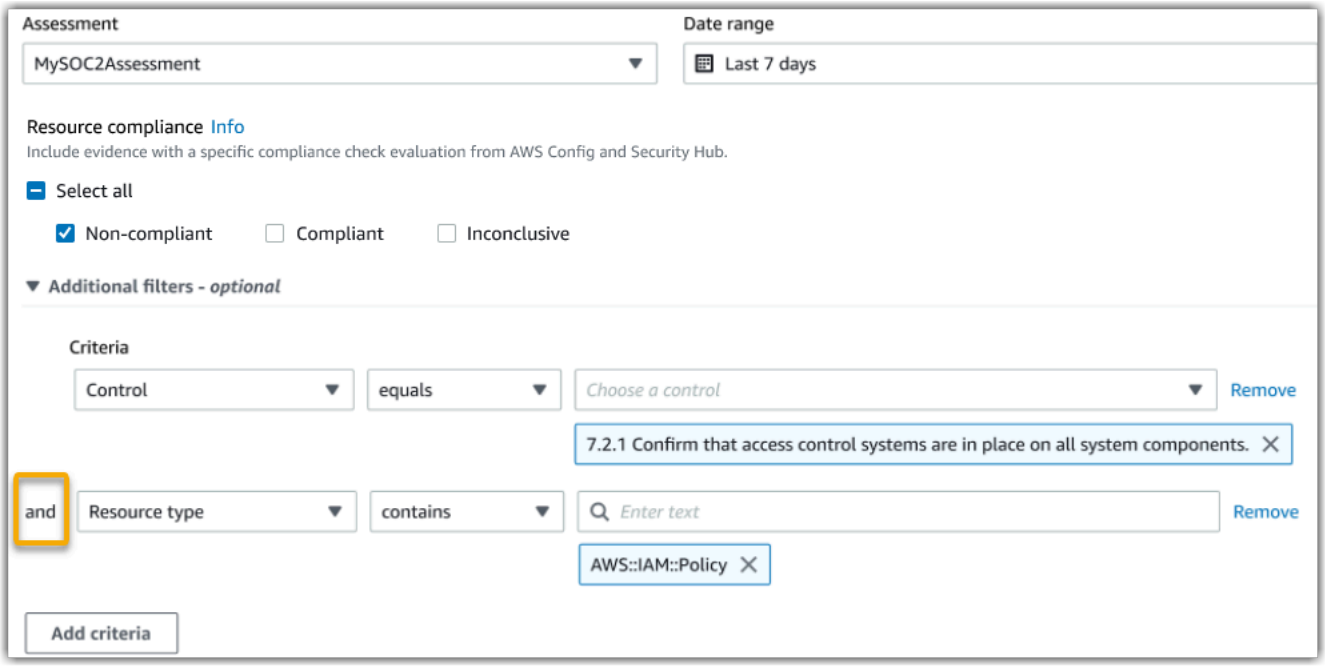
フィルターの組み合わせ

基準の動作

複数の基準を指定すると、Audit Manager は選択した基準にAND演算子を適用します。つまり、すべての基準が 1 つのクエリにグループ化され、結果は組み合わされたすべての条件と一致する必要があります。

例

次のフィルター設定では、証拠ファインダーは、**MySOC2Assessment**という評価に対して過去 7 日間の非準拠リソースを返します。さらに、結果は IAM ポリシーと指定されたコントロールの両方に関係します。

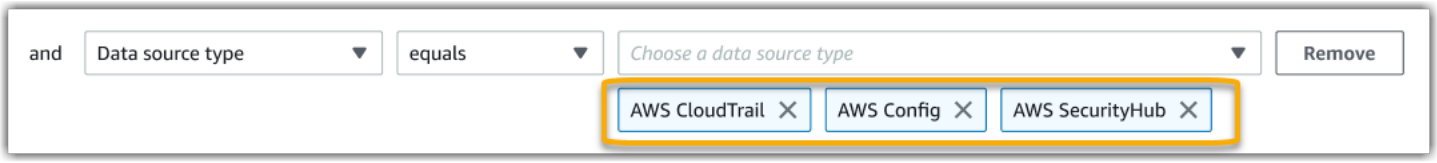


基準値の動作

1 以上の基準値を指定すると、値はOR演算子とリンクされます。証拠ファインダーは、これらの基準値のいずれかに一致する結果を返します。

例

次のフィルター設定では、証拠ファインダーは、 AWS CloudTrail、 AWS Config、または のいずれかから取得した検索結果を返します AWS Security Hub。



グループ化のリファレンス

検索結果をグループ化して、すばやくナビゲートできます。グループ化すると、検索結果の範囲と、検索結果が特定のディメンションにどのように分布しているかがわかります。

以下のいずれかの値によるグループを使用できます。

グループ化	説明
アカウント ID	結果を でグループ化します AWS アカウント。

グループ化	説明
コントロール	結果をコントロール名でグループ化します。
[Data source type]	証拠の出所であるデータソースのタイプ別に結果をグループ化します。
イベント名	結果をイベント名でグループ化します。
リソースARN	結果をAmazon リソースネーム (ARN)でグループ化します。
リソースタイプ	結果をリソースタイプ別でグループ化します。
サービス	結果を AWS のサービス 名前でグループ化します。
サービスのカテゴリ	結果を AWS のサービス カテゴリ別にグループ化します。

証拠ファインダーのユースケースの例

証拠ファインダーはいくつかのユースケースで役立ちます。このページでは、いくつかの例を示し、各シナリオで使用できる検索フィルターを提案します。

トピック

ユースケース 1：非準拠の証拠を検索して委任を組織する

このユースケースは、コンプライアンス責任者、データ保護責任者、または監査準備を監督する GRC の専門家に最適です。

組織のコンプライアンス体制を監視する場合、問題の解決を支援してくれるパートナーチームに依頼する場合があります。証拠ファインダーを使用すると、パートナーチームの業務を整理するのに役立ちます。

フィルターを適用することで、一度に 1 つの領域の証拠に集中できます。さらに、協力する各パートナーチームの責任と範囲を把握しておくこともできます。このようにターゲットを絞った検索を行うことで、検索結果を使用して、各分野において改善が必要な点を正確に特定できます。その後、対象の非準拠の証拠を対応するパートナーチームに委任して是正してもらうことができます。

このワークフローでは、証拠を検索する手順に従ってください。以下のフィルターを使用して、非準拠の証拠を検索します。

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

次に、注目している分野に追加のフィルターを適用します。例えば、サービスカテゴリーフィルターを使用して、IAM に関連する非準拠リソースを検索します。そして、その結果を組織の IAM リソースを所有するチームと共有します。または、標準フレームワークから作成された評価をクエリする場合は、コントロールドメインフィルターを使用して、ID およびアクセス管理ドメインに関連する非準拠の証拠を検索できます。

```
Control domain | <domain that you're focusing on>
or
Service category | <AWS ##### category that you're focusing on>
```

必要な証拠を見つけたら、手順に従って検索結果から評価レポートを生成します。手順については、「検索結果から評価レポートを生成する」を参照してください。このレポートをパートナーチームと共有して、改善チェックリストとして使用できます。

ユースケース 2：準拠している証拠の特定

このユースケースは SecOps、、IT/DevOps、またはクラウドアセットを所有および修正する別のロールで作業する場合に最適です。

監査の一環として、所有しているリソースの問題の修正を求められる場合があります。この作業を終えたら、証拠ファインダーを使用してリソースがコンプライアンスに準拠していることを検証できます。

このワークフローでは、証拠を検索する手順に従ってください。以下のフィルターを使用して、準拠している証拠を検索してください。

```
Assessment | <assessment name>
```

```
Date range | <date range>
Resource compliance | Compliant
```

次に、追加のフィルターを適用して、自分が担当する証拠のみを表示します。所有範囲に応じて、必要に応じて対象を絞って検索を実行します。以下のフィルター例は、最も広範なものから最も正確なものの順に並べられています。適切なオプションを選択し、*<############>*を独自の値に置き換えてください。

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of AWS ##### that you own>
Service | <a specific AWS ##### that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

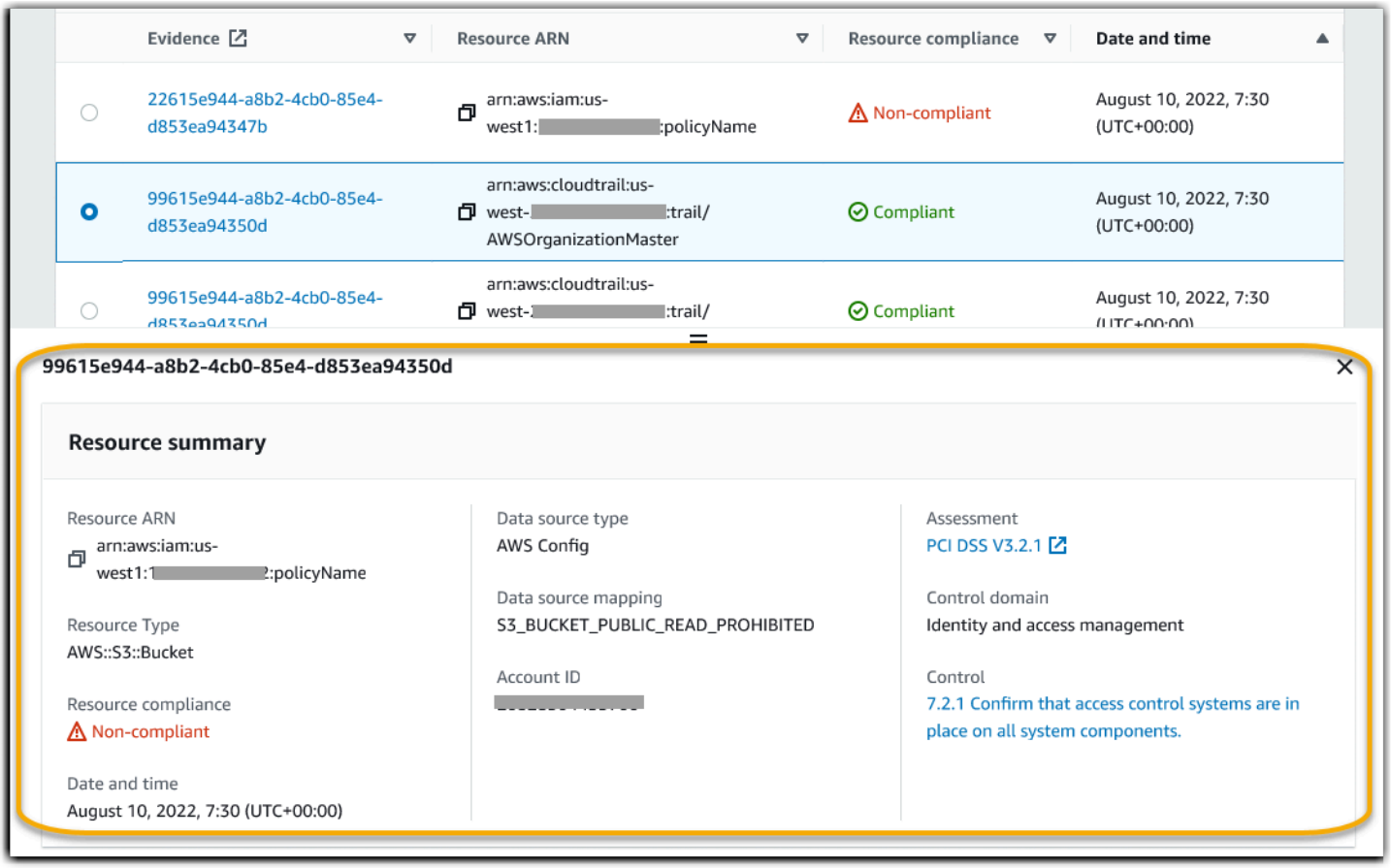
同じ条件の複数のインスタンス (たとえば、複数の を所有している AWS のサービス) を担当している場合は、その値で結果をグループ化できます。これにより、各 AWS のサービスに一致する証拠の合計が得られます。その後、所有しているサービスの結果を取得できます。

ユースケース 3：証拠リソースのクイックプレビューの実行

このユースケースは、Audit Manager のすべてのお客様に最適です。

以前は、個々の証拠の詳細を確認するのに時間がかかっていました。証拠をプレビューしたい場合は、その評価に直接アクセスし、深くネストされた証拠フォルダを閲覧する必要がありました。証拠ファインダーでは、この情報を簡単にプレビューできるようになりました。検索クエリに一致する証拠項目ごとに、その証拠の個々のリソースをプレビューできます。

はじめに、証拠を検索する手順に従ってください。次に、結果の横にあるラジオボタンを選択すると、現在のページにリソースの概要が表示されます。証拠項目に関連する個々のリソースをプレビューできます。リソースの証拠詳細をすべて表示するには、証拠名を選択します。詳細については、「リソース概要のプレビュー」を参照してください。


Evidence
Resource ARN
Resource compliance
Date and time
22615e944-a8b2-4cb0-85e4-d853ea94347b
arn:aws:iam:us-west1:[redacted]:policyName
Non-compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/AWSOrganizationMaster
Compliant
August 10, 2022, 7:30 (UTC+00:00)
99615e944-a8b2-4cb0-85e4-d853ea94350d
arn:aws:cloudtrail:us-west-[redacted]:trail/
Compliant
August 10, 2022, 7:30
99615e944-a8b2-4cb0-85e4-d853ea94350d
Resource summary
Resource ARN
arn:aws:iam:us-west1:[redacted]:policyName
Resource Type
AWS::S3::Bucket
Resource compliance
Non-compliant
Date and time
August 10, 2022, 7:30 (UTC+00:00)
Data source type
AWS Config
Data source mapping
S3_BUCKET_PUBLIC_READ_PROHIBITED
Account ID
[redacted]
Assessment
PCI DSS V3.2.1
Control domain
Identity and access management
Control
7.2.1 Confirm that access control systems are in place on all system components.

Audit Manager のダウンロードセンター

ダウンロードセンターでは、ダウンロード可能なすべての Audit Manager ファイルを検索して管理できます。評価レポートを生成したり、エビデンスファインダーから検索結果をエクスポートしたりすると、ファイルはダウンロードセンターに表示されます。

目次

ダウンロードセンターを閲覧する

ダウンロードセンターでファイルを参照するには、次の手順に従います。

ダウンロードセンターでファイルを検索するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左のナビゲーションペインで、[ダウンロードセンター] をクリックします。
3. 評価レポートタブを選択すると、ダウンロード可能な評価レポートが表示されます。
   - このタブには、生成した評価レポートが表示されます。評価レポートは、削除するまでダウンロードセンターで引き続き利用できます。
   - 評価レポートの最新のステータスを確認するには、更新アイコン (#) を選択して表をリロードします。評価レポートテーブルの各行には、レポートの名前、作成日、および以下のステータスのいずれかが表示されます。

ステータス	説明
進行中	Audit Manager は評価レポートを生成しています。
準備完了	評価レポートはダウンロードできます。

ステータス	説明
エラー	評価レポートの生成に失敗しました。この場合、Audit Manager は、エラーについて説明するメッセージを表示します。 これらのエラーを解決する方法については、「」を参照してください評価レポートの問題のトラブルシューティング。

4. エクスポートタブを選択すると、ダウンロード可能な CSV エクスポートが表示されます。

   - このタブには、過去 7 日間にエクスポートした証拠ファインダーの検索結果が表示されます。CSV ファイルは 7 日後にダウンロードセンターから削除されますが、エクスポート先の S3 バケットでは引き続き使用できます。S3 宛先バケットでエビデンスファインダーの CSV エクスポートを検索する方法については、結果をエクスポートした後の表示 を参照してください。
   - CSV エクスポートの最新のステータスを確認するには、更新アイコン (#) を選択してテーブルをリロードします。エクスポートテーブルの各行には、ファイル名、エクスポート日、および以下のステータスのいずれかが表示されます。

ステータス	説明
進行中	Audit Manager は CSV ファイルを準備しています。
準備完了	エクスポートは成功し、ファイルはダウンロードできます。
エラー	エクスポートに失敗しました。この場合、Audit Manager は、エラーについて説明するメッセージを表示します。 これらのエラーを解決する方法については、「」を参照してくださいcsv-exports。

> **Note**
>
> エクスポートタブには、 AWS CloudTrail Lake で直接実行したクエリの CSV ファイルも表示される場合があることに注意してください。これには、 CloudTrail コンソールまたは CloudTrail API を使用して行われたクエリが含まれます。 CloudTrail Audit

Manager イベントデータストアにクエリを実行し、結果を Amazon S3 に保存することを選択した場合、エクスポートはこのタブに表示されます。

ファイルのダウンロード

ダウンロードセンターからファイルをダウンロードするには、次の手順に従います。

ファイルをダウンロードするには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左のナビゲーションペインで、[ダウンロードセンター] をクリックします。
3. [評価レポート] タブまたは [エクスポート] タブを選択します。
4. ダウンロードしたいファイルを選択し、[ダウンロード] を選択します。

S3 送信先バケットから直接ファイルをダウンロードする方法については、Amazon Simple Storage Service (Amazon S3) ユーザーガイドの「オブジェクトのダウンロード」を参照してください。

ファイルの削除

ダウンロードセンターで不要になった評価レポートを削除するには、次の手順に従います。

> **Note**
>
> 現在、ダウンロードセンターからの CSV エクスポートの削除はサポートされていません。CSV のエクスポートは 7 日後にダウンロードセンターから自動的に削除されます。

評価レポートを削除するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左のナビゲーションペインで、[ダウンロードセンター] をクリックします。
3. [評価レポート] タブを選択します。
4. 削除する評価を選択し、[削除] を選択します。

S3 宛先バケットから評価レポートまたは CSV エクスポートを削除する場合は、このタスクを Amazon S3 で直接実行することをお勧めします。手順については、「Amazon Simple Storage Service (Amazon S3) ユーザーガイド」の「Amazon S3 オブジェクトの削除」を参照してください。

追加リソース

- エビデンスファインダーのデフォルトのエクスポート先の設定
- デフォルトの評価レポートの送信先の設定
- 評価レポートの問題のトラブルシューティング
- CSV エクスポートの問題のトラブルシューティング
- Amazon S3 からのオブジェクトのダウンロード
- Amazon S3 オブジェクトの削除

フレームワークライブラリを使用して でフレームワークを管理する AWS Audit Manager

フレームワークは、 のフレームワークライブラリで検索および管理できます AWS Audit Manager。

フレームワークは、一定の期間にわたって環境でテストされるコントロールを決定します。これは、特定のコンプライアンス標準または規制について、コントロールとそのデータソースマッピングを定義します。また、Audit Manager の評価の構造化と自動化にも使用されます。フレームワークを出発点として使用して、 AWS のサービス 使用状況を監査し、証拠収集の自動化を開始できます。

重要ポイント

フレームワークライブラリでは、フレームワークは次のカテゴリに分類されます。

- 標準フレームワークは、 AWS によって提供される構築済みのフレームワークです。これらのフレームワークは、GDPR や HIPAA など、さまざまなコンプライアンス標準や規制の AWS ベストプラクティスに基づいています。標準フレームワークには、フレームワークがサポートするコンプライアンス標準または規制に基づいてコントロールセットに編成されたコントロールが含まれます。

  標準フレームワークの内容を表示することはできますが、編集または削除することはできません。ただし、標準フレームワークの編集可能なコピーを作成して、特定の要件を満たす新しいフレームワークを作成できます。
- カスタムフレームワークは、作成するフレームワークです。カスタムフレームワークは、最初から作成することも、既存のフレームワークの編集可能なコピーを作成することもできます。カスタムフレームワークを使用して、特定の要件を満たす方法でコントロールをコントロールセットに編成できます。

標準またはカスタムのフレームワークから評価を作成できます。

> **Note**
>
> AWS Audit Manager は、特定のコンプライアンス標準および規制への準拠の検証に関連する証拠の収集を支援します。ただし、コンプライアンス自体を評価するものではありません。AWS Audit Manager したがって、 によって収集された証拠には、監査に必要な AWS 使用状

況に関するすべての情報が含まれていない場合があります。 AWS Audit Manager は、法律顧問やコンプライアンスの専門家に代わるものではありません。

追加リソース

Audit Manager でフレームワークを作成および管理するには、ここで概説されている手順に従ってください。

- で利用可能なフレームワークの検索 AWS Audit Manager
- でのフレームワークの確認 AWS Audit Manager
- でのカスタムフレームワークの作成 AWS Audit Manager
  - でゼロからカスタムフレームワークを作成する AWS Audit Manager
  - で既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager
- でのカスタムフレームワークの編集 AWS Audit Manager
- でのカスタムフレームワークの削除 AWS Audit Manager
- でのカスタムフレームワークの共有 AWS Audit Manager
  - フレームワークの共有に関する概念と用語
  - でカスタムフレームワークを共有するためのリクエストの送信 AWS Audit Manager
  - でリクエストを共有する応答 AWS Audit Manager
  - での共有リクエストの削除 AWS Audit Manager
- でサポートされているフレームワーク AWS Audit Manager

で利用可能なフレームワークの検索 AWS Audit Manager

使用可能なすべてのフレームワークは、Audit Manager コンソールのフレームワークライブラリページで確認できます。

Audit Manager API または AWS Command Line Interface () を使用して、使用可能なすべてのフレームワークを表示することもできますAWS CLI。

前提条件

IAM アイデンティティに、 でフレームワークを表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、

AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager console

Audit Manager コンソールで使用可能なフレームワークを表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Framework library] (フレームワークライブラリ) を選択します。
3. [Standard frameworks] (標準フレームワーク) のタブまたは [Custom frameworks] (カスタムフレームワーク) のタブを選択して、使用可能な標準フレームワークおよびカスタムフレームワークを参照します。

AWS CLI

で使用可能なフレームワークを表示するには AWS CLI

Audit Manager でフレームワークを表示するには、 list-assessment-frameworks コマンドを使用して を指定します`--framework-type`。いずれの方法でも、標準フレームワークのリストを取得できます。または、カスタムフレームワークのリストを取得できます。

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

API を使用して使用可能なフレームワークを表示するには

ListAssessmentFrameworks オペレーションを使用して frameworkTypeを指定します。いずれの方法でも、標準フレームワークのリストを返すことができます。または、カスタムフレームワークのリストを返すこともできます。

詳細については、前述のリンクのいずれかを選択して、AWS Audit Manager API リファレンスの詳細をご覧ください。これには、言語固有の AWS SDKsの 1 つで

ListAssessmentFrameworksオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

フレームワークの詳細を確認する準備ができたら、「」のステップに従いますでのフレームワークの確認 AWS Audit Manager。このページでは、フレームワークの詳細について説明し、表示される情報について説明します。

フレームワークライブラリページから、 の作成、 の編集、 の削除、カスタムフレームワークの共有を行うこともできます。

追加リソース

Audit Manager で問題をフレームワークする解決策については、「」を参照してくださいフレームワークの問題のトラブルシューティング。

でのフレームワークの確認 AWS Audit Manager

フレームワークの詳細は、Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface (AWS CLI) を使用して確認できます。

前提条件

IAM アイデンティティに、 でフレームワークを表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager console

Audit Manager コンソールでフレームワークの詳細を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。

2. 左側のナビゲーションペインで、[Framework library] (フレームワークライブラリ) を選択して、使用可能なフレームワークのリストを表示します。
3. [標準フレームワーク] のタブまたは [カスタムフレームワーク] のタブを選択して、使用可能な標準フレームワークおよびカスタムフレームワークを参照します。
4. フレームワークを開くには、その名前を選択します。
5. 以下の情報をリファレンスとして使用して、フレームワークの詳細を確認します。

フレームワークの詳細セクション

このセクションでは、フレームワークの概要を説明します。このセクションでは、次の情報を確認できます。

名前	説明
説明	フレームワークが提供された場合の説明。
フレームワークタイプ	フレームワークが標準フレームワークかカスタムフレームワークかを指定します。
コンプライアンスタイプ	フレームワークがサポートするコンプライアンス標準または規制。

カスタムフレームワークを表示している場合は、次の詳細も確認できます。

名前	説明
作成者	カスタムフレームワークを作成したアカウント。
作成日	カスタムフレームワークが作成された日付。
最終更新日	このフレームワークが最後に編集された日付。

[コントロール] タブ

このタブには、フレームワーク内のコントロールがコントロールセット別にグループ化されて一覧表示されます。このタブでは、次の情報を確認できます。

名前	説明
コントロールセット別にグループ化されたコントロール	ツリービューアイコンを選択すると、各コントロールセットに属するコントロールが表示されます。
タイプ	コントロールが標準コントロールかカスタムコントロールかを指定します。
データソース	Audit Manager がそのフレームワークコントロールのために証拠を収集するデータソースを指定します。

タグタブ

このタブは、フレームワークに関連付けられているタグを一覧表示します。このタブでは、次の情報を確認できます。

名前	説明
キー	タグキー (コンプライアンス標準、規制、カテゴリなど) 。
値	タグ値。

AWS CLI

でフレームワークの詳細を表示するには AWS CLI

1. 確認するフレームワークを特定するには、 list-assessment-frameworks コマンドを実行してを指定します`--framework-type`。いずれの方法でも、標準フレームワークのリストを取得できます。または、カスタムフレームワークのリストを取得できます。

   次の例では、`############`を `Custom` または `Standard` に置き換えます。

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   レスポンスはフレームワークのリストを返します。レビューするフレームワークを見つけ、フレームワーク ID と Amazon リソースネーム (ARN) をメモします。

2. フレームワークの詳細を取得するには、 get-assessment-framework コマンドを実行し、 を指定します--framework-id。

   次の例では、次の *placeholder text* を独自の情報に置き換えます。

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

   > **Tip**
   >
   > フレームワークの詳細は JSON 形式で返されます。このデータを理解するには、「 コマンドリファレンス」のget-assessment-framework 「出力」を参照してください。 AWS CLI

3. フレームワークのタグを表示するには、 list-tags-for-resource コマンドを使用してフレームワーク--resource-arnの を指定します。

   次の例では、次の *placeholder text* を独自の情報に置き換えます。

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Audit Manager のタグの詳細については、「AWS Audit Manager リソースのタグ付け」を参照してください。

Audit Manager API

API を使用してフレームワークの詳細を表示するには

1. レビューするフレームワークを特定するには、 ListAssessmentFrameworksオペレーションを使用して frameworkTypeを指定します。いずれの方法でも、標準フレームワークのリストを返すことができます。または、カスタムフレームワークのリストを返すこともできます。

   レスポンスからレビューするフレームワークを見つけ、フレームワーク ID と Amazon リソースネーム (ARN) をメモします。

2. フレームワークの詳細を取得するには、 GetAssessmentFrameworkオペレーションを使用します。リクエストで、ステップ 1 で取得した frameworkId を指定します。

> **Tip**
>
> フレームワークの詳細は JSON 形式で返されます。このデータを理解するには、AWS Audit Manager 「 API リファレンス」のGetAssessmentFramework 「レスポンス要素」を参照してください。

3. フレームワークのタグを表示するには、 ListTagsForResourceオペレーションを使用します。リクエストで、ステップ 1 で取得したフレームワーク resourceArn を指定します。

Audit Manager のタグの詳細については、AWS Audit Manager 「リソースのタグ付け」を参照してください。

これらの API オペレーションの詳細については、前の手順のリンクのいずれかを選択して、AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

フレームワークの詳細ページから、フレームワークから評価を作成するか、フレームワークの編集可能なコピーを作成できます。

カスタムフレームワークを確認する場合は、 を編集したり、 を削除したり、フレームワークを共有したりすることもできます。

追加リソース

- カスタムフレームワークの詳細ページで、カスタムフレームワークを再作成するように求められます。
- カスタムフレームワークのコピーを作成したり、それを使用して評価を作成したりすることはできません

でのカスタムフレームワークの作成 AWS Audit Manager

カスタムフレームワークを使用して、特定の要件を満たす方法でコントロールをコントロールセットに編成できます。

重要ポイント

Audit Manager でカスタムフレームワークを作成する場合、次の 2 つの方法から選択できます。

1. カスタムフレームワークをゼロから作成する - これにより、クリーンなスレートから始めて、仕様に従ってフレームワークのあらゆる側面を定義する柔軟性が得られます。このアプローチは、要件が既存の標準フレームワークから大幅に逸脱している場合、または組織に固有の独自のコントロールセットを組み込む必要がある場合に特に役立ちます。
2. 既存のフレームワークの編集可能なコピーの作成 - このアプローチにより、既存のフレームワークの構造とコンテンツを活用しながら、特定のニーズに合わせて自由にカスタマイズできます。確立された基盤から始めることで、カスタムフレームワークを構築するプロセスを合理化し、組織の固有の要件に合わせてカスタマイズすることに集中できます。

選択したアプローチに関係なく、カスタムフレームワークの作成には、フレームワークの詳細の指定、コントロールセットの定義、作成を確定する前にフレームワークを確認するなどの一連のステップが含まれます。このプロセスを通じて、組織の特定のコントロールセットを組み込むことができ、カスタムフレームワークが GRC 要件を正確に反映するようにします。

追加リソース

カスタムフレームワークを作成する方法については、以下のリソースを参照してください。

- でゼロからカスタムフレームワークを作成する AWS Audit Manager
- で既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager

でゼロからカスタムフレームワークを作成する AWS Audit Manager

組織のコンプライアンス要件が、 で利用可能な構築済みの標準フレームワークと一致しない場合は AWS Audit Manager、代わりに独自のカスタムフレームワークをゼロから作成できます。

このページでは、特定のニーズに合わせてカスタムフレームワークを作成する手順の概要を説明します。

前提条件

IAM アイデンティティに、 でカスタムフレームワークを作成するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、

AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

タスク

- ステップ 1: フレームワークの詳細を指定する
- ステップ 2: コントロールセットを指定する
- ステップ 3: フレームワークを確認して作成する

ステップ 1: フレームワークの詳細を指定する

まず、カスタムフレームワークの詳細を指定します。

フレームワークの詳細を指定するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、フレームワークライブラリ を選択し、カスタムフレームワークの作成 を選択します。
3. フレームワークの詳細 に、名前、コンプライアンスタイプ (オプション) 、フレームワークの説明 (オプション) を入力します。PCI_DSS や GDPR などのコンプライアンスタイプを入力すると、このキーワードを使用して後でフレームワークを検索できます。
4. [タグ] で、[新しいタグを追加] を選択して、タグをフレームワークに関連付けます。タグごとにキーと値を指定できます。タグキーは必須です。フレームワークライブラリでこのフレームワークを検索するときに、検索条件として使用できます。
5. [次へ] をクリックします。

ステップ 2: コントロールセットを指定する

次に、フレームワークに追加するコントロールと、それらを整理する方法を指定します。フレームワークにコントロールセットを追加することから始めて、それからコントロールセットにコントロールを追加します。

> **Note**
>
> AWS Audit Manager コンソールを使用してカスタムフレームワークを作成する場合、フレームワークごとに最大 10 個のコントロールセットを追加できます。
> Audit Manager API を使用してカスタムフレームワークを作成する場合は、10 を超えるコントロールセットを作成できます。コンソールで現在許可されているコントロールセットよりも多くのコントロールセットを追加するには、Audit Manager が提供する CreateAssessmentFramework API を使用します。

コントロールセットを指定するには

1. [Control set name] (コントロールセット名) で、コントロールセットの名前を入力します。
2. 「コントロールの追加」で、コントロールタイプのドロップダウンリストを使用して、標準コントロールまたはカスタムコントロールの 2 つのコントロールタイプのいずれかを選択します。
3. 前のステップで選択したオプションに基づいて、標準コントロールまたはカスタムコントロールのいずれかのリストが表示されます。1 つ以上のコントロールを選択し、コントロールセットに追加を選択します。
4. 表示されるポップアップウィンドウで、コントロールセット に追加を選択します。
5. 選択したコントロールリストに表示されるコントロールを確認します。
   - さらにコントロールを追加するには、ステップ 2~4 を繰り返します。
   - 不要なコントロールを削除するには、1 つ以上のコントロールを選択し、コントロールの削除を選択します。
6. 新しいコントロールセットを追加するには、コントロールセットの追加 を選択します。
7. 不要なコントロールセットを削除するには、コントロールセットの削除 を選択します。
8. コントロールセットとコントロールの追加が完了したら、[次へ] を選択します。

ステップ 3: フレームワークを確認して作成する

フレームワークに関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。

完了したら、[カスタムフレームワークを作成] を選択します。

次のステップ

新しいカスタムフレームワークを作成したら、フレームワークから評価を作成できます。詳細については、「での評価の作成 AWS Audit Manager」を参照してください。

後でカスタムフレームワークを再確認するには、「」を参照してくださいで利用可能なフレームワークの検索 AWS Audit Manager。カスタムフレームワークを表示、編集、共有、または削除できるように、次のステップに従ってカスタムフレームワークを見つけることができます。

追加リソース

Audit Manager で問題をフレームワークする解決策については、「」を参照してくださいフレームワークの問題のトラブルシューティング。

で既存のフレームワークの編集可能なコピーを作成する AWS Audit Manager

カスタムフレームワークをゼロから作成する代わりに、既存のフレームワークを開始点として使用し、編集可能なコピーを作成できます。これを行うと、既存のフレームワークはフレームワークライブラリに残り、特定の設定で新しいカスタムフレームワークが作成されます。

既存のフレームワークの編集可能なコピーを作成できます。標準フレームワークまたはカスタムフレームワークのいずれかとすることができます。

前提条件

IAM アイデンティティに、 でカスタムフレームワークを作成するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

タスク

- ステップ 1: フレームワークの詳細を指定する
- ステップ 2: コントロールセットを指定する
- ステップ 3: フレームワークを確認して作成する

ステップ 1: フレームワークの詳細を指定する

タグを除くすべてのフレームワークの詳細は、元のフレームワークから引き継がれます。必要に応じて、これらの詳細を確認して変更します。

フレームワークの詳細を指定するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Framework library] (フレームワークライブラリ) を選択します。
3. 開始点として使用するフレームワークを選択し、カスタムフレームワークの作成 を選択し、コピーの作成 を選択します。
4. 表示されるポップアップウィンドウで、新しいカスタムフレームワークの名前を入力し、続行 を選択します。
5. フレームワークの詳細 で、フレームワークの名前、コンプライアンスタイプ、説明を確認し、必要に応じて変更します。コンプライアンスタイプは、フレームワークに関連付けられているコンプライアンス標準または規制を示すものである必要があります。このキーワードを使用して、フレームワークを検索できます。
6. [タグ] で、[新しいタグを追加] を選択して、タグをフレームワークに関連付けます。タグごとにキーと値を指定できます。タグキーは必須であり、フレームワークライブラリでこのフレームワークを検索するときに検索条件として使用できます。
7. [次へ] をクリックします。

ステップ 2: コントロールセットを指定する

コントロールセットは、元のフレームワークから引き継がれます。必要に応じて、コントロールをさらに追加するか、既存のコントロールを削除して、現在の設定を変更します。

> **Note**
>
> Audit Manager コンソールを使用してカスタムフレームワークを作成する場合、フレームワークごとに最大 10 個のコントロールセットを追加できます。
> Audit Manager API を使用してカスタムフレームワークを作成する場合は、10 を超えるコントロールセットを追加できます。コンソールで現在許可されているコントロー

ルセットよりも多くのコントロールセットを追加するには、Audit Manager が提供する CreateAssessmentFramework API を使用します。

コントロールセットを指定するには

1. コントロールセット名 で、必要に応じてコントロールセットの名前を変更します。
2. 「コントロールの追加」で、ドロップダウンリストを使用して、標準コントロールまたはカスタムコントロールの 2 つのコントロールタイプのいずれかを選択して、新しいコントロールを追加します。
3. 前のステップで選択したオプションに基づいて、標準コントロールまたはカスタムコントロールのいずれかのリストが表示されます。1 つ以上のコントロールを選択し、コントロールセットに追加を選択します。
4. 表示されるポップアップウィンドウで、コントロールセット に追加 を選択します。
5. 選択したコントロールリストに表示されるコントロールを確認します。
   - さらにコントロールを追加するには、ステップ 2~4 を繰り返します。
   - 不要なコントロールを削除するには、1 つ以上のコントロールを選択し、コントロールの削除を選択します。
6. フレームワークに新しいコントロールセットを追加するには、コントロールセットの追加 を選択します。
7. 不要なコントロールセットを削除するには、コントロールセットの削除 を選択します。
8. コントロールセットとコントロールの追加が完了したら、[次へ] を選択します。

ステップ 3: フレームワークを確認して作成する

フレームワークに関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。

完了したら、[カスタムフレームワークを作成] を選択します。

次のステップ

新しいカスタムフレームワークを作成したら、フレームワークから評価を作成できます。詳細については、「での評価の作成 AWS Audit Manager」を参照してください。

後でカスタムフレームワークを再確認するには、「」を参照してください[で利用可能なフレームワークの検索 AWS Audit Manager]。カスタムフレームワークを表示、編集、共有、または削除できるように、次のステップに従ってカスタムフレームワークを見つけることができます。

追加リソース

Audit Manager で問題をフレームワークする解決策については、「」を参照してください[フレームワークの問題のトラブルシューティング]。

でのカスタムフレームワークの編集 AWS Audit Manager

コンプライアンス要件の変化 AWS Audit Manager に応じて、 でカスタムフレームワークを変更する必要がある場合があります。

このページでは、カスタムフレームワークの詳細とコントロールセットを編集する手順の概要を説明します。

前提条件

次の手順は、カスタムフレームワークを以前に作成したことを前提としています。

IAM アイデンティティに、 でカスタムフレームワークを編集するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、[AWSAuditManagerAdministratorAccess]と です[ユーザーには AWS Audit Managerへの管理アクセスを許可します]。

手順

タスク

- [ステップ 1: フレームワークの詳細を編集する]
- [ステップ 2: コントロールセットを編集する]
- [ステップ 3。確認して保存する]

ステップ 1: フレームワークの詳細を編集する

既存のフレームワークの詳細を確認して編集することから始めます。

フレームワークの詳細を編集するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[フレームワークライブラリ] を選択し、[カスタムフレームワークを作成] を選択します。
3. 編集するフレームワークを選択し、[アクション]、[編集] の順に選択します。
   - または、カスタムフレームワークを開き、フレームワークの詳細ページの右上にある編集を選択します。
4. フレームワークの詳細 で、フレームワークの名前、コンプライアンスタイプ、説明を確認し、必要な変更を加えます。
5. [次へ] をクリックします。

> **Tip**
>
> フレームワークのタグを編集するには、フレームワークを開いて、フレームワーク タグ タブを選択します。そこで、フレームワークに関連付けられているタグを表示および編集できます。

ステップ 2: コントロールセットを編集する

次に、フレームワークのコントロールとコントロールセットを確認して編集します。

> **Note**
>
> AWS Audit Manager コンソールを使用してカスタムフレームワークを編集する場合、フレームワークごとに最大 10 個のコントロールセットを追加できます。
> Audit Manager API を使用してカスタムフレームワークを編集する場合は、10 を超えるコントロールセットを追加できます。コンソールで現在許可されているコントロールセットよりも多くのコントロールセットを追加するには、Audit Manager が提供する UpdateAssessmentFramework API を使用します。

コントロールセットを編集するには

1. [コントロールセット名] で、必要に応じてコントロールセットの名前を確認および編集します。

2. 「コントロールの追加」の「コントロールタイプ」ドロップダウンリストを使用して、「標準コントロール」または「カスタムコントロール」の 2 つのコントロールタイプのいずれかを選択します。
3. 前のステップで選択したオプションに応じて、標準コントロールまたはカスタムコントロールのいずれかのテーブルリストが表示されます。1 つ以上のコントロールを選択し、コントロールセット に追加を選択します。
4. 表示されるポップアップウィンドウで、「追加」を選択します。
5. 選択したコントロールリストに表示されるコントロールを確認して編集します。
   - さらにコントロールを追加するには、ステップ 2～4 を繰り返します。
   - 不要なコントロールを削除するには、1 つ以上のコントロールを選択し、コントロールセットから削除を選択します。
6. フレームワークに新しいコントロールセットを追加するには、コントロールセットの追加 を選択します。
7. 不要なコントロールセットを削除するには、コントロールセットの削除 を選択します。
8. コントロールセットとコントロールの追加が完了したら、[次へ] を選択します。

ステップ 3。確認して保存する

フレームワークに関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。

完了したら、[変更の保存] を選択します。

次のステップ

カスタムフレームワークが不要になったことを確認したら、フレームワークを削除して Audit Manager 環境をクリーンアップできます。手順については、「でのカスタムフレームワークの削除 AWS Audit Manager」を参照してください。

追加リソース

Audit Manager で問題をフレームワークする解決策については、「」を参照してくださいフレームワークの問題のトラブルシューティング。

でのカスタムフレームワークの共有 AWS Audit Manager

のフレームワーク共有機能を使用して AWS Audit Manager 、作成したカスタムフレームワークをすばやくレプリケートできます。カスタムフレームワークを別の と共有したり AWS アカウント、自分のアカウント AWS リージョン で別の にフレームワークをレプリケートしたりできます。その後、受信者はカスタムフレームワークにアクセスし、それを使用して評価を作成できます。これらの受信者は、そのフレームワークの設定作業を繰り返すことなく、評価を作成できます。

重要ポイント

カスタムフレームワークを共有するには、[共有リクエスト] を作成します。共有リクエストの受信者は、120 日以内にリクエストを承諾または拒否できます。受信者が共有リクエストを承諾すると、Audit Manager は、共有カスタムフレームワークを、それらの受信者のフレームワークライブラリにレプリケートします。カスタムフレームワークをレプリケートすることに加えて、Audit Manager は、そのフレームワークの一部であるカスタムコントロールセットとカスタムコントロールもレプリケートします。これらのカスタムコントロールは、受信者のコントロールライブラリに追加されます。Audit Manager は、標準のフレームワークまたはコントロールをレプリケートしません。デフォルトでは、これらは Audit Manager が有効になっているすべての AWS アカウント とリージョンで使用できます。

フレームワーク共有機能は、有料階層でのみ使用できます。ただし、カスタムフレームワークを共有したり、共有リクエストを承諾したりするための追加料金はかかりません。の料金の詳細については AWS Audit Manager、「 のAWS Audit Manager 料金」ページを参照してください。

> **Important**
>
> 標準フレームワークの所有者から許可を取得していない限り、標準フレームワークが による共有の対象外として指定されている場合 AWS、標準フレームワークから派生したカスタムフレームワークを共有することはできません。共有のための要件を満たさない標準フレームワーク、および詳細を確認するには、「フレームワーク共有の適格性」を参照してください。

追加リソース

Audit Manager でカスタムフレームワークを共有する方法の詳細については、以下のリソースを参照してください。

- フレームワークの共有に関する概念と用語
- でカスタムフレームワークを共有するためのリクエストの送信 AWS Audit Manager

- でリクエストを共有する応答 AWS Audit Manager
- での共有リクエストの削除 AWS Audit Manager

フレームワークの共有に関する概念と用語

次の重要な概念について学ぶことで、 AWS Audit Manager カスタムフレームワーク共有機能をさらに活用できます。

重要ポイント

送信者

これは共有リクエストの作成者と、カスタムフレームワークが存在する AWS アカウント です。送信者は、任意の とカスタムフレームワークを共有できます AWS アカウント。または、独自のアカウントでサポートされている にカスタムフレームワークをレプリケート AWS リージョン します。

受取人

これは、共有フレームワークの利用者です。受信者は、送信者からの共有リクエストを承諾または拒否できます。

> **Note**
>
> 委任された管理者アカウントも受信者となることができます。ただし、カスタムフレームワーク AWS Organizations を管理アカウントと共有することはできません。

フレームワークの適格性

共有できるのはカスタムフレームワークのみです。デフォルトでは、標準フレームワークは、 が有効になっているすべての AWS アカウント と AWS リージョン AWS Audit Manager にすでに存在します。さらに、共有するカスタムフレームワークに機密データが含まれていてはなりません。これには、フレームワーク自体、そのコントロールセット、およびカスタムフレームワークの一部であるカスタムコントロール内にあるデータが含まれます。

> **Important**
>
> が提供する標準フレームワークの一部には、ライセンス契約の対象となる著作権で保護されたマテリアル AWS Audit Manager が含まれています。カスタムフレームワークには、

これらのフレームワークから派生したコンテンツが含まれている場合があります。標準フレームワークの所有者から共有の許可を取得していない限り、標準フレームワークが によるAWS共有の対象外として指定されている場合、標準フレームワークから派生したカスタムフレームワークを共有することはできません。
共有の要件を満たしている標準フレームワークについては、次の表」を参照してください。

標準フレームワーク名	共有の要件を満たしているカスタムバージョン
オーストラリアサイバーセキュリティセンター (ACSC) Essential Eight	 はい
オーストラリアサイバーセキュリティセンター (ACSC) 情報セキュリティマニュアル (ISM) 2023 年 3 月 2 日	 はい
Amazon Web Services (AWS) Audit Manager サンプルフレームワーク	 はい
AWS Control Tower ガードレール	 はい
AWS 生成 AI ベストプラクティスフレームワーク v2	 はい

標準フレームワーク名	共有の要件を満たしているカスタムバージョン
AWS License Manager	はい
AWS 基本的なセキュリティのベストプラクティス	はい
AWS 運用のベストプラクティス	はい
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	はい
カナダサイバーセキュリティセンター (CCCS) Medium Cloud Control	いえ
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0、レベル 1	いえ
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0、レベル 1 および 2	いえ

標準フレームワーク名	共有の要件を満たしているカスタムバージョン	
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0、レベル 1	 いえ	い
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0、レベル 1 および 2	 いえ	い
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0、レベル 1	 いえ	い
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0、レベル 1 および 2	 いえ	い
Center for Internet Security (CIS) v7.1、IG1	 い	は
CIS Critical Security Controls バージョン 8.0 (CIS v8.0)、IG1	 いえ	い
Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4、Moderate	 い	は

標準フレームワーク名	共有の要件を満たしているカスタムバージョン
一般データ保護規則 (GDPR) 2016 年	 はい
グラムリーチブライリー法 (GLBA、Gramm-Leach-Bliley Act)	 はい
タイトル 21 連邦規則 (CFR) Part 11、電子記録、電子署名 - スコープとアプリケーション 2023 年 5 月 24 日	 はい
EudraLex - 欧州連合 (EU) の医薬品を管理する規則 - 第 4 部: 適正製造規範 (GMP) 人間および獣医学用の医薬品 - Annex 11	 はい
医療保険の相互運用性と説明責任に関する法律 (HIPAA) セキュリティルール: 2003 年 2 月	 はい
医療保険の相互運用性と説明責任に関する法律 (HIPAA) オムニバス最終規則	 はい
国際標準化機構 (ISO)/国際電気標準会議 (IEC) 27001:2013 附属書 A	 いえ

標準フレームワーク名	共有の要件を満たしているカスタムバージョン
NIST 800-53 Rev 5: 情報システムと組織のセキュリティとプライバシーコントロール	 はい
NIST サイバーセキュリティフレームワーク (CSF) v1.1	 はい
NIST 800-171 リビジョン 2: 非連邦システムおよび組織における制御された未分類情報の保護	 はい
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	 いいえ
Payment Card Industry Data Security Standard (PCI DSS) v4.0	 いいえ
認証エンゲージメント標準に関するステートメント (SSAE) No. 18、Service Organizations Controls (SOC) Report 2	 いいえ

共有リクエスト

カスタムフレームワークを共有するには、[share request] (共有リクエスト) を作成します。共有リクエストは、受信者を指定し、カスタムフレームワークが利用可能であることを通知します。

受信者は、承諾または辞退によって共有リクエストに応答するまでに 120 日間の猶予期間があります。120 日以内にアクションが実行されない場合、共有リクエストは期限切れになり、受信者はカスタムフレームワークをフレームワークライブラリに追加できなくなります。送信者と受信者は、フレームワークライブラリの共有リクエストのページから共有リクエストを表示してアクションを実行できます。

共有リクエストのステータス

共有リクエストのステータスは以下のいずれかです。

ステータス	説明
[アクティブ]	これは、受信者に正常に送信され、応答を待っている共有リクエストを示します。
有効期限切れ	これは、30 日以内に期限切れになる共有リクエストを示します。
共有	これは、受信者が承諾した共有リクエストを示します。
無効	これは、受信者がアクションを実行する前に取り消し、拒否、または期限切れになった共有リクエストを示します。
レプリケーション	これは、受信者のフレームワークライブラリにレプリケートされる承認済みの共有リクエストを示します。
[失敗]	これは、受信者に正常に送信されなかった共有リクエストを示します。

リクエスト通知を共有する

Audit Manager は、受信者が共有リクエストを受信すると通知します。共有リクエストの有効期限が 30 日以内に迫ると、受信者と送信者の両方に通知が届きます。

- 受信者の場合、受信したリクエストの横に青い通知ドットが、[Active] (アクティブ) または [Expiring] (まもなく期限切れ) のステータスとともに表示されます。受信者は、共有リクエストを承諾または辞退することで通知を解決できます。
- 送信者の場合、送信したリクエストの横に青い通知ドットが、[Expiring] (まもなく期限切れ) のステータスとともに表示されます。受信者がリクエストを承諾または辞退すると、通知は解決

されます。それ以外の場合は、リクエストの有効期限が切れたときに解決されます。さらに、送信者は共有リクエストを取り消すことで通知を解決できます。

送信者の所有権

送信者は、共有するカスタムフレームワークに引き続き完全にアクセスできます。有効期限が切れる前に共有リクエストを取り消すことで、アクティブな共有リクエストをいつでもキャンセルできます。ただし、受信者が共有リクエストを承諾すると、送信者はそのカスタムフレームワークへの受信者のアクセスを取り消すことができなくなります。これは、受信者がリクエストを受け入れると、Audit Manager が受信者のフレームワークライブラリにカスタムフレームワークの独立したコピーを作成するためです。

送信者のカスタムフレームワークをレプリケートすることに加えて、Audit Manager は、そのフレームワークの一部であるカスタムコントロールセットとカスタムコントロールもレプリケートします。ただし、Audit Manager は、カスタムフレームワークにアタッチされているタグをレプリケートしません。

受信者の所有権

受信者は、承諾したカスタムフレームワークに完全にアクセスできます。受信者がリクエストを承諾すると、Audit Manager は、フレームワークライブラリのカスタムフレームワークのタブにカスタムフレームワークをレプリケートします。受信者は、他のカスタムフレームワークと同じ方法で共有カスタムフレームワークを管理できます。受信者は、他の送信者から受信したカスタムフレームワークを共有できます。受信者は、送信者が共有リクエストを送信するのをブロックすることはできません。

共有されたフレームワークの有効期限

送信者が共有リクエストを作成する際、Audit Manager は、120 日後に期限切れになるようにリクエストを設定します。受信者は、リクエストの有効期限が切れる前に、共有されたフレームワークを承諾してアクセスできます。この間に受信者が承諾しない場合、共有リクエストは期限切れになります。この時点を過ぎると、期限切れの共有リクエストの記録は履歴に残ります。期限切れの共有フレームワークのスナップショットは、監査の目的のために 1 年間の TTL で S3 バケットにアーカイブされます。

送信者は、有効期限が切れる前であればいつでも共有リクエストを取り消すことができます。

共有フレームワークのデータストレージとバックアップ

共有リクエストを作成すると、Audit Manager はカスタムフレームワークのスナップショットを米国東部 (バージニア北部) に保存します。 AWS リージョン Audit Manager は、同じスナップショットのバックアップを米国西部 (オレゴン) にも保存します AWS リージョン。

Audit Manager は、次のいずれかのイベントが発生したときにスナップショットとバックアップスナップショットを削除します。

- 送信者が共有リクエストを取り消す。
- 受信者が共有リクエストを拒否する。
- 受信者がエラーに遭遇し、共有リクエストを正常に承諾できない。
- 受信者がリクエストに応答する前に、共有リクエストの有効期限が切れる。

送信者が共有リクエストを再送信すると、スナップショットはカスタムフレームワークの最新バージョンに対応する更新バージョンに置き換えられます。

受信者が共有リクエストを受け入れると、スナップショットは共有リクエストで AWS リージョン 指定された AWS アカウント の にレプリケートされます。

共有されたフレームワークのバージョン管理

カスタムフレームワークを共有すると、Audit Manager は指定された AWS アカウント およびリージョンにそのフレームワークの独立したコピーを作成します。このことは、次の点に留意する必要があることを意味します。

- 受信者が承諾する共有されたフレームワークは、共有リクエストの作成時のフレームワークのスナップショットです。共有リクエストを送信した後に元のカスタムフレームワークを更新しても、リクエストは自動的に更新されません。更新されたフレームワークの最新バージョンを共有するには、共有リクエストを再送信できます。この新しいスナップショットの有効期限は、再共有された日から 120 日です。
- カスタムフレームワークを別のフレームワークと共有し AWS アカウント 、フレームワークライブラリから削除すると、共有カスタムフレームワークは受信者のフレームワークライブラリに残ります。
- AWS リージョン アカウントの別の とカスタムフレームワークを共有し、最初の でそのカスタムフレームワークを削除すると AWS リージョン、カスタムフレームワークは 2 番目のリージョンに残ります。
- 共有されたカスタムフレームワークを承諾した後に削除すると、カスタムフレームワークの一部としてレプリケートされたカスタムコントロールはすべてコントロールライブラリに残ります。

追加リソース

- でカスタムフレームワークを共有するためのリクエストの送信 AWS Audit Manager

- でリクエストを共有する応答 AWS Audit Manager
- での共有リクエストの削除 AWS Audit Manager
- フレームワークの問題のトラブルシューティング

でカスタムフレームワークを共有するためのリクエストの送信 AWS Audit Manager

このチュートリアルでは、カスタムフレームワークを AWS アカウント および 間で共有する方法について説明します AWS リージョン。

カスタムフレームワークを共有すると、Audit Manager は、フレームワークのスナップショットを作成し、共有リクエストを受信者に送信します。受信者が共有されたフレームワークを承諾するまでに 120 日間の猶予期間があります。承諾されると、Audit Manager は、指定された AWS リージョンのフレームワークライブラリに共有されたカスタムフレームワークをレプリケートします。カスタムフレームワークを自分のアカウントで別のリージョンにレプリケートする場合は、次のチュートリアルを使用して、受信者アカウント AWS アカウント ID として自分の ID を入力します。

前提条件

このチュートリアルを開始する前に、次の条件を満たしていることを確認してください。

- Audit Manager のフレームワークに関する概念と用語に精通していること。
- 共有するカスタムフレームワークが共有のための要件を満たしており、 AWS Audit Manager 環境のフレームワークライブラリに存在していること。
- 受信者は、カスタムフレームワークを共有する AWS リージョン AWS Audit Manager で既に を有効にしています。
- 受信者は AWS Organizations 管理アカウントではありません。
- IAM アイデンティティには、 でカスタムフレームワークを共有するための適切なアクセス許可があります AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

> **Tip**
>
> 開始する前に、カスタムフレームワークを共有する AWS アカウント ID を書き留めます。これは、フレームワークをアカウント AWS リージョン 内の別の にレプリケートすることを目

標としている場合、独自のアカウント ID にすることができます。この情報は、チュートリアルのステップ 2 で必要です。

手順

タスク

- ステップ 1: 共有するカスタムフレームワークを特定する
- ステップ 2: 共有リクエストを送信する
- ステップ 3: 送信済みのリクエストを表示する
- ステップ 4 (オプション): 共有リクエストを取り消す

ステップ 1: 共有するカスタムフレームワークを特定する

共有するカスタムフレームワークを特定することから始めます。使用可能なすべてのカスタムフレームワークのリストは、Audit Manager のフレームワークライブラリのページにあります。

Important

機密データを含むカスタムフレームワークを共有しないでください。これには、フレームワーク自体、そのコントロールセット、およびカスタムフレームワークを構成するカスタムコントロール内にあるデータが含まれます。詳細については、「フレームワーク適格性」を参照してください。

使用可能なカスタムフレームワークを表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Framework library] (フレームワークライブラリ) を選択します。
3. [Custom frameworks] (カスタムフレームワーク) のタブを選択します。これにより、使用可能なカスタムフレームワークのリストが表示されます。任意のフレームワーク名を選択して、そのカスタムフレームワークの詳細を表示できます。

ステップ 2: 共有リクエストを送信する

次に、受信者を指定して、カスタムフレームワークの共有リクエストを送信します。受信者は、シェア要求が期限切れになる前に、120 日以内に返答しなければならない。

共有リクエストを送信するには

1. フレームワークライブラリの [カスタムフレームワーク] タブから、フレームワークの名前を選択して詳細ページを開きます。ここから、[Actions] (アクション) を選択してから、[Share custom framework] (カスタムフレームワークを共有) を選択します。
   - または、フレームワークライブラリのリストからカスタムフレームワークを選択し、[アクション]、[カスタムフレームワークを共有] の順に選択します。カスタムフレームワークのサイズによっては、Audit Manager による共有リクエストの準備中、このメソッドに数秒かかることがあります。
2. ダイアログボックスに表示される通知を確認します。
   - カスタムフレームワークを共有できるかどうかわからない場合は、[Framework eligibility] (フレームワークの適格性) を確認して、詳細なガイダンス」を参照してください。
   - フレームワークにデータソースとしてカスタム AWS Config ルールを使用するコントロールがある場合は、受信者に連絡して通知することをお勧めします。その後、受信者は のインスタンスで同じ AWS Config ルールを作成して有効にできます AWS Config。詳細については、「共有フレームワークには、データソースとしてカスタム AWS Config ルールを使用するコントロールがあります。受信者はこれらのコントロールを収集することができますか?」を参照してください。
3. **agree** と入力し、[同意] を選択して続行します。
4. 次の画面で、以下のステップを実行します。
   - AWS アカウント で、受信者のアカウント ID を入力します。自分のアカウント ID も使用できます。
   - AWS リージョン で、ドロップダウンリストから受信者のリージョンを選択します。
   - (オプション) [受信者へのメッセージ] で、共有しようとしているカスタムフレームワークに関するオプションのコメントを入力します。
   - [カスタムフレームワークの詳細] で、詳細を確認して、このフレームワークを共有することを確認します。
5. [共有] を選択します。

> **Note**
>
> 次のポイントに注意が必要です。
>
> - カスタムフレームワークを別の と共有する場合 AWS アカウント、フレームワークは指定された にのみレプリケートされます AWS リージョン。共有リクエストを承諾すると、受信者は、必要に応じて複数のリージョンでフレームワークをレプリケートできます。
> - 間でカスタムフレームワークを共有する場合 AWS リージョン、共有リクエストアクションの処理に最大 10 分かかることがあります。クロスリージョン共有リクエストを送信した後、後でもう一度確認して、共有リクエストが正常に送信されたことを確認することをお勧めします。
> - 共有リクエストを送信すると、Audit Manager は、共有リクエストの作成時にカスタムフレームワークのスナップショットを取得します。共有リクエストを送信した後にカスタムフレームワークを更新しても、リクエストは自動的に更新されません。更新されたフレームワークの最新バージョンを共有するには、共有リクエストを再送信できます。この新しいスナップショットの有効期限は、再共有された日から 120 日です。

ステップ 3: 送信済みのリクエストを表示する

[Sent requests] (送信済みリクエスト) のタブを選択すると、送信したすべての共有リクエストのリストが表示されます。必要に応じて、このリストをフィルタリングできます。例えば、フィルターを適用して、今後 30 日以内に期限切れになるリクエストのみを表示できます。

送信済みのリクエストを表示してフィルタリングするには

1. ナビゲーションペインから、[Share requests] (共有リクエスト) を選択します。
2. [Sent requests] (送信済みのリクエスト) のタブを選択します。
3. (オプション) フィルターを適用して、表示される送信済みのリクエストを微調整します。これを実行するには、[All statuses] (すべてのステータス) のドロップダウンリストを見つけて、フィルターを次のいずれかに変更します。

ステータス	説明
[アクティブ]	このフィルターは、受信者からの応答を待っている共有リクエストを表示します。

ステータス	説明
有効期限切れ	このフィルターは、30 日以内に期限切れになる共有リクエストを表示します。
共有	このフィルターは、受信者が承諾した共有リクエストを表示します。共有されたカスタムフレームワークは、受信者のフレームワークライブラリに存在するようになりました。
無効	このフィルターは、受信者がアクションを実行する前に拒否、取り消し、または期限切れになった共有リクエストを表示します。詳細を表示するには、[Inactive] (非アクティブ) という単語を選択します。
レプリケーション	これは、受信者のフレームワークライブラリにレプリケートされる承認済みの共有リクエストを示します。
[失敗]	このフィルターは、受信者に正常に送信されなかった共有リクエストを表示します。詳細を表示するには、[Failed] (失敗) という単語を選択します。

> **Note**
>
> 共有リクエストの処理には最長で 15 分かかる場合があります。その結果、共有リクエストを受信者に送信するときにエラーが発生した場合、[Failed] (失敗) ステータスがすぐに表示されない場合があります。後でもう一度確認して、共有リクエストが正常に送信されたことを確認することをお勧めします。

ステップ 4 (オプション): 共有リクエストを取り消す

有効期限が切れる前にアクティブな共有リクエストをキャンセルする必要がある場合は、いつでもリクエストを取り消すことができます。この手順は省略可能です。何もしなかった場合、受信者は、有効期限が切れると共有リクエストを承諾できなくなります。

共有リクエストを取り消すには

1. ナビゲーションペインから、[Share requests] (共有リクエスト) を選択します。

2. [Sent requests] (送信済みのリクエスト) のタブを選択します。
3. 取り消すフレームワークを選択し、[Revoke request] (リクエストを取り消す) を選択します。
4. 表示されるポップアップウィンドウで、[Revoke] (取り消す) を選択します。

> **Note**
>
> ステータスが [Active] (アクティブ) または [Expiring] (まもなく期限切れ) の共有リクエストへのアクセスのみを取り消すことができます。受信者が共有リクエストを承諾すると、そのカスタムフレームワークへのアクセスを取り消すことはできなくなります。これは、カスタムフレームワークのコピーが受信者のフレームワークライブラリに存在するようになるためです。
> 間でフレームワークを共有する場合 AWS リージョン、共有リクエストアクションの処理に最大 10 分かかることがあります。クロスリージョン共有リクエストを取り消した後、後でもう一度確認して、共有リクエストが正常に取り消されたことを確認することをお勧めします。

次のステップ

更新されたフレームワークの共有リクエストを再送信する

カスタムフレームワークの共有リクエストを送信し、後で同じフレームワークを更新することができます。この操作を実行すると、フレームワークの最新バージョンを反映するように共有リクエストが自動的に更新されません。ただし、そのステータスが [active] (アクティブ)、[shared] (共有)、または [expiring] (まもなく期限切れ) の場合は、既存の共有リクエストを更新できます。これを実行するには、既存のリクエストと同じ一連の詳細を使用して、新しい共有リクエストを再送信します。新しい共有リクエストには、同じカスタムフレームワーク ID、受信者アカウント ID、および受信者の AWS リージョンを含めます。新しい共有リクエストで新しいコメントを提供することもできます。

共有リクエストを再送信するときは、次の点に注意してください。

- 更新を正常に完了するには、新しいリクエストが同じカスタムフレームワーク ID についてのものである必要があります。また、既存のリクエストと同じ受信者アカウント ID およびリージョンを指定する必要があります。
- カスタムフレームワークの名前が変更された場合、更新された共有リクエストは最新の名前を表示します。
- 新しいコメントを提供すると、更新された共有リクエストは最新のコメントを表示します。

- 共有リクエストを再送信すると、有効期限が 6 か月間延長されます。

更新されたフレームワークの共有リクエストを再送信するには

1. フレームワークライブラリの [カスタムフレームワーク] のタブから、リクエストを再送信する更新されたフレームワークを選択します。これにより、フレームワークの詳細ページが開きます。
2. アクション を選択し、カスタムフレームワークの共有 を選択します。
3. ダイアログ ボックスに表示される通知を確認し、「**agree**」を入力し、[同意] を選択して続行します。
4. 次の画面で、以下のステップを実行します。
   - AWS アカウント で、既存の共有リクエストで指定したものと同じアカウント ID を入力します。
   - AWS リージョン で、既存の共有リクエストで指定したものと同じリージョンを選択します。
   - (オプション) [受信者へのメッセージ] で、更新されたカスタムフレームワークに関するオプションのコメントを入力します。
   - [カスタムフレームワークの詳細] で、詳細を確認して、共有リクエストを再送信することを確認します。
5. [共有] を選択して、共有リクエストを再送信および更新します。

追加リソース

カスタムフレームワークの共有時に発生する可能性のある問題の解決策については、「」を参照してくださいフレームワークの問題のトラブルシューティング。

でリクエストを共有する応答 AWS Audit Manager

このチュートリアルでは、カスタムフレームワークの共有リクエストを受信したときに実行するアクションについて説明します。Audit Manager は、ユーザーが共有リクエストを受信すると通知します。また、共有リクエストが 30 日以内に期限切れになる場合に注意喚起するための通知を受け取ります。

前提条件

開始する前に、まず Audit Manager のフレームワークの共有の概念と用語の詳細を確認することをお勧めします。

手順

タスク

- ステップ 1: 受信したリクエスト通知を確認する
- ステップ 2: リクエストに対してアクションを実行する
- ステップ 3: 受信したリクエストの履歴を表示する

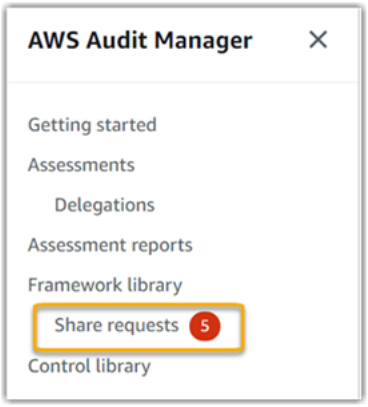
ステップ 1: 受信したリクエスト通知を確認する

共有リクエストの通知を確認することから始めます。受信リクエストタブには、他の から受信した共有リクエストのリストが表示されます AWS アカウント。レスポンスを待機しているリクエストについては青いドットが表示されます。このビューをフィルタリングして、今後 30 日以内に期限切れになるリクエストのみを表示することもできます。

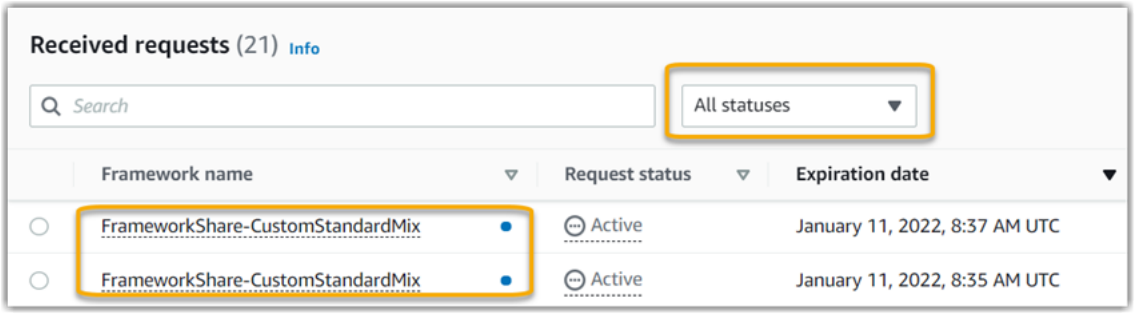
受信したリクエストを表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 共有リクエスト通知がある場合、Audit Manager は、ナビゲーションメニューのアイコンの横に赤いドットを表示します。

3. ナビゲーションペインを展開し、[共有リクエスト] の横を確認します。通知バッジは、注意が必要な共有リクエストの数を示します。



4. [共有リクエスト] を選択します。デフォルトでは、このページは [受信したリクエスト] のタブで開きます。
5. 青いドットが表示されている項目を探して、アクションが必要な共有リクエストを特定します。



6. (オプション) 今後 30 日以内に期限切れになるリクエストのみを表示するには、[すべてのステータス] ドロップダウンリストを見つけて、[まもなく期限切れ] を選択します。

ステップ 2: リクエストに対してアクションを実行する

青い通知ドットを削除するには、共有リクエストを承諾または辞退する必要があります。

共有フレームワークの承諾

共有リクエストを承諾すると、Audit Manager は、元のフレームワークのスナップショットをフレームワークライブラリのカスタムフレームワークのタブにレプリケートします。Audit Manager は、Audit Manager の設定で指定した KMS キーを使用して、新しいカスタムフレームワークをレプリケートおよび暗号化します。

共有リクエストを承諾するには

1. [共有リクエスト] のページを開き、[受信したリクエスト] のタブが表示されていることを確認します。
2. (オプション) フィルターのドロップダウンリストから [アクティブ] または [まもなく期限切れ] を選択します。
3. (オプション) フレームワーク名を選択して、共有リクエストの詳細を表示します。これには、フレームワークの説明、フレームワーク内にあるコントロールの数、送信者からのメッセージなどの情報が含まれます。
4. 承諾する共有リクエストを選択し、[アクション]、[承諾] の順に選択します。

共有リクエストを承諾すると、共有されたカスタムフレームワークがフレームワークライブラリに追加されている間、ステータスは [レプリケート中] に変わります。フレームワークにカスタムコントロールが含まれている場合、これらのコントロールは、この時点でコントロールライブラリに追加されます。

フレームワークのレプリケートが完了すると、ステータスが [共有済み] に変わります。正常に完了した旨のバナーは、カスタムフレームワークを使用する準備ができたことを通知するものです。

> **Tip**
>
> カスタムフレームワークを承諾すると、現在の AWS リージョンにのみレプリケートされます。 AWS アカウント内のすべてのリージョンで共有された新しいフレームワークを利用できるようにすることができます。その場合、共有リクエストを承諾した後、必要に応じて、アカウントで他のリージョンとフレームワークを共有できます。

共有フレームワークの辞退

共有リクエストを辞退すると、Audit Manager は、そのカスタムフレームワークをフレームワークライブラリに追加しません。ただし、辞退された共有リクエストの記録は [受信したリクエスト] タブに残り、ステータスは [非アクティブ] になります。

共有リクエストを辞退するには

1. [Share requests] (共有リクエスト) のページを開き、[Received requests] (受信したリクエスト) のタブが表示されていることを確認します。
2. (オプション) フィルターのドロップダウンリストから [アクティブ] または [まもなく期限切れ] を選択します。
3. (オプション) フレームワーク名を選択して、共有リクエストの詳細を表示します。これには、フレームワークの説明、フレームワーク内にあるコントロールの数、送信者からのメッセージなどの情報が含まれます。
4. 辞退する共有リクエストを選択し、[Actions] (アクション)、[Decline] (辞退) の順に選択します。
5. 表示されるダイアログボックスで、[Decline] (拒否) を選択して、選択内容を確認します。

> **Tip**
>
> 考えが変わり、辞退した後に共有されたフレームワークにアクセスしたい場合は、送信者に新しい共有リクエストを送信するように依頼してください。

> **Note**
>
> フレームワークが複数の AWS リージョンで共有されている場合、共有リクエストのアクションの処理には最長で 10 分かかる場合があります。クロスリージョンの共有リクエストに対してアクションを実行した後、後でもう一度確認して、共有リクエストが正常に承諾または辞退されたかを確認することをお勧めします。

ステップ 3: 受信したリクエストの履歴を表示する

共有されたフレームワークを承諾または辞退した後、[Share requests] (共有リクエスト) のページに戻って、共有リクエストの履歴を確認できます。必要に応じて、このリストをフィルタリングできます。例えば、フィルターを適用して、承諾したリクエストのみを表示できます。

共有リクエストの履歴を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[Share requests] (共有リクエスト) を選択します。
3. [Received requests] (受信したリクエスト) のタブを選択します。
4. すべてのステータスドロップダウンリストを見つけ、次のいずれかのフィルターを選択します。

名前	説明
[アクティブ]	このフィルターには、まだ承諾または拒否していない共有リクエストが表示されます。
有効期限切れ	このフィルターは、30 日以内に期限切れになる共有リクエストを表示します。
共有	このフィルターには、承諾した共有リクエストが表示されます。共有されたフレームワークがフレームワークライブラリで利用できるようになりました。
無効	このフィルターは、拒否または期限切れの共有リクエストを表示します。

名前	説明
[失敗]	このフィルターは、正常に送信されなかった共有リクエストを表示します。詳細を表示するには、[Failed] (失敗) という単語を選択します。

次のステップ

共有カスタムフレームワークを承諾すると、フレームワークライブラリのカスタムフレームワークのタブで見つけることができます。これで、そのフレームワークを使用して評価を作成できるようになりました。詳細については、「での評価の作成 AWS Audit Manager」を参照してください。

新しいカスタムフレームワークを編集する方法については、「」を参照してくださいでのカスタムフレームワークの編集 AWS Audit Manager。

追加リソース

発生する可能性のある問題の解決策については、「」を参照してくださいフレームワークの問題のトラブルシューティング。

での共有リクエストの削除 AWS Audit Manager

共有リクエストが不要になった場合は、Audit Manager 環境から削除できます。これにより、ワークスペースをクリーンアップし、現在のタスクと優先順位に関連するリクエストに集中できます。

共有リクエストを削除すると、そのリクエスト自体のみが削除されます。共有フレームワーク自体は、フレームワークライブラリに残ります。

前提条件

次の手順では、共有リクエストを以前に送信または受信したことを前提としています。ステータスが [active] (アクティブ) または [replicating] (レプリケート中) の共有リクエストを削除することはできません。

IAM アイデンティティに、 で共有リクエストを削除するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

共有リクエストを削除するには

1. ナビゲーションペインから、[Share requests] (共有リクエスト) を選択します。
2. [Sent requests] (送信済みリクエスト) または [Received requests] (受信したリクエスト) のいずれかのタブを選択します。
3. 不要になったフレームワークを選択し、[Delete] (削除) を選択します。
4. 表示されるポップアップウィンドウで、[Delete] (削除) を選択します。

追加リソース

発生する可能性のある問題の解決策については、「」を参照してくださいフレームワークの問題のトラブルシューティング。

でのカスタムフレームワークの削除 AWS Audit Manager

カスタムフレームワークが不要になった場合は、Audit Manager 環境から削除できます。これにより、ワークスペースをクリーンアップし、現在のタスクと優先順位に関連するカスタムフレームワークに集中できます。

前提条件

次の手順は、カスタムフレームワークを以前に作成したことを前提としています。

IAM アイデンティティに、 でカスタムフレームワークを削除するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用してカスタムフレームワークを削除できますAWS CLI。

> **Note**
>
> カスタムフレームワークを削除しても、削除前にそのフレームワークから作成された既存の評価には影響しません。

Audit Manager console

Audit Manager コンソールでカスタムフレームワークを削除するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、[フレームワークライブラリ] を選択し、[カスタムフレームワークを作成] を選択します。
3. 削除するフレームワークを選択し、[アクション]、[削除] の順に選択します。
   - あるいは、カスタムフレームワークを開いて、フレームワークの概要ページの右上にある [アクション]、[削除] の順に選択することもできます。
4. ポップアップウィンドウで、[削除] を選択して削除を確認します。

AWS CLI

でカスタムフレームワークを削除するには AWS CLI

1. 最初に、削除するカスタムフレームワークを特定します。これを行うには、 list-assessment-frameworks コマンドを実行し、 を `--framework-type`として指定しますCustom。

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   レスポンスはカスタムフレームワークのリストを返します。削除するカスタムフレームワークを見つけて、フレームワーク ID をメモします。
2. 次に、 delete-assessment-framework コマンドを実行し、削除するフレームワーク`--framework-id`の を指定します。

   次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

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

Audit Manager API

API を使用してカスタムフレームワークを削除するには

1. ListAssessmentFrameworks オペレーションを使用して、 frameworkType を として指定しますCustom。レスポンスから削除するカスタムフレームワークを見つけ、フレームワーク ID をメモします。
2. DeleteAssessmentFramework オペレーションを使用してフレームワークを削除します。リクエストで frameworkId パラメータを使用して、削除するフレームワークを指定します。

これらの API オペレーションの詳細については、前の手順のリンクのいずれかを選択して、AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

追加リソース

Audit Manager のデータ保持の詳細については、「」を参照してくださいAudit Manager のデータの削除。

コントロールライブラリを使用して でコントロールを管理する AWS Audit Manager

のコントロールライブラリからコントロールにアクセスして管理できます AWS Audit Manager。

重要ポイント

コントロールライブラリでは、コントロールは次のカテゴリに分類されます。

- 共通コントロールは、重複する複数のコンプライアンス標準をサポートする証拠を収集します。自動共通コントロールには、それぞれが事前定義されたデータソースグループからサポート証拠を収集する 1 つ以上の関連するコアコントロールが含まれています。これにより、コンプライアンス要件のポートフォリオにマッピングされる AWS データソースを効率的に特定できます。各自動化された共通コントロールの基盤となるデータソースは、AWS セキュリティ保証サービスで業界認定評価者によって検証され、維持されます。
- 標準コントロールは、特定のコンプライアンス標準をサポートする証拠を収集します。標準コントロールの詳細を表示できますが、編集または削除することはできません。ただし、標準コントロールの編集可能なコピーを作成して、特定の要件を満たす新しいコントロールを作成できます。
- カスタムコントロールは、ユーザーが所有および定義するコントロールです。カスタムコントロールを作成するときは、目標を表す一般的なコントロールを選択し、証拠ソースとして使用することをお勧めします。その結果、カスタムコントロールは、これらの一般的なコントロールに関連するすべての証拠を収集できます。また、コアコントロールを証拠ソースとして使用したり、自分で定義した他のソースを使用したりできます。完了したら、カスタムコントロールをカスタムフレームワークに追加し、評価を作成して証拠の収集を開始します。

追加リソース

Audit Manager でコントロールを作成および管理するには、ここで概説されている手順に従ってください。

- で使用可能なコントロールの検索 AWS Audit Manager
- でのコントロールの確認 AWS Audit Manager
  - 共通コントロールの確認

で使用可能なコントロールの検索 AWS Audit Manager

Audit Manager コンソールのコントロールライブラリページで、使用可能なすべてのコントロールを確認できます。

Audit Manager API または AWS Command Line Interface () を使用して、使用可能なすべてのコントロールを表示することもできますAWS CLI。

前提条件

IAM アイデンティティに、 でコントロールを表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager console

Audit Manager コンソールで使用可能なコントロールを表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Control library] (ライブラリを管理) を選択します。
3. タブを選択して、使用可能なコントロールを参照します。

   - Common を選択すると、 によって提供される一般的なコントロールが表示されます AWS。
   - 標準 を選択して、 が提供する標準コントロールを表示します AWS。
   - カスタム を選択して、作成したカスタムコントロールを表示します。

AWS CLI

で一般的なコントロールを見つけるには (AWS CLI

list-common-controls コマンドを実行して、一般的なコントロールのリストを表示します。

```
aws controlcatalog list-common-controls
```

オプションの common-control-filter 属性を使用して、特定の目的を持つ一般的なコントロールのリストを返すこともできます。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

で他のタイプのコントロールを検索するには AWS CLI

list-controls コマンドを実行し、 を Custom、Standard、または --control-typeとして指定しますCore。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager list-controls --control-type Type
```

Audit Manager API

API を使用して一般的なコントロールを見つけるには

ListCommonControls オペレーションを使用して、使用可能な一般的なコントロールのリストを表示します。オプションの `commonControlFilter` 属性を使用して、特定の目的を持つコントロールのリストを返すこともできます。

API を使用して他のタイプのコントロールを検索するには

ListControls オペレーションを使用して、controlType を `Custom`、`Standard`、または として指定しますCore。

詳細については、前の手順のリンクのいずれかを選択して、 AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

コントロールの詳細を確認する準備ができたら、「」のステップに従いますでのコントロールの確認 AWS Audit Manager。このページでは、コントロールの詳細を説明し、表示される情報について説明します。

コントロールライブラリページから、カスタムコントロール の作成、カスタムコントロール の編集、カスタムコントロール の削除を行うこともできます。

追加リソース

Audit Manager の問題を制御する解決策については、「」を参照してくださいコントロールとコントロールセットの問題のトラブルシューティング。

でのコントロールの確認 AWS Audit Manager

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して、コントロールの詳細を確認できますAWS CLI。

Audit Manager でコントロールの確認を開始するには、ここで概説されている手順に従ってください。

共通コントロールの確認

コントロールの詳細を確認する必要がある場合は、コントロールの詳細ページのいくつかのセクションに情報がまとめられています。これらのセクションは、そのコントロールに関連する情報に簡単にアクセスして理解するのに役立ちます。

前提条件

IAM アイデンティティに、Audit Manager で一般的なコントロールを表示するための適切なアクセス許可があることを確認します。具体的には、 AWS Control Catalog によって提供される一般的なコントロール、コントロール目標、コントロールドメインを表示するには、次のアクセス許可が必要です。

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

これらのアクセス許可を付与する推奨ポリシーは ですAWSAuditManagerAdministratorAccess。

手順

Audit Manager コンソール、Control Catalog API、または AWS Command Line Interface () を使用して、共通の AWS コントロールを確認できますAWS CLI。

Audit Manager console

Audit Manager コンソールで一般的なコントロールの詳細を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Control library] (ライブラリを管理) を選択します。
3. Common を選択すると、 によって提供される一般的なコントロールが表示されます AWS。

4. 一般的なコントロール名を選択して、そのコントロールの詳細を表示します。
5. 以下の情報をリファレンスとして使用して、一般的なコントロールの詳細を確認します。

概要セクション

このセクションでは、一般的なコントロールについて説明します。

証拠ソースタブ

このタブには、次の情報が含まれます。

名前	説明
コアコントロール	これらは、共通のコントロールをサポートするために証拠を収集する中核的なコントロールです。 • この共通コントロールの証拠を収集すると、ここにリストされているすべてのコアコントロールの証拠が自動的に収集されます。これらのコアコントロールのそれぞれが正常に実装されると、共通コントロールの要件を満たしていることを実証するのに役立ちます。 • 各コアコントロールは、事前に定義されたデータソースのグループを使用して、 AWS これらのデータソースに関する証拠を収集します AWS のサービス。つまり、規制や標準が変更され、新しいデータソースが特定されるたびに自動的に更新されます。コアコントロールを選択して、基盤となるデータソースを表示します。

関連する要件タブ

この共通コントロールの証拠を収集すると、同じ証拠が、このタブに記載されている関連する標準コントロールの要件への準拠を示すのに役立ちます。標準コントロールを選択すると、詳細が表示されます。

> **Note**
>
> • 共通コントロールは、標準コントロールへの部分的なコンプライアンスのみを示す証拠を生成する場合があります。標準コントロールへの完全なコンプライアンスを実証するために、追加の証拠が必要になる場合があります。

- 現時点では、関連要件タブには関連する標準コントロールのみが表示されます。共通コントロールは 1 つ以上のカスタムコントロールに関連付けることができますが、これらの関係はこのタブに表示されません。

AWS CLI

で一般的なコントロールの詳細を表示するには AWS CLI

1. list-common-controls コマンドを実行して、使用可能な一般的なコントロールのリストを表示します。このオペレーションを使用すると、オプションの を適用common-control-filterして、特定の目的を持つ一般的なコントロールを表示できます。

```
aws controlcatalog list-common-controls
```

2. レスポンスで、レビューする一般的なコントロールを特定し、その詳細を書き留めます。

AWS Control Catalog API

API を使用して一般的なコントロールの詳細を表示するには

1. ListCommonControls オペレーションを使用して、使用可能な一般的なコントロールのリストを表示します。このオペレーションを使用すると、オプションの を適用commonControlFilterして、特定の目的を持つコントロールのリストを表示できます。
2. レスポンスで、レビューするコントロールを特定し、その詳細を書き留めます。

これらの API オペレーションの詳細については、Control AWS Catalog API リファレンスの「」を参照するには、この手順のリンクを選択してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

目標を表す一般的なコントロールを選択し、それらを構成要素として使用してカスタムコントロールを作成できます。各自動共通コントロールは、Audit Manager が処理する AWS データソースの事前定義されたグループにマッピングされます。つまり、どのデータソースが目標に関連する証拠を収集するかを知るために、 AWS エキスパートである必要はありません。さらに、これらのデータソースマッピングを自分で管理する必要はありません。

一般的なコントロールを証拠ソースとして使用するカスタムコントロールを作成する方法については、「」を参照してくださいでのカスタムコントロールの作成 AWS Audit Manager。

追加リソース

- コアコントロールの確認
- 標準コントロールの確認
- カスタムコントロールの確認

コアコントロールの確認

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して、コアコントロールの詳細を確認できますAWS CLI。

前提条件

IAM アイデンティティに、 でコントロールを表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager console

Audit Manager コンソールでコアコントロールの詳細を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Control library] (ライブラリを管理) を選択します。
3. Common を選択すると、 によって提供される一般的なコントロールが表示されます AWS。
4. ユースケースに合った一般的なコントロールを探します。
5. 一般的なコントロール名の横にあるツリービューアイコンを選択します。これにより、共通コントロールをサポートするコアコントロールが表示されます。
6. 確認するコアコントロールの名前を選択します。
7. 以下の情報をリファレンスとして使用して、コアコントロールの詳細を確認します。

概要セクション

このセクションでは、コアコントロールについて説明し、証拠を収集するデータソースタイプを一覧表示します。

証拠ソースタブ

このタブには、次の情報が含まれます。

名前	説明

データソース	これらは、コアコントロールが証拠を収集する AWS マネージドデータソースです。これらのデータソースは、規制や標準が変更され、新しいデータソースが特定されるたびに自動的に更新されます。
	• マッピング — 証拠の収集に使用される特定のキーワード。
	  • タイプが の場合AWS Config、マッピングは AWS Config ルール (などSNS_ENCRYPTED_KMS) です。
	  • タイプが の場合AWS Security Hub、マッピングは Security Hub コントロール (などEC2.1) です。
	  • タイプが AWS API コールの場合、マッピングは API コール (などkms_ListKeys) です。
	  • タイプが の場合AWS CloudTrail、マッピングは CloudTrail イベント (など) ですCreateAccessKey 。
	• Type – 証拠のソースとなるデータソースのタイプ。
	  • Audit Manager が証拠を収集する場合、タイプは AWS Security Hub、、AWS CloudTrail、または API AWS Configコール です。 AWS
	  • 独自の証拠をアップロードする場合、タイプは手動 です。説明では、必要な手動証拠がファイルアップロードまたはテキスト応答であるかことが示されます。
	• 頻度 — Audit Manager が AWS API コールデータソースの証拠を収集する頻度。

[詳細] タブ

このタブには、次の情報が含まれます。

名前	説明
Instructions	コントロールをテストおよび修正する方法を説明する指示。
テスト情報	推奨されるテスト手順。
アクションプラン	コントロールを修正する必要がある場合に実行する推奨アクション。

AWS CLI

でコアコントロールの詳細を表示するには AWS CLI

1. 手順に従ってコントロール を見つけます。を `--control-type`に設定し`Core`、必要に応じてオプションのフィルターを適用してください。

```
aws auditmanager list-controls --control-type Core
```

2. レスポンスで、レビューするコントロールを特定し、コントロール ID と Amazon リソースネーム (ARN) を書き留めます。
3. get-control コマンドを実行し、 を指定します`--control-id`。次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

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

> **Tip**
>
> コントロールの詳細は JSON 形式で返されます。このデータを理解するには、AWS CLI 「 コマンドリファレンス」の「get-control Output」を参照してください。

4. タグの詳細を表示するには、 list-tags-for-resource コマンドを実行し、 を指定します`--resource-arn`。次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

API を使用してコアコントロールの詳細を表示するには

1. 手順に従ってコントロール を検索します。controlType を に設定しCore、必要に応じてオプションのフィルターを適用してください。
2. レスポンスで、レビューするコントロールを特定し、コントロール ID と Amazon リソースネーム (ARN) を書き留めます。
3. GetControl オペレーションを使用して、ステップ 2 でメモした controlId を指定します。

   > **Tip**
   >
   > コントロールの詳細は JSON 形式で返されます。このデータを理解するには、AWS Audit Manager 「 API リファレンス」のGetControl 「レスポンス要素」を参照してください。

4. タグの詳細を表示するには、 ListTagsForResourceオペレーションを使用して、ステップ 2 でメモした resourceArn を指定します。

これらの API オペレーションの詳細については、この手順のリンクのいずれかを選択して、AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

目標を表すコアコントロールを選択し、それらを構成要素として使用してカスタムコントロールを作成できます。各自動コアコントロールは、Audit Manager が処理する AWS データソースの事前定義されたグループにマッピングされます。つまり、どのデータソースが目標に関連する証拠を収集するかを知るために、 AWS エキスパートである必要はありません。さらに、これらのデータソースマッピングを自分で管理する必要はありません。

コアコントロールを証拠ソースとして使用するカスタムコントロールを作成する方法については、「」を参照してくださいでのカスタムコントロールの作成 AWS Audit Manager。

追加リソース

- 共通コントロールの確認
- 標準コントロールの確認
- カスタムコントロールの確認

標準コントロールの確認

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して、標準コントロールの詳細を確認できますAWS CLI。

前提条件

IAM アイデンティティに、 でコントロールを表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して、標準コントロールの詳細を確認できますAWS CLI。

Audit Manager console

Audit Manager コンソールで標準コントロールの詳細を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Control library] (ライブラリを管理) を選択します。
3. 標準 を選択して、 が提供する標準コントロールを表示します AWS。
4. 標準コントロール名を選択して、そのコントロールの詳細を表示します。
5. 以下の情報をリファレンスとして使用して、標準コントロールの詳細を確認します。

概要セクション

このセクションでは、標準コントロールについて説明し、証拠の収集に使用するデータソースタイプを一覧表示します。

証拠ソースタブ

このタブには、次の情報が含まれます。

名前	説明
コアコントロール	これらは、標準コントロールをサポートするために証拠を収集するコアコントロールです。 各コアコントロールは、事前に定義されたデータソースのグループを使用して、 に関する証拠を収集します AWS のサービス。これらのデータソースは によって管理され AWS、規制や標準が変更され、新しいデータソースが特定されるたびに自動的に更新されます。コアコントロールを選択して、基盤となるデータソースを表示します。

データソース	これらは、標準コントロールをサポートするために証拠を収集する他の AWS マネージドデータソースです。
	• マッピング — 証拠の収集に使用される特定のキーワード。
	  • タイプが の場合AWS Config、マッピングは AWS Config ルール (などSNS_ENCRYPTED_KMS) です。
	  • タイプが の場合AWS Security Hub、マッピングは Security Hub コントロール (など) ですEC2.1。
	  • タイプが AWS API コールの場合、マッピングは API コール (などkms_ListKeys) です。
	  • タイプが の場合AWS CloudTrail、マッピングは CloudTrail イベント (など) ですCreateAccessKey 。
	• Type – 証拠のソースとなるデータソースのタイプ。
	  • Audit Manager が証拠を収集する場合、タイプは AWS Security Hub、、AWS CloudTrail、または API AWS Configコール です。 AWS

名前	説明
	• 独自の証拠をアップロードする場合、タイプは手動 です。説明では、必要な手動証拠がファイルアップロード またはテキスト応答であるかことが示されます。 • 頻度 — Audit Manager が AWS API コールデータソースの証拠を収集する頻度。

[詳細] タブ

このタブには、次の情報が含まれます。

名前	説明
Instructions	コントロールをテストおよび修正する方法を説明する指示。
テスト情報	推奨されるテスト手順。
アクションプラン	コントロールを修正する必要がある場合に実行する推奨アクション。
タグ	コントロールに関連付けられているタグ。
キー	タグキー (コンプライアンス標準、規制、カテゴリなど) 。
値	タグ値。

AWS CLI

で標準コントロールの詳細を表示するには AWS CLI

1. 手順に従ってコントロール を見つけます。を `--control-type`に設定し`Standard`、必要に応じてオプションのフィルターを適用してください。

```
aws auditmanager list-controls --control-type Standard
```

2. レスポンスで、確認するコントロールを特定し、コントロール ID と Amazon リソースネーム (ARN) を書き留めます。

3. get-control コマンドを実行し、 を指定します--control-id。次の例では、次の *placeholder text* を独自の情報に置き換えます。

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

> **Tip**
>
> コントロールの詳細は JSON 形式で返されます。このデータを理解するには、 AWS CLI コマンドリファレンスの「get-control Output」を参照してください。

4. タグの詳細を表示するには、 list-tags-for-resource コマンドを実行し、 を指定します--resource-arn。次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

API を使用して標準コントロールの詳細を表示するには

1. 手順に従ってコントロール を見つけます。controlType を に設定しStandard、必要に応じてオプションのフィルターを適用してください。
2. レスポンスで、確認するコントロールを特定し、コントロール ID と Amazon リソースネーム (ARN) を書き留めます。
3. GetControl オペレーションを使用して、ステップ 2 でメモした controlId を指定します。

> **Tip**
>
> コントロールの詳細は JSON 形式で返されます。このデータを理解するには、AWS Audit Manager 「 API リファレンス」のGetControl 「レスポンス要素」を参照してください。

4. タグの詳細を表示するには、 ListTagsForResourceオペレーションを使用して、ステップ 2 でメモした resourceArn を指定します。

これらの API オペレーションの詳細については、この手順のリンクのいずれかを選択して、AWS Audit Manager 「 API リファレンス」で詳細を確認してください。これには、言語固有の AWS

SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

任意のカスタムフレームワークに標準コントロールを追加できます。手順については、「でのカスタムフレームワークの作成 AWS Audit Manager」を参照してください。

標準コントロールをカスタマイズして、ニーズを満たすこともできます。手順については、「でコントロールの編集可能なコピーを作成する AWS Audit Manager」を参照してください。

追加リソース

- 共通コントロールの確認
- コアコントロールの確認
- カスタムコントロールの確認

カスタムコントロールの確認

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して、カスタムコントロールの詳細を確認できますAWS CLI。

前提条件

IAM アイデンティティに、 でコントロールを表示するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用して、カスタムコントロールの詳細を確認できますAWS CLI。

Audit Manager console

Audit Manager コンソールでカスタムコントロールの詳細を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Control library] (ライブラリを管理) を選択します。
3. カスタム を選択して、作成したカスタムコントロールを表示します。
4. カスタムコントロール名を選択して、そのコントロールの詳細を表示します。
5. 次の情報をリファレンスとして使用して、カスタムコントロールの詳細を確認します。

概要セクション

このセクションでは、カスタムコントロールについて説明し、証拠の収集に使用するデータソースタイプを一覧表示します。また、コントロールがいつ作成され、最後に更新されたかに関する情報も提供します。

証拠ソースタブ

このタブには、カスタムコントロールが証拠を収集する場所が表示されます。次の情報が含まれています。

名前	説明
一般的なコントロール	これらは、カスタムコントロールをサポートするために証拠を収集する一般的なコントロールです。 一般的なコントロールは、 が AWS 管理する基盤となるデータソースを使用して証拠を収集します。リストされているすべての一般的なコントロールについて、Audit Manager は、サポートされているすべてのコアコントロールに関連する証拠を収集します。共通コントロールを選択すると、関連するコアコントロールが表示されます。
コアコントロール	これらは、カスタムコントロールをサポートするために証拠を収集するコアコントロールです。 コアコントロールは、 が AWS 管理する定義済みのデータソースグループを使用して証拠を収集します。コアコント

名前	説明
	ロールを選択すると、基盤となるデータソースが表示されます。

データソース	これらは、カスタムコントロールをサポートするために証拠を収集するデータソースです。
	
	Note
	これらのデータソースは によって管理されません AWS。ユーザーはそれらを維持する責任があります。
	
	• 名前 – データソースの名前。
	• Type – 証拠のソースとなるデータソースのタイプ。
	  • Audit Manager が証拠を収集する場合、タイプは AWS Security Hub、、AWS CloudTrail、または API AWS Configコール です。 AWS
	  • 独自の証拠をアップロードする場合、タイプは手動 です。説明では、必要な手動証拠がファイルアップロードまたはテキスト応答であるかことが示されます。
	• マッピング — 証拠の収集に使用される特定のキーワード。
	  • タイプが の場合AWS Config、マッピングは AWS Config ルール (などSNS_ENCRYPTED_KMS) です。
	  • タイプが の場合AWS Security Hub、マッピングは Security Hub コントロール (などEC2.1) です。
	  • タイプが AWS API コールの場合、マッピングは API コール (などkms_ListKeys) です。
	  • タイプが の場合AWS CloudTrail、マッピングは CloudTrail イベント (などCreateAccessKey) です。
	• 頻度 — Audit Manager が AWS API コールデータソースの証拠を収集する頻度。

[詳細] タブ

このタブには、次の情報が含まれます。

名前	説明
Instructions	コントロールをテストおよび修正する方法を説明する指示。
テスト情報	推奨されるテスト手順。
アクションプラン	コントロールを修正する必要がある場合に実行する推奨アクション。
タグ	コントロールに関連付けられているタグ。
キー	タグキー (コンプライアンス標準、規制、カテゴリなど) 。
値	タグ値。

AWS CLI

でカスタムコントロールの詳細を表示するには AWS CLI

1. 手順に従ってコントロール を検索します。を `--control-type`に設定し`Custom`、必要に応じてオプションのフィルターを適用してください。

```
aws auditmanager list-controls --control-type Custom
```

2. レスポンスで、確認するコントロールを特定し、コントロール ID と Amazon リソースネーム (ARN) を書き留めます。
3. get-control コマンドを実行し、 を指定します`--control-id`。次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

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

> **Tip**
>
> コントロールの詳細は JSON 形式で返されます。このデータを理解するには、AWS CLI 「 コマンドリファレンス」の「get-control Output」を参照してください。

4. コントロールのタグを表示するには、 list-tags-for-resource コマンドを使用して を指定します--resource-arn。次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

API を使用してカスタムコントロールの詳細を表示するには

1. 手順に従ってコントロール を検索します。controlType を に設定しCustom、必要に応じてオプションのフィルターを適用してください。
2. レスポンスで、レビューするコントロールを特定し、コントロール ID とその Amazon リソースネーム (ARN) を書き留めます。
3. GetControl オペレーションを使用して、ステップ 2 でメモした controlId を指定します。

> **Tip**
>
> コントロールの詳細は JSON 形式で返されます。このデータを理解するには、AWS Audit Manager 「 API リファレンス」のGetControl 「レスポンス要素」を参照してください。

4. コントロールのタグを表示するには、 ListTagsForResourceオペレーションを使用して、ステップ 2 でメモしたコントロール resourceArn を指定します。

これらの API オペレーションの詳細については、この手順のリンクのいずれかを選択して、AWS Audit Manager API リファレンス で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

任意のカスタムフレームワークにカスタムコントロールを追加できます。手順については、「でのカスタムフレームワークの作成 AWS Audit Manager」を参照してください。

カスタムコントロール の編集、カスタムコントロール の編集可能なコピーの作成、不要になったカスタムコントロールの削除を行うこともできます。

追加リソース

- 共通コントロールの確認
- コアコントロールの確認
- 標準コントロールの確認

でのカスタムコントロールの作成 AWS Audit Manager

カスタムコントロールを使用して、特定のコンプライアンスニーズに関する証拠を収集できます。

標準コントロールと同様に、カスタムコントロールは評価で有効になっている間は継続的に証拠を収集します。また、作成したカスタムコントロールには手動証拠を追加できます。証拠はそれぞれ、カスタムコントロールの要件への準拠を実証するのに役立つ記録になります。

まず、カスタムコントロールの使用方法の例をいくつか示します。

エンタープライズコントロールをデータソースの AWS 事前定義されたグループにマッピングする

一般的なコントロールを証拠ソースとして使用することで、エンタープライズコントロールを Audit Manager にオンボードできます。目標を表す一般的なコントロールを選択し、それらを構成要素として使用して、コンプライアンスニーズのポートフォリオ全体で証拠を収集するコントロールを作成します。各自動化された共通コントロールは、データソースの事前定義されたグループにマッピングされます。つまり、どのデータソースが目標に関連する証拠を収集するかを知るために、 AWS エキスパートである必要はありません。また、一般的なコントロールを証拠ソースとして使用すると、Audit Manager がこれを処理するため、データソースマッピングを維持する必要がなくなります。

ベンダーリスク評価用の質問を作成する

カスタムコントロールを使用して、ベンダーリスク評価の管理方法をサポートすることができます。作成した各コントロールで、個々のリスク評価に関する質問を表すことができます。例え

ば、コントロール名は質問にすることができます。また、ファイルをアップロードしたり、手動証拠としてテキストレスポンスを入力したりして、回答を提供できます。

重要ポイント

Audit Manager でカスタムコントロールを作成する場合、次の 2 つの方法から選択できます。

1. 最初からコントロールを作成する - この方法では、最大限の柔軟性が得られ、正確なニーズに合わせてコントロールを調整できます。これは、既存のコントロールで適切にカバーされていない特定のコンプライアンス要件がある場合に適しています。この方法は、組織のエンタープライズコントロールをデータソースの AWS 事前定義されたグループにマッピングする必要がある場合や、ベンダーリスク評価の質問を個々のコントロールとして作成する場合に特に便利です。
2. 既存のコントロールの編集可能なコピーの作成 - 既存の標準コントロールまたはカスタムコントロールが部分的にニーズを満たしている場合は、そのコントロールの編集可能なコピーを作成できます。このアプローチは、既存のコントロールにわずかな変更を加えるだけで済む場合、より効率的です。これは、コントロールを特定の要件に合わせて調整する場合に適しています。例えば、コントロールが API コールを使用して証拠を収集する頻度を変更し、それを反映するようにコントロールの名前を変更することができます。

追加リソース

カスタムコントロールを作成する方法については、以下のリソースを参照してください。

- でゼロからカスタムコントロールを作成する AWS Audit Manager
- でコントロールの編集可能なコピーを作成する AWS Audit Manager

でゼロからカスタムコントロールを作成する AWS Audit Manager

組織のコンプライアンス要件が、 で利用可能な構築済みの標準コントロールと一致しない場合は AWS Audit Manager、独自のカスタムコントロールをゼロから作成できます。

このページでは、特定のニーズに合わせてカスタムコントロールを作成する手順の概要を説明します。

前提条件

IAM アイデンティティに、 でカスタムコントロールを作成するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

AWS Config と Security Hub から証拠を正常に収集するには、次の操作を行います。

- を有効にし AWS Config、Audit Manager AWS Config で を使用するために必要な設定を適用します。
- Security Hub を有効にし、Audit Manager で Security Hub を使用するために必要な設定を適用する

Audit Manager は、特定の AWS Config ルールまたは Security Hub コントロールの評価が行われるたびに証拠を収集できます。

手順

タスク

- ステップ 1: コントロールの詳細を指定する
- ステップ 2: 証拠ソースを指定する
- ステップ 3 (オプション): アクションプランを定義する
- ステップ 4: コントロールを確認および作成する

ステップ 1: コントロールの詳細を指定する

カスタムコントロールの詳細を指定することから開始します。

> **Important**
>
> 機密性の高い識別情報を、コントロールの詳細やテスト情報などの自由形式のフィールドに決して入力しないことを強くお勧めします。機密情報を含むカスタムコントロールを作成する場合、これらのコントロールを含むカスタムフレームワークを共有することはできません。

コントロールの詳細を指定するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[コントロールライブラリ] を選択し、[カスタムコントロールを作成] を選択します。
3. [コントロールの詳細] に、コントロールに関する次の情報を入力します。
   - [コントロール] — わかりやすい名前、タイトル、またはリスク評価に関する質問を入力します。この値は、コントロールライブラリ内のコントロールを識別するのに役立ちます。
   - [説明 (オプション)] — 他のユーザーがコントロールの目的を理解しやすいように詳細を入力します。この説明は、コントロールの詳細のページに表示されます。
4. [テスト情報] で、コントロールテストの推奨手順を入力します。
5. [タグ] で、[新しいタグを追加] を選択して、タグをコントロールに関連付けます。このコントロールがサポートするコンプライアンスフレームワークを最もよく表す各タグについてキーを指定できます。タグキーは必須であり、コントロールライブラリでこのコントロールを検索するときに検索条件として使用できます。
6. [次へ] をクリックします。

ステップ 2: 証拠ソースを指定する

次に、いくつかの証拠ソースを指定します。証拠ソースは、カスタムコントロールが証拠を収集する場所を決定します。 AWS マネージドソース、カスタマーマネージドソース、またはその両方を使用できます。

> **Tip**
>
> AWS マネージドソースを使用することをお勧めします。 AWS マネージドソースが更新されるたびに、これらのソースを使用するすべてのカスタムコントロールに同じ更新が自動的に適用されます。つまり、カスタムコントロールは、その証拠ソースの最新の定義に照らして証拠を収集します。

どのオプションを選択するかわからない場合は、以下の例と推奨事項を参照してください。

役割	目標	推奨される証拠ソース
GRC プロフェッショナル	特定のドメインまたは目標に関する証拠を収集したい	AWS マネージド (common control) 特定の共通コントロールにマッピングするデータソースの事前定義されたグループを使用します。
技術エキスパート	自分が担当する AWS リソースに関する証拠を収集したい	AWS マネージド (core control) 要件にマッピングするデータソースの事前定義されたグループを使用します AWS 。
技術エキスパート	カスタム AWS Config ルールを使用して証拠を収集する	カスタマー管理 (自動 data source) カスタムデータソースを使用して、特定の自動証拠を収集します。
GRC プロフェッショナル	ドキュメントやテキストレスポンスなどの証拠を収集したい	カスタマー管理 (手動 data source) カスタムデータソースを使用して、独自の手動証拠をアップロードします。

マネージドソースを指定する AWS には (推奨)

まず、1 つ以上の一般的なコントロールを選択することをお勧めします。目標を表す共通コントロールを選択すると、Audit Manager は、サポートしているすべてのコアコントロールに関連する証拠を収集します。 AWS 環境に関するターゲットを絞った証拠を収集する場合は、個々のコアコントロールを選択することもできます。

AWS マネージドソースを指定するには

1. ページのAWS マネージドソースセクションに移動します。
2. 共通コントロールを追加するには、次の手順に従います。
   a. 「コンプライアンス目標 に一致する共通のコントロールを使用する」を選択します。
   b. ドロップダウンリストから共通のコントロールを選択します。
   c. (オプション) 必要に応じてステップ 2 を繰り返します。最大 5 つの共通コントロールを追加できます。
3. 共通コントロールを削除するには、コントロール名の横にある X を選択します。
4. コアコントロールを追加するには、次の手順に従います。
   a. 「規範的なガイドライン」に一致するコアコントロールを使用する AWS 」を選択します。
   b. ドロップダウンリストから共通のコントロールを選択します。
   c. (オプション) 必要に応じてステップ 4 を繰り返します。最大 50 個のコアコントロールを追加できます。
5. コアコントロールを削除するには、コントロール名の横にある X を選択します。
6. カスタマーマネージドデータソースを追加するには、次の手順を使用します。それ以外の場合は、次へ を選択します。

カスタマーマネージドソースを指定するには

データソースから自動証拠を収集するには、データソースタイプとデータソースマッピングを選択する必要があります。これらの詳細は AWS 使用状況にマッピングされ、証拠の収集元を Audit Manager に伝えます。独自の証拠を提供する場合は、代わりに手動データソースを選択します。

> **Note**
>
> このステップで作成するデータソースマッピングは、ユーザーが管理する必要があります。

カスタマーマネージドソースを指定するには

1. ページの「カスタマーマネージドソース」セクションに移動します。
2. データソースを使用して手動または自動の証拠を収集する を選択します。
3. 追加を選択します。

4. 以下のオプションのいずれかを選択します。

   - AWS API コール を選択し、API コールと証拠収集の頻度を選択します。
   - AWS CloudTrail イベント を選択し、イベント名を選択します。
   - AWS Config マネージドルール を選択し、ルール識別子を選択します。
   - AWS Config カスタムルール を選択し、ルール識別子を選択します。
   - AWS Security Hub コントロール を選択し、Security Hub コントロールを選択します。
   - 手動データソース を選択し、オプションを選択します。
     - ファイルのアップロード — コントロールで証拠としてドキュメントが必要な場合は、このオプションを使用します。
     - テキストレスポンス — コントロールがリスク評価の質問に対する回答を必要とする場合は、このオプションを使用します。

   > **Tip**
   >
   > 自動データソースタイプとトラブルシューティングのヒントについては、「」を参照してください自動証拠でサポートされているデータソースタイプ。
   > エキスパートとデータソースの設定を検証する必要がある場合は、現時点では手動データソースを選択します。そうすれば、今すぐコントロールを作成してフレームワークに追加し、後日必要に応じてコントロールを編集できます。

5. データソース名 で、わかりやすい名前を指定します。
6. (オプション) [その他の詳細] に、データソースの説明とトラブルシューティングの説明を入力します。
7. [データソースを追加する] を選択する。
8. (オプション) 別のデータソースを追加するには、「追加」を選択し、ステップ 1 ~ 7 を繰り返します。最大 100 個のデータソースを追加できます。
9. データソースを削除するには、テーブルからデータソースを選択し、 の削除を選択します。
10. 完了したら、[Next (次へ)] を選択します。

ステップ 3 (オプション): アクションプランを定義する

次に、このコントロールを修正する必要がある場合に実行するアクションを指定します。

> **Important**
>
> アクションプラン などの自由形式のフィールドに機密の識別情報を配置しないことを強くお勧めします。機密情報を含むカスタムコントロールを作成する場合、これらのコントロールを含むカスタムフレームワークを共有することはできません。

アクションプランを定義するには

1. [Title] (タイトル) で、アクションプランについてのわかりやすいタイトルを入力します。
2. 手順 に、アクションプランの詳細な手順を入力します。
3. [次へ] をクリックします。

ステップ 4: コントロールを確認および作成する

コントロールに関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。

完了したら、[カスタムコントロールを作成]を選択します。

次のステップ

新しいカスタムコントロールを作成したら、それをカスタムフレームワークに追加できます。詳細については、「でのカスタムフレームワークの作成 AWS Audit Manager」または「でのカスタムフレームワークの編集 AWS Audit Manager」を参照してください。

カスタムフレームワークにカスタムコントロールを追加したら、評価を作成して証拠の収集を開始できます。詳細については、「での評価の作成 AWS Audit Manager」を参照してください。

後でカスタムコントロールを再確認するには、「」を参照してくださいで使用可能なコントロールの検索 AWS Audit Manager。カスタムコントロールを表示、編集、または削除できるように、これらの手順に従ってカスタムコントロールを見つけることができます。

追加リソース

Audit Manager の問題を制御する解決策については、「」を参照してくださいコントロールとコントロールセットの問題のトラブルシューティング。

でコントロールの編集可能なコピーを作成する AWS Audit Manager

カスタムコントロールをゼロから作成する代わりに、既存の標準コントロールまたはカスタムコントロールを開始点として使用し、ニーズを満たす編集可能なコピーを作成できます。これを行うと、既存の標準コントロールはコントロールライブラリに残り、カスタム設定で新しいコントロールが作成されます。

前提条件

IAM アイデンティティに、 でカスタムフレームワークを作成するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

AWS Config と Security Hub から証拠を正常に収集するには、次の操作を行います。

- を有効にし AWS Config、Audit Manager AWS Config で を使用するために必要な設定を適用します。
- Security Hub を有効にし、Audit Manager で Security Hub を使用するために必要な設定を適用します。

Audit Manager は、特定の AWS Config ルールまたは Security Hub コントロールの評価が行われるたびに証拠を収集できます。

手順

タスク

- ステップ 1: コントロールの詳細を指定する
- ステップ 2: 証拠ソースを指定する
- ステップ 3: (オプション): アクションプランを定義する
- ステップ 4: コントロールを確認および作成する

ステップ 1: コントロールの詳細を指定する

コントロールの詳細は元のコントロールから引き継がれます。必要に応じて、これらの詳細を確認して変更します。

> **Important**
>
> 機密性の高い識別情報を、コントロールの詳細やテスト情報などの自由形式のフィールドに入れないことを強くお勧めします。機密情報を含むカスタムコントロールを作成する場合、これらのコントロールを含むカスタムフレームワークを共有することはできません。

コントロールの詳細を指定するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Control library] (ライブラリを管理) を選択します。
3. 変更する標準コントロールまたはカスタムコントロールを選択し、コピー を選択します。
4. コントロールの新しい名前を指定し、続行 を選択します。
5. [コントロールの詳細] で、必要に応じてコントロールの詳細をカスタマイズします。
6. テスト情報 で、必要に応じて手順を変更します。
7. [タグ] で、必要に応じてタグをカスタマイズします。
8. [次へ] をクリックします。

ステップ 2: 証拠ソースを指定する

証拠ソースは元のコントロールから継承されます。必要に応じて、証拠ソースを変更、追加、または削除できます。

マネージドソースを指定する AWS には (推奨)

> **Tip**
>
> まず、1 つ以上の一般的なコントロールを選択することをお勧めします。よりきめ細かなコンプライアンス要件がある場合は、1 つ以上の特定のコアコントロールを選択することもできます。

AWS マネージドソースを指定するには

1. AWS マネージドソース で、現在の選択内容を確認し、必要に応じて変更を加えます。
2. 共通コントロールを追加するには、次の手順に従います。

a. 「コンプライアンス目標 に一致する共通のコントロールを使用する」を選択します。
b. ドロップダウンリストから共通のコントロールを選択します。
c. (オプション) 必要に応じてステップ 2 を繰り返します。最大 5 つの共通コントロールを追加できます。

3. 共通コントロールを削除するには、コントロール名の横にある X を選択します。
4. コアコントロールを追加するには、次の手順に従います。

a. 「規範的なガイドライン」に一致するコアコントロールを使用する AWS 」を選択します。
b. ドロップダウンリストから共通のコントロールを選択します。
c. (オプション) 必要に応じてステップ 4 を繰り返します。最大 50 個のコアコントロールを追加できます。

5. コアコントロールを削除するには、コントロール名の横にある X を選択します。
6. カスタマー管理のデータソースを編集するには、次の手順を使用します。それ以外の場合は、次へ を選択します。

カスタマーマネージドソースを指定するには

データソースから自動証拠を収集するには、データソースタイプとデータソースマッピングを選択する必要があります。これらの詳細は AWS 使用状況にマッピングされ、証拠の収集元を Audit Manager に伝えます。独自の証拠を提供する場合は、代わりに手動データソースを選択します。

> **Note**
>
> このステップで作成するデータソースマッピングは、ユーザーが管理する必要があります。

カスタマーマネージドソースを指定するには

1. 「カスタマーマネージドソース」で、現在のデータソースを確認し、必要に応じて変更を加えます。
2. データソースを削除するには、テーブルからデータソースを選択し、 の削除を選択します。
3. 新しいデータソースを追加するには、次の手順に従います。

a. データソースを使用して手動または自動の証拠を収集する を選択します。
b. 追加を選択します。

c. 以下のオプションのいずれかを選択します。

- AWS API コール を選択し、API コールと証拠収集の頻度を選択します。
- AWS CloudTrail イベント を選択し、イベント名を選択します。
- AWS Config マネージドルール を選択し、ルール識別子を選択します。
- AWS Config カスタムルール を選択し、ルール識別子を選択します。
- AWS Security Hub コントロール を選択し、Security Hub コントロールを選択します。
- 手動データソース を選択し、オプションを選択します。
  - ファイルのアップロード — コントロールで証拠としてドキュメントが必要な場合は、このオプションを使用します。
  - テキストレスポンス — コントロールがリスク評価の質問に対する回答を必要とする場合は、このオプションを使用します。

> **Tip**
>
> 自動データソースタイプとトラブルシューティングのヒントについては、「」を参照してください自動証拠でサポートされているデータソースタイプ。
> エキスパートとデータソースの設定を検証する必要がある場合は、現時点では手動データソースを選択してください。そうすれば、今すぐコントロールを作成してフレームワークに追加し、後日必要に応じてコントロールを編集できます。

d. データソース名 で、わかりやすい名前を指定します。

e. (オプション) [その他の詳細] に、データソースの説明とトラブルシューティングの説明を入力します。

f. [データソースを追加する] を選択する。

g. (オプション) 別のデータソースを追加するには、追加を選択してステップ 3 を繰り返します。最大 100 個のデータソースを追加できます。

4. 完了したら、[Next (次へ)] を選択します。

ステップ 3: (オプション): アクションプランを定義する

アクションプランは元のコントロールから引き継がれます。このアクションプランは必要に応じて編集できます。

> **Important**
>
> 機密性の高い識別情報をアクションプラン などの自由形式のフィールドに入力しないことを強くお勧めします。機密情報を含むカスタムコントロールを作成する場合、これらのコントロールを含むカスタムフレームワークを共有することはできません。

手順を指定するには

1. タイトル で、タイトルを確認し、必要に応じて変更を加えます。
2. 手順 で、手順を確認し、必要に応じて変更を加えます。
3. [次へ] をクリックします。

ステップ 4: コントロールを確認および作成する

コントロールに関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。完了したら、[カスタムコントロールを作成]を選択します。

次のステップ

新しいカスタムコントロールを作成したら、それをカスタムフレームワークに追加できます。詳細については、「でのカスタムフレームワークの作成 AWS Audit Manager」または「でのカスタムフレームワークの編集 AWS Audit Manager」を参照してください。

カスタムフレームワークにカスタムコントロールを追加したら、評価を作成して証拠の収集を開始できます。詳細については、「での評価の作成 AWS Audit Manager」を参照してください。

後でカスタムコントロールを再確認するには、「」を参照してくださいで使用可能なコントロールの検索 AWS Audit Manager。カスタムコントロールを表示、編集、または削除できるように、これらの手順に従ってカスタムコントロールを見つけることができます。

追加リソース

Audit Manager の問題を制御する解決策については、「」を参照してくださいコントロールとコントロールセットの問題のトラブルシューティング。

でのカスタムコントロールの編集 AWS Audit Manager

コンプライアンス要件の変化 AWS Audit Manager に応じて、 でカスタムコントロールを変更する必要がある場合があります。

このページでは、カスタムコントロールの詳細、証拠ソース、およびアクションプランの手順を編集する手順の概要を説明します。

前提条件

次の手順では、カスタムコントロールを以前に作成したことを前提としています。

IAM アイデンティティに、 でカスタムコントロールを編集するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

カスタムコントロールを編集するには、次の手順に従います。

> **Note**
>
> コントロールを編集すると、コントロールがアクティブなすべての評価に変更が適用されます。これらのすべての評価で、Audit Manager は最新のコントロール定義に従って証拠の収集を自動的に開始します。

タスク

- ステップ 1: コントロールの詳細を編集する
- ステップ 2: 証拠ソースを編集する
- ステップ 3: アクションプランを編集する

ステップ 1: コントロールの詳細を編集する

必要に応じて、コントロールの詳細を確認して編集します。

> **Important**
>
> コントロールの詳細やテスト情報 などの自由形式のフィールドに機密の識別情報を入力しないことを強くお勧めします。機密情報を含むカスタムコントロールを作成する場合、これらのコントロールを含むカスタムフレームワークを共有することはできません。

コントロールの詳細を編集するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、コントロールライブラリを選択し、カスタムタブを選択します。
3. 編集するコントロールを選択したら、[Edit] (編集) を選択します。
4. [コントロールの詳細] で、必要に応じてコントロールの詳細を編集します。
5. テスト情報 で、必要に応じて説明を編集します。
6. [次へ] をクリックします。

ステップ 2: 証拠ソースを編集する

次に、コントロールの証拠ソースを編集、削除、または追加できます。

> **Note**
>
> コントロールを編集して証拠ソースを増減すると、コントロールがアクティブな評価で収集する証拠の量に影響する可能性があります。例えば、証拠ソースを追加すると、Audit Manager が以前よりも多くのリソース評価を実行し、より多くの証拠を収集していることに気付くかもしれません。証拠ソースを削除すると、コントロールが今後収集する証拠が少なくなる可能性があります。
> リソースの評価と料金の詳細については、AWS Audit Manager 「 の料金」を参照してください。

AWS マネージドソースを編集するには

AWS マネージドソースを編集するには

1. AWS マネージドソース で、現在の選択内容を確認し、必要に応じて変更を加えます。

2. 共通コントロールを追加するには、次の手順に従います。

    a. 「コンプライアンス目標 に一致する共通のコントロールを使用する」を選択します。

    b. ドロップダウンリストから共通のコントロールを選択します。

    c. (オプション) 必要に応じてステップ 2 を繰り返します。最大 5 つの共通コントロールを追加できます。

3. 共通コントロールを削除するには、コントロール名の横にある X を選択します。

4. コアコントロールを追加するには、次の手順に従います。

    a. 「規範的なガイドライン」に一致するコアコントロールを使用する AWS 」を選択します。

    b. ドロップダウンリストから共通のコントロールを選択します。

    c. (オプション) 必要に応じてステップ 4 を繰り返します。最大 50 個のコアコントロールを追加できます。

5. コアコントロールを削除するには、コントロール名の横にある X を選択します。

6. カスタマーマネージドデータソースを追加するには、次の手順を使用します。それ以外の場合は、次へ を選択します。

カスタマーマネージドソースを編集するには

> **Note**
>
> このステップで編集するデータソースマッピングは、ユーザーが管理する必要があります。

カスタマーマネージドソースを編集するには

1. 「カスタマーマネージドソース」で、現在のデータソースを確認し、必要に応じて変更を加えます。

2. データソースを削除するには、テーブルからデータソースを選択し、 の削除を選択します。

3. 新しいデータソースを追加するには、次の手順に従います。

    a. データソースを使用して手動または自動の証拠を収集する を選択します。

    b. 追加を選択します。

    c. 以下のオプションのいずれかを選択します。

        - AWS API コール を選択し、API コールと証拠収集の頻度を選択します。

- AWS CloudTrail イベント を選択し、イベント名を選択します。
- AWS Config マネージドルール を選択し、ルール識別子を選択します。
- AWS Config カスタムルール を選択し、ルール識別子を選択します。
- AWS Security Hub コントロール を選択し、Security Hub コントロールを選択します。
- 手動データソース を選択し、オプションを選択します。
  - ファイルのアップロード — コントロールで証拠としてドキュメントが必要な場合は、このオプションを使用します。
  - テキストレスポンス — コントロールがリスク評価の質問に対する回答を必要とする場合は、このオプションを使用します。

> **Tip**
>
> 自動データソースタイプとトラブルシューティングのヒントについては、「」を参照してください自動証拠でサポートされているデータソースタイプ。
> エキスパートとデータソースの設定を検証する必要がある場合は、現時点では手動データソースを選択します。そうすれば、今すぐコントロールを作成してフレームワークに追加し、後日必要に応じてコントロールを編集できます。

d. データソース名 で、わかりやすい名前を指定します。

e. (オプション) [その他の詳細] に、データソースの説明とトラブルシューティングの説明を入力します。

f. [データソースを追加する] を選択する。

g. （ オプション) 別のデータソースを追加するには、追加を選択してステップ 3 を繰り返します。最大 100 個のデータソースを追加できます。

4. 完了したら、[Next (次へ)] を選択します。

ステップ 3: アクションプランを編集する

次に、オプションのアクションプランを確認および編集します。

> **Important**
>
> 機密性の高い識別情報をアクションプラン などの自由形式のフィールドに入力しないことを強くお勧めします。機密情報を含むカスタムコントロールを作成する場合、これらのコントロールを含むカスタムフレームワークを共有することはできません。

アクションプランを編集するには

1. [Title] (タイトル) で、必要に応じてタイトルを編集します。
2. 手順 で、必要に応じて手順を編集します。
3. [次へ] をクリックします。

ステップ 4: 確認して保存する

コントロールに関する情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。

完了したら、[変更の保存] を選択します。

> **Note**
>
> コントロールを編集すると、そのコントロールを含むすべてのアクティブな評価で次のように変更が有効になります。
>
> - AWS API コールをデータソースタイプとするコントロールについては、変更は翌日の 00:00 (UTC) に有効になります。
> - 他のすべてのコントロールについては、変更はすぐに反映されます。

次のステップ

カスタムコントロールが不要になったことを確認したら、コントロールを削除して Audit Manager 環境をクリーンアップできます。手順については、「でのカスタムコントロールの削除 AWS Audit Manager」を参照してください。

追加リソース

Audit Manager の問題を制御する解決策については、「」を参照してくださいコントロールとコントロールセットの問題のトラブルシューティング。

コントロールが証拠を収集する頻度の変更

AWS Audit Manager は、さまざまなデータソースから証拠を収集できます。証拠収集の頻度は、コントロールが使用するデータソースのタイプによって異なります。

次のセクションでは、各コントロールのデータソースについての証拠収集の頻度と、その変更方法 (該当する場合) について詳しく説明します。

トピック

重要ポイント

- AWS [API コール] については、Audit Manager は、別の AWS のサービスに describe API コールを使用して証拠を収集します。証拠収集の頻度は、Audit Manager で直接指定できます (カスタムコントロールの場合のみ)。
- の場合AWS Config、Audit Manager はコンプライアンスチェックの結果を から直接報告します AWS Config。頻度は、 AWS Config ルールで定義されているトリガーに従います。
- AWS Security Hubの場合、Audit Manager は Security Hub から直接コンプライアンスチェックの結果をレポートします。その頻度は、Security Hub チェックのスケジュールに従います。
- の場合AWS CloudTrail、Audit Manager は から継続的に証拠を収集します CloudTrail。この証拠タイプの頻度は変更できません。

AWS API コールからの設定スナップショット

> **Note**
>
> 以下の記載内容は、カスタムコントロールにのみ適用されます。標準コントロールの証拠収集の頻度を変更することはできません。

カスタムコントロールがデータソースタイプとして AWS API コールを使用している場合は、以下の手順に従って Audit Manager で証拠収集の頻度を変更できます。

API コールのデータソースを使用したカスタムコントロールについての証拠収集の頻度を変更するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、コントロールライブラリ を選択し、カスタムタブを選択します。
3. 編集するカスタムコントロールを選択したら、[Edit] (編集) を選択します。
4. [Edit control details] (コントロールの詳細を編集) ページで、[Next] (次へ) を選択します。
5. 「カスタマーマネージドソース」で、更新する API コールデータソースを探します。
6. テーブルからデータソースを選択し、 の削除を選択します。
7. 追加を選択します。
8. AWS API コール を選択します。
9. ステップ 5 で削除したのと同じ API コールを選択し、希望する証拠収集頻度を選択します。
10. データソース名 で、わかりやすい名前を指定します。
11. (オプション) [その他の詳細] に、データソースの説明とトラブルシューティングの説明を入力します。
12. [次へ] をクリックします。
13. [アクションプランを編集]のページで、[次へ] を選択します。
14. 確認と更新ページで、カスタムコントロールの情報を確認します。ステップに関する情報を変更するには、[編集] を選択します。
15. 完了したら、[変更の保存] を選択します。

コントロールを編集すると、そのコントロールを含むすべてのアクティブな評価で、その変更は翌日の 00:00 UTC に有効になります。

AWS Configからのコンプライアンスチェック

> **Note**
>
> 以下は、データソースとして AWS Config ルール を使用する標準コントロールとカスタムコントロールの両方に適用されます。

コントロールがデータソースタイプ AWS Config として を使用する場合、証拠収集の頻度を Audit Manager で直接変更することはできません。これは、頻度が AWS Config ルールで定義されているトリガーに従うためです。

には 2 種類のトリガーがあります AWS Config ルール。

1. 設定の変更 - 特定のタイプのリソースが作成、変更、または削除されたときに、ルールの評価 AWS Config を実行します。
2. 定期的 - 選択した頻度 (24 時間ごとなど) でルールの評価 AWS Config を実行します。

のトリガーの詳細については AWS Config ルール、「 AWS Config デベロッパーガイド」の「トリガータイプ」を参照してください。

を管理する方法については AWS Config ルール、「ルールの管理 AWS Config」を参照してください。

Security Hub からのコンプライアンスチェック

> **Note**
>
> 以下は、データソースとして Security Hub チェックを使用する標準コントロールとカスタムコントロールの両方に適用されます。

コントロールが Security Hub をデータソースタイプとして使用する場合、Audit Managerで証拠収集の頻度を直接変更することはできません。これは、証拠収集の頻度が Security Hubチェックのスケジュールに従うためです。

- 定期的なチェックは、最後に実行してから 12 時間以内に自動的に実行されます。周期を変更することはできません。
- 変更によってトリガーされるチェックは、関連付けられたリソースの状態が変更されたときに実行されます。リソースの状態が変わらない場合でも、変更によってトリガーされるチェックの更新時刻は 18 時間ごとに更新されます。これは、コントロールがまだ有効であることを知るのに便利です。一般的に、Security Hub は、可能な限り、変更によってトリガーされるルールを使用します。

詳細については、AWS Security Hub ユーザーガイドの「セキュリティチェックの実行スケジュール」を参照してください。

AWS CloudTrailからのユーザーアクティビティログ

> **Note**
>
> 以下は、データソースとして AWS CloudTrail ユーザーアクティビティログを使用する標準コントロールとカスタムコントロールの両方に適用されます。

アクティビティログをデータソースタイプ CloudTrail として使用するコントロールの証拠収集頻度は、 から変更することはできません。Audit Manager は、この証拠タイプ CloudTrail を から継続的に収集します。頻度は継続的です。これは、ユーザーアクティビティが 1 日のうち、いつでも発生する可能性があるためです。

でのカスタムコントロールの削除 AWS Audit Manager

カスタムコントロールを作成し、不要になった場合は、Audit Manager 環境から削除できます。これにより、ワークスペースをクリーンアップし、現在のタスクと優先順位に関連するカスタムコントロールに集中できます。

前提条件

次の手順は、カスタムコントロールを以前に作成したことを前提としています。

IAM アイデンティティに、 でカスタムコントロールを削除するための適切なアクセス許可があることを確認します AWS Audit Manager。これらのアクセス許可を付与する 2 つの推奨ポリシーは、AWSAuditManagerAdministratorAccessと ですユーザーには AWS Audit Managerへの管理アクセスを許可します。

手順

Audit Manager コンソール、Audit Manager API、または AWS Command Line Interface () を使用してカスタムコントロールを削除できますAWS CLI。

> **Important**
>
> カスタムコントロールを削除すると、そのアクションによって現在関連しているすべてのカスタムフレームワークまたは評価からそのコントロールが削除されます。その結果、Audit Manager はすべての評価においてそのカスタムコントロールの証拠収集を停止します。これには、カスタムコントロールを削除する前に作成した評価も含まれます。

Audit Manager console

Audit Manager コンソールでカスタムコントロールを削除するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. ナビゲーションペインで、[Control library] (コントロールライブラリ) を選択してから、[Custom controls] (カスタムコントロール) のタブを選択します。
3. 削除するコントロールを選択し、[Delete] (削除) を選択します。
4. 表示されるポップアップウィンドウで、[Delete] (削除) を選択して削除を確認します。

AWS CLI

でカスタムコントロールを削除するには AWS CLI

1. まず、削除するカスタムコントロールを特定します。これを行うには、list-controls コマンドを実行して`--control-type`を`Custom`として指定します。

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   レスポンスはカスタムコントロールのリストを返します。削除するコントロールを見つけ、コントロール ID を書き留めます。
2. 次に、delete-control コマンドを実行し、`--control-id`パラメータを使用して削除するコントロールを指定します。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

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

Audit Manager API

API を使用してカスタムコントロールを削除するには

1. ListControls オペレーションを使用して、controlType を として指定しますCustom。レスポンスから、削除するコントロールを見つけ、コントロール ID を書き留めます。
2. DeleteControl オペレーションを使用して、カスタムコントロールを削除します。リクエストで、ControlID パラメータを使用して、削除するコントロールを指定します。

これらの API オペレーションの詳細については、前の手順のリンクのいずれかを選択して、AWS Audit Manager 「 API リファレンス」で詳細を確認してください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

追加リソース

Audit Manager のデータ保持の詳細については、「」を参照してくださいAudit Manager のデータの削除。

AWS Audit Manager 設定の確認と設定

AWS Audit Manager 設定はいつでも確認および設定して、特定のニーズを満たすようにすることができます。

この章では、Audit Manager の設定 にアクセス、確認、および調整するプロセスについて説明します step-by-step。これに従うことで、進化するコンプライアンス目標とビジネス要件に合わせて、一般的な設定、評価設定、証拠ファインダー設定を変更する方法を学習できます。

手順

開始するには、以下の手順に従って Audit Manager の設定を表示します。Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI)、または Audit Manager API を使用して、Audit Manager の設定を表示できます。

設定を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左のナビゲーションペインの [設定] を選択します。
3. 目標を達成するタブを選択します。
   - 一般設定 - このタブを選択すると、一般的な Audit Manager の設定を確認および更新できます。
   - 評価設定 - 評価のデフォルト設定を確認して更新するには、このタブを選択します。
   - 証拠ファインダーの設定 - このタブを選択すると、証拠ファインダーの設定を確認および更新できます。

次のステップ

ユースケースに合わせて Audit Manager の設定をカスタマイズするには、ここに記載されている手順に従ってください。

- 全般設定
  - データ暗号化設定の構成

  - 委任された管理者の追加
  - 委任管理者の変更
  - 委任された管理者を削除する
  - 無効化 AWS Audit Manager
- 評価設定
  - デフォルトの監査所有者の設定
  - デフォルトの評価レポートの送信先の設定
  - Audit Manager 通知の設定
- 証拠ファインダーの設定
  - 証拠ファインダーの有効化
  - 証拠ファインダーのステータスの確認
  - エビデンスファインダーのデフォルトのエクスポート先の設定
  - 証拠ファインダーを無効にする

データ暗号化設定の構成

でデータを暗号化する方法を選択できます AWS Audit Manager。Audit Manager は、データの安全なストレージ AWS マネージドキー 用に一意の を自動的に作成します。デフォルトでは、Audit Manager のデータはこの KMS キーで暗号化されます。ただし、データ暗号化設定をカスタマイズする場合は、独自の対称暗号化カスタマーマネージドキーを指定できます。独自の KMS キーを使用することにより、キーの作成、ローテーション、無効化ができるなど、より高い柔軟性が得られます。

前提条件

カスタマーマネージドキーを指定する場合、評価レポートを生成し、証拠ファインダーの検索結果を正常にエクスポートするには、評価 AWS リージョン と同じ にある必要があります。

手順

データ暗号化設定は、Audit Managerコンソール、 AWS Command Line Interface (AWS CLI)、または Audit Manager API を使用して更新できます。

> **Note**
>
> Audit Manager のデータ暗号化の設定を変更すると、これらの変更は今後作成する新しい評価に適用されます。これには、新しい評価から作成する評価レポートと証拠ファインダーのエクスポートが含まれます。
> この変更は、暗号化の設定を変更する前に作成した既存の評価には適用されません。これには、既存の評価レポートと CSV エクスポートに加え、既存の評価から作成する新しい評価レポートと CSV エクスポートが含まれます。既存の評価とそれらのすべての評価レポートおよび CSV レポートは、引き続き古い KMS キーを使用します。評価レポートを生成する IAM ID が古い KMS キーを使用できない場合は、キーポリシーレベルで許可を付与します。

Audit Manager console

Audit Manager コンソールでデータ暗号化設定を更新するには

1. [全般] 設定タブから、データ暗号化セクションに移動します。
2. Audit Manager によって提供されるデフォルトの KMS キーを使用するには、[暗号化設定をカスタマイズ (詳細)] チェックボックスをクリアします。
3. カスタマーマネージドキーを使用するには、[暗号化設定をカスタマイズ (詳細)] チェックボックスを選択します。その後、既存の KMS キーを選択するか、新しい KMS キーを作成できます。

AWS CLI

でデータ暗号化設定を更新するには AWS CLI

update-settings コマンドを実行して、`--kms-key` パラメータを使用して独自のカスタマーマネージドキーを指定します。

次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

API を使用してデータ暗号化設定を更新するには

UpdateSettings オペレーションを呼び出し、kmsKey パラメータを使用して独自のカスタマーマネージドキーを指定します。

詳細については、前述のリンクを選択して、Audit Manager API リファレンスをご覧ください。これには、言語固有の AWS SDKs のいずれかでこのオペレーションとパラメータを使用する方法に関する情報が含まれます。

追加リソース

- キーの作成方法の詳細については、「AWS Key Management Service ユーザーガイド」の「キーの作成」を参照してください。
- キーポリシーレベルでアクセス許可を付与する方法については、「 AWS Key Management Service デベロッパーガイド」の「他のアカウントのユーザーに KMS キーの使用を許可する」を参照してください。

委任された管理者の追加

を使用して AWS Organizations いて、 のマルチアカウントサポートを有効にする場合は AWS Audit Manager、組織内のメンバーアカウントを Audit Manager の委任管理者として指定できます。

複数の で Audit Manager を使用する場合は AWS リージョン、リージョンごとに委任管理者アカウントを個別に指定する必要があります。Audit Manager の設定で、すべてのリージョンで同じ委任管理者アカウントを使用する必要があります。

前提条件

Audit Manager の委任管理者が操作方法を定義する、次の要素に注意してください。

- アカウントは組織の一部である必要があります。
- 委任管理者を指定する前に、組織のすべての機能を有効にする必要があります。組織の Security Hub 設定も構成する必要があります。このように、Audit Manager はメンバーアカウントから Security Hub の証拠を収集できます。
- 委任管理者アカウントには、Audit Manager の設定時に提供した KMS キーへのアクセス権が必要です。
- Audit Manager では AWS Organizations 、管理アカウントを委任管理者として使用することはできません。

手順

Audit Manager コンソール、 AWS Command Line Interface (AWS CLI)、または Audit Manager API を使用して、委任管理者を追加できます。

> **Note**
>
> Audit Manager 設定で委任管理者を追加すると、管理アカウントは Audit Manager で追加の評価を作成できなくなります。さらに、管理アカウントによって作成された既存の評価の証拠収集は停止します。Audit Manager が証拠を収集し、組織の評価を管理するための主要アカウントである委任管理者アカウントに添付します。

Audit Manager console

Audit Manager コンソールで委任管理者を追加するには

1. [全般] 設定タブから、委任管理者セクションに移動します。
2. [委任管理者のアカウント ID] で、委任管理者アカウント ID を入力します。
3. [委任] を選択します。

AWS CLI

で委任された管理者を追加するには AWS CLI

register-organization-admin-account コマンドを実行し、 `--admin-account-id`パラメータを使用して委任された管理者のアカウント ID を指定します。

次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

API を使用して委任管理者を追加するには

RegisterOrganizationAdminAccount オペレーションを呼び出し、 adminAccountIdパラメータを使用して委任された管理者のアカウント ID を指定します。

詳細については、前述のリンクを選択して、Audit Manager API リファレンスをご覧ください。これには、言語固有の AWS SDKs のいずれかでこのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

委任管理者アカウントを変更するには、「」を参照してください委任管理者の変更。

委任管理者アカウントを削除するには、「」を参照してください委任された管理者を削除する。

追加リソース

- 組織の作成と管理
- 委任された管理者と AWS Organizations 問題のトラブルシューティング

委任管理者の変更

で委任された管理者を変更すると、2 ステップのプロセス AWS Audit Manager になります。まず、現在の委任管理者アカウントを削除する必要があります。その後、委任された管理者として新しいアカウントを追加できます。

このページの手順に従って、委任された管理者を変更します。

目次

前提条件

現在のアカウントを削除する前に

現在の委任管理者アカウントを削除する前に、次の考慮事項に注意してください。

- 証拠ファインダーのクリーンアップタスク - 現在の委任管理者 (アカウント A) が証拠ファインダーを有効にしている場合は、アカウント B を新しい委任管理者として割り当てる前にクリーンアップタスクを実行する必要があります。

  管理アカウントを使用してアカウント A を削除する前に、アカウント A が Audit Manager にサインインし、証拠ファインダーを無効にしていることを確認してください。エビデンスファインダーを無効にすると、エビデンスファインダーが有効だったときにアカウントで作成されたイベントデータストアが自動的に削除されます。

  このタスクが完了しない場合、イベントデータストアはアカウント A に残ります。この場合、元の委任管理者は CloudTrail Lake を使用してイベントデータストア を手動で削除することをお勧めします。

  このクリーンアップタスクは、複数のイベントデータストアで終了しないようにするために必要です。委任管理者アカウントを削除または変更すると、Audit Manager は未使用のイベントデータストアを無視します。ただし、未使用のイベントデータストアを削除しない場合、イベントデータストアには CloudTrail Lake からのストレージコストが引き続き発生します。
- データ削除 - Audit Manager の委任管理者アカウントを削除しても、そのアカウントのデータは削除されません。委任管理者アカウントのリソースデータを削除する場合は、アカウントを削除する前にそのタスクを別途実行する必要があります。どちらの場合も、Audit Manager コンソールでできます。または、Audit Manager が提供する削除 API 操作のいずれかを使用することもできます。実行可能な削除操作のリストについては、「Audit Manager データの削除」を参照してください。

  現時点では、Audit Manager は特定の委任管理者の証拠を削除するオプションを提供していません。代わりに、管理アカウントが Audit Manager の登録を解除すると、登録解除時に現在の委任管理者アカウントのクリーンアップが実行されます。

新しいアカウントを追加する前に

新しい委任管理者アカウントを追加する前に、次の考慮事項に注意してください。

- 新しいアカウントは組織の一部である必要があります。
- 新しい委任管理者を指定する前に、組織 のすべての機能を有効にする必要があります。組織の Security Hub 設定も構成する必要があります。このように、Audit Manager はメンバーアカウントから Security Hub の証拠を収集できます。
- 委任管理者アカウントには、Audit Manager の設定時に提供した KMS キーへのアクセス権が必要です。

- Audit Manager では AWS Organizations 、管理アカウントを委任管理者として使用することはできません。

手順

委任管理者は、Audit Manager コンソール、 AWS Command Line Interface (AWS CLI)、または Audit Manager API を使用して変更できます。

> **Warning**
>
> 委任管理者を変更しても、古い委任管理者アカウントで以前に収集した証拠に引き続きアクセスできます。ただし、Audit Manager は証拠の収集と、古い委任管理者アカウントへの証拠の添付を停止します。

Audit Manager console

Audit Manager コンソールで現在の委任管理者を変更するには

1. (オプション) 現在の委任管理者 (アカウント A) が証拠ファインダーを有効にしている場合は、次のクリーンアップタスクを実行します。

   - アカウント B を新しい委任管理者として割り当てる前に、アカウント A が Audit Manager にサインインして、エビデンスファインダーを無効にしていることを確認します。

     エビデンスファインダーを無効にすると、アカウント A がエビデンスファインダーを有効にした作成されたイベントデータストアは自動的に削除されます。このステップを完了しない場合、アカウント A は CloudTrail Lake に移動し、イベントデータストア を手動で削除する必要があります。それ以外の場合、イベントデータストアはアカウント A に残り、引き続き CloudTrail Lake ストレージ料金が発生します。
2. [全般] 設定タブから、委任管理者セクションに移動して、[削除] を選択します。
3. 表示されるポップアップウィンドウで、[Remove(削除)] を選択して確認します。
4. [委任管理者のアカウント ID] で、新しい委任管理者アカウントの ID を入力します。
5. [委任] を選択します。

AWS CLI

で現在の委任管理者を変更するには AWS CLI

まず、 `--admin-account-id`パラメータを使用して deregister-organization-admin-account コマンドを実行し、現在の委任管理者のアカウント ID を指定します。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

次に、 `--admin-account-id`パラメータを使用して register-organization-admin-account コマンドを実行し、新しい委任管理者のアカウント ID を指定します。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

API を使用して現在の委任管理者を変更するには

まず、 DeregisterOrganizationAdminAccountオペレーションを呼び出し、 adminAccountIdパラメータを使用して現在の委任管理者のアカウント ID を指定します。

次に、 RegisterOrganizationAdminAccountオペレーションを呼び出し、 adminAccountIdパラメータを使用して新しい委任管理者のアカウント ID を指定します。

詳細については、前述のリンクを選択して、Audit Manager API リファレンスをご覧ください。これには、言語固有の AWS SDKs のいずれかでこのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

委任管理者アカウントを削除するには、「」を参照してください委任された管理者を削除する。

追加リソース

- 組織の作成と管理
- 委任された管理者と AWS Organizations 問題のトラブルシューティング

委任された管理者を削除する

委任された管理者アカウントを削除すると、そのアカウントの証拠収集は停止しますが、以前に収集された証拠へのアクセスは保持されます。

Audit Manager の委任管理者アカウントを削除する必要がある場合は、このページの必要なステップに従います。不要なストレージコストを避けるためにリソースをクリーンアップする必要があるため、前提条件と手順を慎重に実行してください。

前提条件

Audit Manager から委任された管理者アカウントを削除する前に、次の考慮事項に注意してください。

エビデンスファインダーのクリーンアップタスク

現在の委任管理者が証拠ファインダーを有効にしている場合は、クリーンアップタスクを実行する必要があります。

管理アカウントを使用して現在の委任管理者を削除する前に、現在の委任管理者アカウントが Audit Manager にサインインし、証拠ファインダーを無効にしていることを確認してください。エビデンスファインダーを無効にすると、エビデンスファインダーが有効だったときにアカウントで作成されたイベントデータストアが自動的に削除されます。

このタスクが完了しない場合、イベントデータストアはアカウントに残ります。この場合、元の委任管理者は CloudTrail Lake を使用してイベントデータストア を手動で削除することをお勧めします。

このクリーンアップタスクは、複数のイベントデータストアで終了しないようにするために必要です。委任管理者アカウントを削除または変更すると、Audit Manager は未使用のイベントデータストアを無視します。ただし、未使用のイベントデータストアを削除しない場合、イベントデータストアには CloudTrail Lake からのストレージコストが引き続き発生します。

データ削除

Audit Manager の委任管理者アカウントを削除しても、そのアカウントのデータは削除されません。委任管理者アカウントのリソースデータを削除する場合は、アカウントを削除する前にそのタスクを別途実行する必要があります。どちらの場合も、Audit Manager コンソールでできます。または、Audit Manager が提供する削除 API 操作のいずれかを使用することもできます。実行可能な削除操作のリストについては、「Audit Manager データの削除」を参照してください。

現時点では、Audit Manager は特定の委任管理者の証拠を削除するオプションを提供していません。代わりに、管理アカウントが Audit Manager の登録を解除すると、登録解除時に現在の委任管理者アカウントのクリーンアップが実行されます。

手順

Audit Manager コンソール、 AWS Command Line Interface (AWS CLI)、または Audit Manager API を使用して、委任管理者を削除できます。

> **Warning**
>
> 委任管理者を変更しても、委任管理者アカウントで以前に収集した証拠に引き続きアクセスできます。ただし、Audit Manager は証拠の収集と、古い委任管理者アカウントへの証拠の添付を停止します。

Audit Manager console

Audit Manager コンソールで現在の委任管理者を削除するには

1. (オプション) 現在の委任管理者がエビデンスファインダーを有効にしている場合は、次のクリーンアップタスクを実行します。
   - 現在の委任管理者が Audit Manager にサインインして、エビデンスファインダーを無効にしていることを確認します。

     エビデンスファインダーを無効にすると、エビデンスファインダーを有効にしたときにアカウントで作成されたイベントデータストアが自動的に削除されます。このステップが完了しない場合、委任管理者アカウントは CloudTrail Lake を使用してイベントデータストア を手動で削除する必要があります。それ以外の場合、イベントデータストアはアカウントに残り、引き続き CloudTrail Lake ストレージ料金が発生します。
2. [全般] 設定タブから、委任管理者セクションに移動して、[削除] を選択します。
3. 表示されるポップアップウィンドウで、[削除] を選択して確認します。

AWS CLI

エビデンスファインダーを無効にすると、エビデンスファインダーを有効にしたときにアカウントで作成されたイベントデータストアが自動的に削除されます。このステップが完了しない

場合、委任管理者アカウントは CloudTrail Lake を使用してイベントデータストア を手動で削除する必要があります。それ以外の場合、イベントデータストアはアカウントに残り、引き続き CloudTrail Lake ストレージ料金が発生します。

で現在の委任管理者を削除するには AWS CLI

deregister-organization-admin-account コマンドを実行し、 `--admin-account-id`パラメータを使用して委任された管理者のアカウント ID を指定します。

次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

API を使用して現在の委任管理者を削除するには

DeregisterOrganizationAdminAccount オペレーションを呼び出し、 adminAccountIdパラメータを使用して委任された管理者のアカウント ID を指定します。

詳細については、前述のリンクを選択して、Audit Manager API リファレンスをご覧ください。これには、言語固有の AWS SDKs のいずれかでこのオペレーションとパラメータを使用する方法に関する情報が含まれます。

追加リソース

- 委任された管理者と AWS Organizations 問題のトラブルシューティング

デフォルトの監査所有者の設定

この設定を使用して、audit ownerAudit Manager で評価へのプライマリアクセス権を持つデフォルトの を指定できます。

手順

この設定は、Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、または Audit Manager API を使用して更新できます。

Audit Manager console

表に AWS アカウント リストされている から選択するか、検索バーを使用して他の を検索できます AWS アカウント。

Audit Manager コンソールでデフォルトの監査所有者を更新するには

1. [評価] 設定タブから、デフォルト監査責任者セクションに移動して、[編集] を選択します。
2. デフォルトの監査所有者を追加するには、[Audit owner (監査所有者)] の下のアカウント名の横にあるチェックボックスをオンします。
3. デフォルトの監査所有者を削除するには、[Audit owner (監査所有者)] の下のアカウント名の横にあるチェックボックスをオフにします。
4. 完了したら、[保存] を選択します。

AWS CLI

でデフォルトの監査所有者を更新するには AWS CLI

update-settings コマンドを実行して、`--default-process-owners` パラメータを使用して監査所有者を指定します。

次の例では、次の *`placeholder text`* を独自の情報に置き換えます。`roleType` は `PROCESS_OWNER` のみである点に注意してください。

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

API を使用してデフォルトの監査所有者を更新するには

UpdateSettings オペレーションを呼び出し、 defaultProcessOwnersパラメータを使用してデフォルトの監査所有者を指定します。`roleType` は `PROCESS_OWNER` のみである点に注意してください。

追加リソース

- 監査所有者の詳細については、本ガイドの「概念と用語」セクションの「監査所有者」を参照してください。

デフォルトの評価レポートの送信先の設定

評価レポートを生成すると、Audit Manager は、任意の S3 バケットにレポートを発行します。この S3 バケットは と呼ばれますassessment report destination。Audit Manager が評価レポートを保存する S3 バケットを選択できます。

前提条件

評価レポートの送信先設定のヒント

評価レポートを正常に生成するには、評価レポートの宛先に次の設定を使用することをお勧めします。

同じリージョンバケット

評価と同じ AWS リージョン にある S3 バケットを使用することをお勧めします。同じリージョンのバケットと評価を使用する場合、評価レポートには最大 22,000 件の証拠項目を含めることができます。逆に、クロスリージョンバケットと評価を使用する場合、含めることができるのは 3,500 の証拠項目のみです。

AWS リージョン

カスタマーマネージドキー AWS リージョン の (指定した場合) は、評価のリージョンと評価レポートの宛先 S3 バケットと一致する必要があります。KMS キーを変更する方法については、「」を参照してくださいデータ暗号化設定の構成。サポートされている Audit Manager リージョンのリストについては、「Amazon Web Services 全般のリファレンス」の「AWS Audit Manager エンドポイントとクォータ」を参照してください。

S3 バケットの暗号化

評価レポートの宛先に SSE-KMS を使用したサーバー側の暗号化 (SSE) を必要とするバケットポリシーがある場合、そのバケットポリシーで使用される KMS キーは、Audit Manager データ暗号化の設定で構成した KMS キーと一致する必要があります。Audit Manager の設定で KMS キーを設定しておらず、評価レポートの宛先バケットポリシーで SSE が必要な場合は、バケットポリシーで SSE-S3 が許可されているようにしてください。データ暗号化に使用される KMS キーを設定する方法については、「」を参照してくださいデータ暗号化設定の構成。

クロスアカウント S3 バケット

クロスアカウント S3 バケットを評価レポートの宛先として使用することは、Audit Manager コンソールではサポートされていません。 AWS CLI または AWS SDKs の 1 つを使用して、評価レ

ポートの宛先としてクロスアカウントバケットを指定できますが、わかりやすくするために、これを行わないことをお勧めします。評価レポートの宛先としてクロスアカウント S3 バケットを使用することを選択する場合は、次の点を考慮してください。

- デフォルトでは、評価レポートなどの S3 オブジェクトは、オブジェクトをアップロード AWS アカウント する によって所有されます。S3 オブジェクト所有権設定を使用して、このデフォルト動作を変更すると、bucket-owner-full-control既定のアクセスコントロールリスト (ACL) があるアカウントによって記述された新しいオブジェクトが自動的にバケット所有者によって所有されるようにできます。

  必須ではありませんが、クロスアカウントバケットの設定に次の変更を加えることをお勧めします。これらの変更を加えることで、バケット所有者は、バケットに発行する評価レポートを完全に制御できるようになります。

  - S3 バケットのオブジェクト所有権を、デフォルトのオブジェクトライターではなく、優先バケット所有者に設定
  - バケットポリシーを追加して、そのバケットにアップロードされたオブジェクトに bucket-owner-full-control ACL が含まれるようにする

- Audit Manager がクロスアカウント S3 バケットでレポートを発行できるようにするには、次の S3 バケットポリシーを評価レポートの宛先に追加する必要があります。*placeholder text* を独自の情報に置き換えます。このポリシーの Principal 要素は、評価を所有し、評価レポートを作成するユーザーまたはロールです。Resource は、レポートが発行されるクロスアカウント S3 バケットを指定します。

```
{
  "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/*"
            ]
        }
    ]
}
```

手順

この設定は、Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、または Audit Manager API を使用して更新できます。

Audit Manager console

Audit Manager コンソールでデフォルトの評価レポートの送信先を更新するには

1. [評価] 設定タブから、評価レポートの送信先セクションに移動します。
2. 既存の S3 バケットを使用するには、ドロップダウンメニューからバケット名を選択します。
3. 新しい S3 バケットを作成するには、[Create new bucket] (新しいバケットを作成) を選択します。
4. 完了したら、[保存] を選択します。

AWS CLI

でデフォルトの評価レポートの送信先を更新するには AWS CLI

update-settings コマンドを実行して、`--default-assessment-reports-destination` パラメータを使用して S3 バケットを指定します。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://DOC-EXAMPLE-DESTINATION-BUCKET
```

Audit Manager API

API を使用してデフォルトの評価レポートの宛先を更新するには

UpdateSettings オペレーションを呼び出し、defaultAssessmentReportsDestination パラメータを使用して S3 バケットを指定します。

追加リソース

- バケットの作成
- 評価レポート

Audit Manager 通知の設定

選択した Amazon SNS トピックに通知を送信するように Audit Manager を設定できます。その SNS トピックにサブスクライブしている場合は、Audit Manager にサインインするたびに通知が直接届きます。

このページのステップに従って、通知設定を表示および更新して、ユーザー設定に合わせる方法を確認してください。標準 SNS トピックまたは FIFO (first-in-first-out) SNS トピックを使用できます。Audit Manager は FIFO トピックへの通知の送信をサポートしていますが、メッセージの送信順序は保証されていません。

前提条件

自分が所有していない Amazon SNS トピックを使用する場合は、そのために AWS Identity and Access Management (IAM) ポリシーを設定する必要があります。より具体的には、トピックの Amazon リソースネーム (ARN) からの発行を許可するように設定する必要があります。使用できるポリシーの例については、「」を参照してください例 1(SNSトピックへの許可)。

手順

この設定は、Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、または Audit Manager API を使用して更新できます。

Audit Manager console

Audit Manager コンソールで通知設定を更新するには

1. [評価] 設定タブから、通知セクションに移動します。
2. 既存の SNS トピックを使用するには、ドロップダウンメニューからトピック名を選択します。

3. 新しい SNS トピックを作成するには、[新しいトピックを作成] を選択します。
4. 完了したら、[保存] を選択します。

AWS CLI

の通知設定を更新するには AWS CLI

update-settings コマンドを実行し、`--sns-topic` パラメータを使用して SNS トピックを指定します。

次の例では、次の *placeholder text* を独自の情報に置き換えます。

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

API を使用して通知設定を更新するには

UpdateSettings オペレーションを呼び出し、snsTopic パラメータを使用して SNS トピックを指定します。

追加リソース

- Amazon SNS トピックの作成方法については、「Amazon SNS ユーザーガイド」の「Amazon SNS トピックの作成」を参照してください。
- Audit Manager が Amazon SNS トピックに通知を送信することを許可するために使用できるポリシーの例については、「」を参照してください。 例 1(SNSトピックへの許可)
- Audit Manager で通知を呼び出すアクションのリストの詳細については、「の通知 AWS Audit Manager」を参照してください。
- Audit Manager での問題の通知の解決策については、「」を参照してください通知に関する問題のトラブルシューティング。

証拠ファインダーの有効化

Audit Manager の証拠ファインダー機能を有効にして、 で証拠を検索できます AWS アカウント。Audit Manager の委任管理者である場合は、組織内のすべてのメンバーアカウントの証拠を検索できます。

証拠ファインダーを有効にする方法については、次のステップに従います。この機能には Lake でイベントデータストアを作成および管理するための特定のアクセス許可が必要になるため、前提条件に細心の注意 CloudTrail を払ってください。

前提条件

エビデンスファインダーを有効にするために必要な権限

証拠ファインダーを有効にするには、 CloudTrail Lake でイベントデータストアを作成および管理するためのアクセス許可が必要です。この機能を使用するには、 CloudTrail Lake クエリを実行するためのアクセス許可が必要です。使用できるアクセス許可ポリシーの例については、「」を参照してください例 4 (エビデンスファインダーを有効にする許可)。

アクセス許可に関するヘルプが必要な場合は、 AWS 管理者にお問い合わせください。 AWS 管理者の場合は、必要な権限ステートメントをコピーして IAM ポリシーに添付できます。

手順

エビデンスファインダーの有効化をリクエストする

このタスクは、Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、または Audit Manager API を使用して完了できます。

> **Note**
>
> 証拠 AWS リージョン を検索する各 で証拠ファインダーを有効にする必要があります。

Audit Manager console

Audit Manager コンソールで証拠ファインダーの有効化をリクエストするには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. [エビデンスファインダー] 設定タブから、[エビデンスファインダー] セクションに移動します。

3. 必須のアクセス許可ポリシー を選択し、 CloudTrail Lake のアクセス許可を表示して、必要な証拠ファインダーのアクセス許可を表示します。これらの権限をまだ持っていない場合は、このポリシーステートメントをコピーして IAM ポリシーに添付できます。
4. [Enable (有効化)] を選択します。
5. ポップアップウィンドウで、[有効化のリクエスト] を選択します。

AWS CLI

で証拠ファインダーの有効化をリクエストするには AWS CLI

`--evidence-finder-enabled` パラメータで、update-settings コマンドを実行します。

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

API を使用して証拠ファインダーの有効化をリクエストするには

UpdateSettings オペレーションを呼び出し、 evidenceFinderEnabledパラメータを使用します。

詳細については、前述のリンクを選択して、Audit Manager API リファレンスをご覧ください。これには、言語固有の AWS SDKs のいずれかでこのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

証拠ファインダーの有効化をリクエストしたら、リクエストのステータスを確認できます。手順については、「証拠ファインダーのステータスの確認」を参照してください。

追加リソース

- 証拠ファインダー
- 証拠ファインダーの問題のトラブルシューティング

証拠ファインダーのステータスの確認

証拠ファインダーを有効にするリクエストを送信した後、この機能を有効にしてイベントデータストアを作成するまでに最大 10 分かかります。イベントデータストアが作成されるとすぐに、新しいエビデンスはすべてイベントデータストアに取り込まれます。

エビデンスファインダーが有効になってイベントデータストアが作成されると、新しく作成されたイベントデータストアに最大 2 年分の過去のエビデンスをバックフィルします。この処理は自動的に行われ、完了するまでに最大 7日 かかります。

このページの手順に従って、証拠ファインダーを有効にするリクエストのステータスを確認して理解します。

前提条件

証拠ファインダーを有効にするためのステップに従っていることを確認してください。手順については、「証拠ファインダーの有効化」を参照してください。

手順

エビデンスファインダーの現在のステータスは、Audit Manager コンソール、 AWS CLI、または Audit Manager API を使用して確認できます。

Audit Manager console

Audit Manager コンソールで証拠ファインダーの現在のステータスを表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左のナビゲーションペインの [Settings (設定)] を選択します。
3. エビデンスファインダーを有効にする — オプションで、現在のステータスを確認します。

   各ステータスは次のように定義されています。

ステータス	説明
証拠ファインダーが有効になっていない	証拠ファインダーをまだ正常に有効にしていません。

ステータス	説明
エビデンスファインダーの有効化をリクエストしました	リクエストは、イベントデータストアの作成を保留しています。
証拠ファインダーが有効になっている	イベントデータストアが作成されました。エビデンスファインダーを使用できます。 エビデンスの量に応じて、新しいイベントデータストアに過去のエビデンスデータをバックフィルするのに最大 7 日かかります。青の情報パネルは、データのバックフィルが進行中であることを示します。それまでは自由にエビデンスファインダーの探索を始めてください。ただし、バックフィルが完了するまで、すべてのデータが使用できるわけではない点に注意してください。
証拠ファインダーの無効化をリクエストしました	リクエストは、イベントデータストアの削除を保留しています。
証拠ファインダーが無効になっています	証拠ファインダーは完全に無効になっており、イベントデータストアは削除されます。

AWS CLI

で証拠ファインダーの現在のステータスを確認するには AWS CLI

`--attribute` パラメータを `EVIDENCE_FINDER_ENABLEMENT` に設定して、get-settings コマンドを実行します。

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

次のような情報が返されます。

enablementStatus

この属性はエビデンスファインダーの現在のステータスを示します。

- ENABLE_IN_PROGRESS— エビデンスファインダーの有効化をリクエストしました。イベントデータストアは、現在、エビデンスファインダーのクエリをサポートするために作成中です。
- ENABLED— イベントデータストアが作成され、エビデンスファインダーが有効化されています。イベントデータストアが過去のエビデンスデータでバックフィルされるまで 7 日間待つことをお勧めします。その間はエビデンスファインダーを使用できますが、バックフィルが完了するまですべてのデータを使用できるわけではありません。
- DISABLE_IN_PROGRESS — エビデンスファインダーを無効にするようリクエストしましたが、リクエストはイベントデータストアが削除されるまで保留されています。
- DISABLED— エビデンスファインダーは永久に無効化され、イベントデータストアは削除されました。この時点以降、エビデンスファインダーは再有効化できません。

backfillStatus

この属性はエビデンスデータバックフィルの現在のステータスを示します。

- NOT_STARTED— バックフィルはまだ開始していません。
- IN_PROGRESS— バックフィルは進行中です。エビデンスデータの量に応じて、完了するまでに最大 7 日 かかります。
- COMPLETED— バックフィルは完了しました。過去のエビデンスはすべてクエリ可能です。

Audit Manager API

API を使用して証拠ファインダーの現在のステータスを表示するには

attribute パラメータを に設定して GetSettingsオペレーションを呼び出しますEVIDENCE_FINDER_ENABLEMENT。次のような情報が返されます。

enablementStatus

この属性はエビデンスファインダーの現在のステータスを示します。

- ENABLE_IN_PROGRESS — エビデンスファインダーの有効化をリクエストしました。イベントデータストアは、現在、エビデンスファインダーのクエリをサポートするために作成中です。
- ENABLED — イベントデータストアが作成され、エビデンスファインダーが有効化されています。イベントデータストアが過去のエビデンスデータでバックフィルされるまで 7 日間待つことをお勧めします。その間はエビデンスファインダーを使用できますが、バックフィルが完了するまですべてのデータを使用できるわけではありません。

- DISABLE_IN_PROGRESS - エビデンスファインダーの無効化をリクエストしましたが、リクエストはイベントデータストアが削除されるまで保留されています。
- DISABLED — エビデンスファインダーは永久に無効化され、イベントデータストアは削除されました。この時点以降、エビデンスファインダーは再有効化できません。

backfillStatus

この属性はエビデンスデータバックフィルの現在のステータスを示します。

- NOT_STARTED はバックフィルがまだ開始されていないことを意味します。
- IN_PROGRESS はバックフィルが進行中であることを意味します。エビデンスデータの量に応じて、完了するまでに最大 7 日 かかります。
- COMPLETED はバックフィルが完了したことを意味します。過去のエビデンスはすべてクエリ可能です。

詳細については、「Audit Manager API リファレンスevidenceFinderEnablement」の「」を参照してください。

次のステップ

証拠ファインダーが正常に有効になったら、この機能の使用を開始できます。イベントデータストアが過去のエビデンスデータでバックフィルされるまで 7 日間待つことをお勧めします。その間は証拠ファインダーを使用できますが、バックフィルが完了するまですべてのデータが利用できるとは限りません。

証拠ファインダーの使用を開始するには、「」を参照してください証拠ファインダーでの証拠の検索。

追加リソース

- 証拠ファインダーの問題のトラブルシューティング

証拠ファインダーを無効にする

エビデンスファインダーが不要になった場合は、いつでもこの機能を無効にできます。

証拠ファインダーを無効にする方法については、次のステップに従います。証拠ファインダーを有効にしたときに作成された CloudTrail Lake のイベントデータストアを削除するには、特定のアクセス許可が必要になるため、前提条件に細心の注意を払ってください。

前提条件

エビデンスファインダーを無効にするために必要な権限

証拠ファインダーを無効にするには、 CloudTrail Lake のイベントデータストアを削除するためのアクセス許可が必要です。使用できるポリシーの例については、「エビデンスファインダーを無効にする権限」を参照してください。

アクセス許可に関するヘルプが必要な場合は、 AWS 管理者にお問い合わせください。 AWS 管理者の場合は、必要な権限ステートメントを IAM ポリシーに添付できます。

手順

このタスクは、Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、または Audit Manager API を使用して完了できます。

> **Warning**
>
> 証拠ファインダーを無効にすると、Audit Manager が作成した CloudTrail Lake イベントデータストアが削除されます。その結果、この機能は再有効化できません。無効化後にエビデンスファインダーを再度使用するには、サービスを完全に無効化 AWS Audit Managerしてから、再有効化する必要があります。

Audit Manager console

Audit Manager コンソールで証拠ファインダーを無効にするには

1. Audit Manager 設定ページのエビデンスファインダーセクションで、[無効化] を選択します。
2. 表示されるポップアップウィンドウで、**Yes** を入力して決定を確認します。
3. [無効化のリクエスト] を選択します。

AWS CLI

で証拠ファインダーを無効にするには AWS CLI

`--no-evidence-finder-enabled` パラメータで、update-settings コマンドを実行します。

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

API を使用して証拠ファインダーを無効にするには

UpdateSettings オペレーションを呼び出し、 evidenceFinderEnabledパラメータを使用します。

詳細については、前述のリンクを選択して、Audit Manager API リファレンスをご覧ください。これには、言語固有の AWS SDKs のいずれかでこのオペレーションとパラメータを使用する方法に関する情報が含まれます。

追加リソース

- 証拠ファインダーの問題のトラブルシューティング

エビデンスファインダーのデフォルトのエクスポート先の設定

証拠ファインダーでクエリを実行すると、検索結果をカンマ区切り値 (CSV) ファイルにエクスポートできます。この設定を使用して、Audit Manager がエクスポートしたファイルを保存するデフォルトの S3 バケットを選択します。

前提条件

S3 バケットには、 がエクスポートファイルを CloudTrail 書き込むために必要なアクセス許可ポリシーが必要です。より具体的には、バケットポリシーには `s3:PutObject`アクションとバケット ARN が含まれ、サービスプリンシパル CloudTrail としてリストされている必要があります。

- 使用できるアクセス許可ポリシーの例については、「」を参照してください例 3 (エクスポート先のアクセス許可)。
- このポリシーを S3 バケットにアタッチする手順については、Amazon S3コンソール を使用したバケットポリシーの追加」を参照してください。

- その他のヒントについては、このページの「エクスポート先の設定に関するヒント」を参照してください。

エクスポート先の設定に関するヒント

ファイルのエクスポートを確実に成功させるために、エクスポート先の以下の設定を確認することをお勧めします。

AWS リージョン

カスタマーマネージドキー AWS リージョン の (提供した場合) は、評価のリージョンと一致する必要があります。KMS キーの変更方法については、「Audit Manager のデータ暗号化設定」を参照してください。

クロスアカウント S3 バケット

エクスポート先として、クロスアカウント S3 バケットを使用することは、Audit Manager コンソールではサポートされていません。 AWS CLI または AWS SDKs のいずれかを使用してクロスアカウントバケットを指定することは可能ですが、わかりやすくするために、これを行わないことをお勧めします。エクスポート先として、クロスアカウント S3 バケットを使用することを選択する場合は、次の点を考慮してください。

- デフォルトでは、CSV エクスポートなどの S3 オブジェクトは、オブジェクトをアップロード AWS アカウント する によって所有されます。S3 オブジェクト所有権設定を使用して、このデフォルト動作を変更すると、`bucket-owner-full-control`既定のアクセスコントロールリスト (ACL) があるアカウントによって記述された新しいオブジェクトが自動的にバケット所有者によって所有されるようにできます。

  必須ではありませんが、クロスアカウントバケットの設定に次の変更を加えることをお勧めします。これらの変更をすることで、バケット所有者はバケットに発行するエクスポート済みファイルを完全に制御できます。

  - S3 バケットのオブジェクト所有権を、デフォルトのオブジェクトライターではなく、優先バケット所有者に設定
  - バケットポリシーを追加して、そのバケットにアップロードされたオブジェクトに `bucket-owner-full-control` ACL が含まれるようにする
- Audit Manager がファイルをクロスアカウント S3 バケットにエクスポートできるようにするには、次の S3 バケットポリシーをエクスポート先に追加する必要があります。*`placeholder text`* を独自の情報に置き換えます。このポリシーの `Principal` 要素は、評価を所有し、

ファイルをエクスポートするユーザーまたはロールです。Resource は、ファイルのエクスポート先のクロスアカウント S3 バケットを指定します。

```
{
  "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/*"
          ]
      }
  ]
}
```

手順

この設定は、Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、または Audit Manager API を使用して更新できます。

Audit Manager console

Audit Manager コンソールでエクスポート先設定を更新するには

1. [エビデンスファインダー] 設定タブから、[エクスポート先] セクションに移動します。
2. 以下のオプションのいずれかを選択します。

- 現在の S3 バケットを削除する場合は、[削除] を選択して設定をクリアします。
- デフォルト S3 バケットを初めて保存する場合は、ステップ 3 に進みます。

3. エクスポートしたファイルを保存する S3 バケットを指定します。

- [S3 を参照] を選択し、バケットのリストから選択します。
- または、**s3://bucketname/prefix** 形式でバケット URI を入力できます。

> **Tip**
>
> エクスポート先のバケットを整理しておくために、CSV エクスポート用のオプションフォルダを作成できます。そのためには、[リソース URI] ボックス (例: **/evidenceFinderCSVExports**) の値にスラッシュ (**/**) とプレフィックスを追加します。Audit Manager は CSV ファイルをバケットに追加するときにこのプレフィックスを含め、Amazon S3 はプレフィックスで指定されたパスを生成します。Amazon S3 でのプレフィックスの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 コンソールのオブジェクトを整理する」を参照してください。

4. 完了したら、[保存] を選択します。

S3 バケットの作成方法については、「Amazon S3 ユーザーガイド」の「バケットを作成する」を参照してください。

AWS CLI

でエクスポート先設定を更新するには AWS CLI

update-settings コマンドを実行して、`--default-export-destination` パラメータを使用して S3 バケットを指定します。

次の例では、次の *`placeholder text`* を独自の情報に置き換えます。

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=DOC-EXAMPLE-DESTINATION-BUCKET
```

S3 バケットの作成方法については、「AWS CLI コマンドリファレンス」の create-bucket を参照してください。

Audit Manager API

API を使用してエクスポート先設定を更新するには

UpdateSettings オペレーションを呼び出し、 defaultExportDestinationパラメータを使用して S3 バケットを指定します。

S3 バケットを作成する方法については、CreateBucketAmazon S3 API リファレンスの「」を参照してください。

の通知 AWS Audit Manager

AWS Audit Manager は、Amazon Simple Notification Service (Amazon SNS) を通じてユーザーアクションについて通知できます。

Audit Manager は、次のいずれかのイベントが発生したときに通知を送信します。

- 監査所有者がコントロールセットのレビューを委任する。
- 代理人がレビュー済みコントロールセットを監査所有者に送信する。
- 監査所有者がコントロールセットのレビューを完了する。

追加リソース

- Audit Manager で通知を設定するには、「」を参照してくださいAudit Manager 通知の設定。
- 一般的な質問や問題に対する回答を見つけるには、このガイドの通知に関する問題のトラブルシューティング「トラブルシューティング」セクションの「」を参照してください。

の一般的な問題のトラブルシューティング AWS Audit Manager

を使用すると AWS Audit Manager、トラブルシューティングが必要な特定の問題や課題が発生する可能性があります。評価の設定、証拠の収集、またはサービスのその他の側面で課題に直面しているかどうかにかかわらず、このトラブルシューティングガイドを使用して、一般的な問題を迅速かつ効率的に解決するのに役立つ推奨事項を見つけることができます。

以下のトピックのリストを確認し、シナリオに最も適したトピックを見つけ、提供されたガイダンスに従って軌道に戻ることをお勧めします。提供されたトラブルシューティングのステップに従うことで、問題を個別に解決し、Audit Manager の全機能を活用し続けることができます。ただし、特定の問題がここで説明されていない場合や、推奨されたステップに従っても解決できない場合は、 に連絡してサポートAWS Supportを受けることをお勧めします。

トピック

- 評価と証拠収集の問題に関するトラブルシューティング
- 評価レポートの問題のトラブルシューティング
- コントロールとコントロールセットの問題のトラブルシューティング
- ダッシュボードに関する問題のトラブルシューティング
- 委任された管理者と AWS Organizations 問題のトラブルシューティング
- 証拠ファインダーの問題のトラブルシューティング
- フレームワークの問題のトラブルシューティング
- 通知に関する問題のトラブルシューティング
- 許可とアクセスの問題のトラブルシューティング

評価と証拠収集の問題に関するトラブルシューティング

このページの情報を参照して、Audit Manager での一般的な評価と証拠収集の問題を解決できます。

証拠収集の問題

- 評価を作成しましたが、まだ証拠が表示されません
- 私の評価では、 からコンプライアンスチェックの証拠が収集されていません AWS Security Hub

- 私の評価では、 からコンプライアンスチェックの証拠が収集されていません AWS Config
- 私の評価では、 AWS CloudTrailからユーザーアクティビティの証拠が収集されていません
- 評価で AWS API コールの設定データの証拠が収集されていない
- 共通コントロールが自動証拠を収集していない
- 証拠がさまざまな間隔で生成されており、収集頻度がわかりません
- Audit Manager を無効にしてから再度有効にしましたが、既存の評価では証拠が収集されなくなりました
- 評価の詳細ページで、評価を再作成するように求められます。
- データソースと証拠ソースの違いは何ですか？

評価の問題

- 評価の作成に失敗した
- 対象範囲内のアカウントを組織から削除するとどうなりますか?
- 評価の対象となるサービスが表示されない
- 評価の範囲内のサービスを編集できません
- サービスの対象範囲とデータソースタイプにはどのような違いがありますか?

評価を作成しましたが、まだ証拠が表示されません

証拠が表示されない場合は、評価を作成してから 24 時間が経過していなかったか、設定エラーが発生している可能性があります。

次を確認することをお勧めします。

1. 評価を作成してから 24 時間が経過していることを確認してください。自動証拠は、評価を作成してから 24 時間後に利用可能になります。
2. 証拠が表示される予定の AWS リージョン と同じ で Audit Manager AWS のサービス を使用していることを確認してください。
3. AWS Config と からのコンプライアンスチェックの証拠が表示されることが予想される場合は AWS Security Hub、 AWS Config と Security Hub コンソールの両方にこれらのチェックの結果が表示されていることを確認してください。 AWS Config および Security Hub の結果は、Audit Manager を使用する AWS リージョン のと同じ に表示されます。

それでも評価に証拠が見つからず、これらの問題のいずれかが原因ではない場合は、このページで説明されている他の考えられる原因を確認してください。

私の評価では、 からコンプライアンスチェックの証拠が収集されていません AWS Security Hub

AWS Security Hub コントロールのコンプライアンスチェックの証拠が表示されない場合は、次のいずれかの問題が原因である可能性があります。

AWS Security Hub に設定がありません

この問題は、 AWS Security Hubを有効にした際に一部の設定手順が行われなかった場合に発生する可能性があります。

この問題を解決するには、Audit Manager に必要な設定で Security Hub を有効にしていることを確認してください。手順については、「有効化と設定 AWS Security Hub (オプション)」を参照してください。

Security Hub コントロール名が**`ControlMappingSource`**に誤って入力されました

Audit Manager API を使用してカスタムコントロールを作成する場合、証拠収集のデータソースマッピングとして Security Hub コントロールを指定できます。そのためには、コントロール ID を`keywordValue`として入力します。

Security Hub コントロールのコンプライアンスチェック証拠が表示されない場合は、`ControlMappingSource` に`keywordValue`が正しく入力されていない可能性があります。`keywordValue` は、大文字と小文字が区別されます。間違って入力すると、Audit Manager が適用するルールを認識しない可能性があります。その結果、指定のコントロールのコンプライアンスチェックの証拠が期待どおりに収集されない可能性があります。

この問題を解決するには、カスタムコントロールを更新し、`keywordValue`を修正してください。Security Hub キーワードの正しい形式はさまざまです。精度については、 のリストを参照してくださいサポートされている Security Hub コントロール 。

`AuditManagerSecurityHubFindingsReceiver` Amazon EventBridge ルールがありません

Audit Manager を有効にすると、 という名前のルール`AuditManagerSecurityHubFindingsReceiver`が Amazon で自動的に作成され、有効になります EventBridge。このルールにより、Audit Manager は Security Hub の検出結果を証拠として収集できます。

Security Hub を使用する でこのルール AWS リージョン がリストされておらず、有効になっていない場合、Audit Manager はそのリージョンの Security Hub の検出結果を収集できません。

この問題を解決するには、 EventBridge コンソールに移動し、`AuditManagerSecurityHubFindingsReceiver`ルールが に存在することを確認します AWS アカウント。ルールが存在しない場合は、Audit Manager を無効にしてからサービスを再度有効にすることをお勧めします。このアクションを実行しても問題が解決されない場合や、Audit Manager を無効にできない場合は、AWS Supportまでお問い合わせください。

Security Hub によって作成されたサービスにリンクされた AWS Config ルール

Audit Manager は、Security Hub が作成するサービスにリンクされた AWS Config ルールから証拠を収集しないことに注意してください。これは、Security Hub サービスによって有効および制御される特定のタイプのマネージド AWS Config ルールです。Security Hub は、同じルールの他のインスタンスがすでに存在する場合でも、これらのサービスにリンクされたルールのインスタンスを AWS 環境に作成します。そのため、証拠の重複を防ぐため、Audit Manager はサービスにリンクされたルールからの証拠収集をサポートしていません。

Security Hub でセキュリティコントロールを無効にしました。Audit Manager は、そのセキュリティコントロールのコンプライアンスチェックの証拠を収集しますか？

Audit Manager は、無効化されたセキュリティコントロールの証拠を収集しません。

Security Hub でセキュリティコントロールのステータスを無効にすると、現在のアカウントとリージョンでそのコントロールのセキュリティチェックは実行されません。その結果、Security Hub で利用できるセキュリティ検出結果はなく、Audit Manager によって関連する証拠も収集されません。

Security Hub で設定した無効ステータスを尊重することで、Audit Manager は、意図的に無効にしたコントロールを除き、評価が環境に関連するアクティブなセキュリティコントロールと検出結果を正確に反映するようにします。

Security Hub **`Suppressed`**で検出結果のステータスを に設定します。Audit Manager は、その検出結果に関するコンプライアンスチェックの証拠を収集しますか？

Audit Manager は、検出結果を抑制したセキュリティコントロールの証拠を収集します。

Security Hub で検出結果のワークフローステータスを抑制に設定した場合、検出結果を確認し、アクションが必要ではないと判断することを意味します。Audit Manager では、これらの抑制された検出結果は証拠として収集され、評価に添付されます。証拠の詳細には、Security Hub から直接SUPPRESSED報告された の評価ステータスが表示されます。

このアプローチにより、Audit Manager の評価が Security Hub からの結果を正確に表し、監査でさらなるレビューや検討が必要な抑制された調査結果を可視化できます。

私の評価では、 からコンプライアンスチェックの証拠が収集されていません AWS Config

AWS Config ルールのコンプライアンスチェックの証拠が表示されない場合は、次のいずれかの問題が原因である可能性があります。

ルール ID が**ControlMappingSource**に誤って入力されました

Audit Manager API を使用してカスタムコントロールを作成する場合、証拠収集のデータソースマッピングとして AWS Config ルールを指定できます。指定するkeywordValueは、ルールのタイプによって異なります。

AWS Config ルールのコンプライアンスチェックの証拠が表示されない場合は、 が に正しく入力keywordValueされていない可能性がありますControlMappingSource。keywordValue は、大文字と小文字が区別されます。誤って入力すると、Audit Manager が適用するルールを認識しない可能性があります。その結果、そのルールのコンプライアンスチェック証拠が期待どおりに収集されない可能性があります。

この問題を解決するには、カスタムコントロールを更新し、keywordValueを修正してください。

- カスタムルールの場合は、keywordValueにCustom_というプレフィックスがあり、その後にカスタムルール名が続くことを確認してください。カスタムルール名の形式は異なる場合があります。正確さを期すには、AWS Config コンソールにアクセスしてカスタムルール名を確認してください。
- マネージドルールの場合は、keywordValueがALL_CAPS_WITH_UNDERSCORES内のルール識別子であることを確認してください。例えば CLOUDWATCH_LOG_GROUP_ENCRYPTED です。正確さを期すには、サポートされているマネージドルールキーワードのリストを参照してください。

> **Note**
>
> マネージドルールによっては、ルール識別子はルール名と異なる場合があります。例えば、 restricted-ssh のルール識別子は INCOMING_SSH_DISABLED です。ルール名ではなく、必ずルール識別子を使用するようにしてください。ルール ID を検索するには、マネージドルールのリストからルールを選択し、その識別子の値を探します。

このルールはサービスにリンクされた AWS Config ルールである

マネージドルールとカスタムルールを証拠収集用のデータソースマッピングとして使用できます。ただし、Audit Manager は、サービスにリンクされたルールからの証拠はほとんど収集しません。

Audit Manager が証拠を収集するサービスにリンクされたルールには、次の 2 つのタイプしかありません。

- コンフォーマンスパックのサービスにリンクされたルール
- のサービスにリンクされたルール AWS Organizations

Audit Manager は、他のサービスにリンクされたルール、特に以下のプレフィックスを含む Amazon リソースネーム (ARN) を持つルールからの証拠を収集しません。`arn:aws:config:*:*:config-rule/aws-service-rule/...`

Audit Manager がサービスにリンクされた AWS Config ルールからほとんど証拠を収集しない理由は、評価で証拠が重複するのを防ぐためです。サービスにリンクされたルールは、他の がアカウントにルール AWS のサービス を作成できるようにする特定のタイプのマネージド AWS Config ルールです。例えば、一部の Security Hub コントロールは、 AWS Config サービスにリンクされたルールを使用してセキュリティチェックを実行します。サービスにリンクされた AWS Config ルールを使用する Security Hub コントロールごとに、Security Hub は必要な AWS Config ルールのインスタンスを AWS 環境に作成します。これは、アカウントに元のルールが既に存在している場合でも発生します。そのため、同じルールから同じ証拠を 2 回収集することを避けるため、Audit Manager はサービスにリンクされたルールを無視し、そこから証拠を収集しません。

AWS Config が有効になっていない

AWS Config で を有効にする必要があります AWS アカウント。この AWS Config 方法で を設定すると、Audit Manager は AWS Config ルールの評価が行われるたびに証拠を収集します。 AWS Config で を有効にしていることを確認します AWS アカウント。手順については、「 の有効化とセットアップ AWS Config」を参照してください。

AWS Config ルールは、評価を設定する前にリソース設定を評価しました

特定のリソースの設定変更を評価するように AWS Config ルールが設定されている場合、 の評価 AWS Config と Audit Manager の証拠の間に不一致が生じることがあります。これは、Audit Manager 評価でコントロールを設定する前にルール評価が行われた場合に発生します。この場合、基になるリソースの状態が再び変更され、ルールの再評価がトリガーされるまで、Audit Manager は証拠を生成しません。

回避策として、 AWS Config コンソールでルール に移動し、ルール を手動で再評価できます。これにより、そのルールに関連するすべてのリソースの評価が新たに開始されます。

私の評価では、 AWS CloudTrailからユーザーアクティビティの証拠が収集されていません

Audit Manager API を使用してカスタムコントロールを作成する場合、証拠収集のデータソースマッピングとして CloudTrail イベント名を指定できます。そのためには、イベント名を`keywordValue`として入力します。

CloudTrail イベントのユーザーアクティビティの証拠が表示されない場合は、 `keywordValue`が に誤って入力された可能性がありますControlMappingSource。keywordValue は、大文字と小文字が区別されます。誤って入力すると、Audit Manager がイベント名を認識しない可能性があります。その結果、該当イベントのユーザーアクティビティの証拠を意図したとおりに収集できない可能性があります。

この問題を解決するには、カスタムコントロールを更新し、keywordValueを修正してください。イベントが`serviceprefix_ActionName`と記述されていることを確認してください。例えば `cloudtrail_StartLogging` です。正確さを期すために、サービス認証リファレンスで AWS のサービス プレフィックスとアクション名を確認してください。

評価で AWS API コールの設定データの証拠が収集されていない

Audit Manager API を使用してカスタムコントロールを作成する場合、証拠収集のデータソースマッピングとして AWS API コールを指定できます。そのためには、API コールを`keywordValue`として入力します。

AWS API コールの設定データの証拠が表示されない場合は、 `keywordValue`が に誤って入力された可能性がありますControlMappingSource。keywordValue大文字と小文字を区別します。誤って入力すると、Audit Manager がそのAPI コールを認識しない可能性があります。その結果、その API コールに関する構成データの証拠を意図したとおりに収集できない可能性があります。

この問題を解決するには、カスタムコントロールを更新し、keywordValueを修正してください。API コールがserviceprefix_ActionNameと記述されていることを確認してください。例えば iam_ListGroups です。精度については、 のリストを参照してくださいAWS でサポートされている API コール AWS Audit Manager。

共通コントロールが自動証拠を収集していない

共通コントロールを確認すると、次のメッセージが表示されます。この共通コントロールは、コアコントロール から自動証拠を収集しません。

つまり、現在、この共通コントロールをサポートできる AWS マネージド証拠ソースはありません。その結果、証拠ソースタブは空になり、コアコントロールは表示されません。

共通コントロールが自動証拠を収集しない場合、手動共通コントロール と呼ばれます。手動の一般的なコントロールでは、通常、物理的な記録と署名、または AWS 環境外で発生するイベントの詳細を提供する必要があります。このため、多くの場合、コントロールの要件をサポートする証拠を生成できる AWS データソースはありません。

共通コントロールが手動の場合、カスタムコントロールの証拠ソースとして使用できます。唯一の違いは、共通コントロールが証拠を自動的に収集しないことです。代わりに、共通コントロールの要件をサポートするために、独自の証拠を手動でアップロードする必要があります。

手動共通コントロールに証拠を追加するには

1. カスタムコントロールを作成する
   - 手順に従って、カスタムコントロールを作成または編集します。
   - ステップ 2 で証拠ソースを指定するときは、証拠ソースとして手動の共通コントロールを選択します。
2. カスタムフレームワークを作成する
   - 手順に従って、カスタムフレームワークを作成または編集します。
   - ステップ 2 でコントロールセットを指定する場合は、新しいカスタムコントロールを含めます。
3. 評価を作成する
   - 手順に従って、カスタムフレームワークから評価を作成します。
   - この時点で、手動共通コントロールはアクティブな評価コントロールの証拠ソースになりました。
4. 手動証拠をアップロードする

- 手順に従って、評価のコントロールに手動証拠を追加します。

> **Note**
>
> 将来、より多くの AWS データソースが利用可能になるにつれて、 は共通のコントロールを更新して、コアコントロールを証拠ソースとして含め AWS る可能性があります。この場合、共通コントロールが 1 つ以上のアクティブな評価コントロールの証拠ソースである場合、これらの更新から自動的にメリットが得られます。お客様側からこれ以上セットアップする必要はなく、共通コントロールをサポートする自動証拠の収集を開始します。

証拠がさまざまな間隔で生成されており、収集頻度がわかりません

Audit Manager の評価のコントロールでは、さまざまなデータソースの組み合わせにマッピングされます。データソースごとに、証拠収集の頻度が異なります。その結果、証拠が収集される頻度に対する one-size-fits-all 回答はありません。コンプライアンスを評価するデータソースもあれば、リソースの状態をキャプチャし、コンプライアンスに関して判断することなくデータを変更するだけのデータソースもあります。

さまざまなデータソースの種類と証拠を収集する頻度の概要を以下に示します。

[Data source type]	説明	証拠収集の頻度	このコントロールが評価でアクティブになっている場合
AWS CloudTrail	特定のユーザーアクティビティを追跡します。	継続的	Audit Manager は、選択したキーワードに基づいて CloudTrail ログをフィルタリングします。処理されたログは、[ユーザーアクティビティ] の証拠にインポートされます。
AWS Security Hub	Security Hub からの検出結果を報告することにより、リソースのセキュリティ体制のスナップショット	Security Hub チェックのスケジュールに基づく (通常は約 12 時間ごと)	Audit Manager は、Security Hub から直接セキュリティ検出結果を取得します。検出結果はコンプライアンスチェックの証拠としてインポートされます。

[Data source type]	説明	証拠収集の頻度	このコントロールが評価でアクティブになっている場合
	をキャプチャします。		
AWS Config	からの結果をレポートすることで、リソースのセキュリティ体制のスナップショットを取得します AWS Config。	AWS Config ルールで定義されている設定に基づく	Audit Manager は、ルール評価を から直接取得します AWS Config。評価はコンプライアンスチェックの証拠としてインポートされます。
AWS API コール	指定された への API コールを通じて、リソース設定のスナップショットを直接取得します AWS のサービス。	毎日、毎週、または毎月	Audit Manager は、指定された頻度に基づいて API コールを行います。レスポンスは構成データ証拠としてインポートされます。

証拠収集の頻度にかかわらず、評価がアクティブである限り、新しい証拠が自動的に収集されます。詳細については、「証拠収集の頻度」を参照してください。

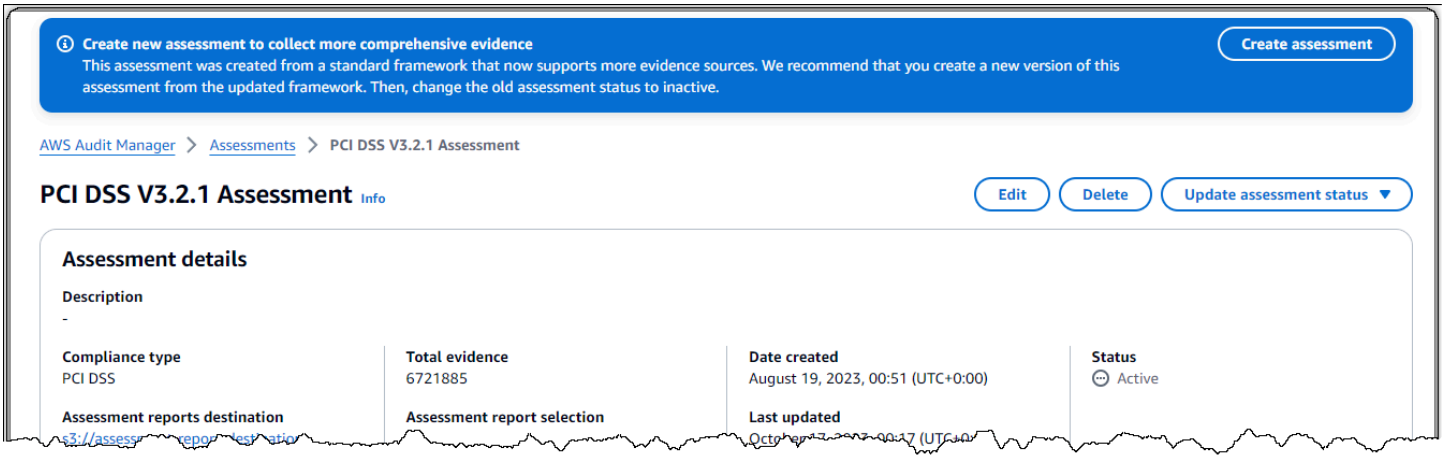
詳細については、「自動証拠でサポートされているデータソースタイプ」および「コントロールが証拠を収集する頻度の変更」を参照してください。

Audit Manager を無効にしてから再度有効にしましたが、既存の評価では証拠が収集されなくなりました

Audit Manager を無効にしてデータを削除しないことを選択すると、既存の評価は休止状態になり、証拠の収集が停止します。つまり、Audit Manager を再度有効にしても、以前に作成した評価は引き続き使用できます。ただし、証拠収集は自動的に再開はされません。

既存のアセスメントの証拠の収集を再開するには、評価を編集し、変更を加えずに保存を選択します。

評価の詳細ページで、評価を再作成するように求められます。



より包括的な証拠を収集するための新しい評価を作成するというメッセージが表示された場合は、Audit Manager が評価の作成元の標準フレームワークの新しい定義を提供するようになったことを示します。

新しいフレームワーク定義では、フレームワークのすべての標準コントロールがAWS マネージドソース から証拠を収集できるようになりました。つまり、共通コントロールまたはコアコントロールの基盤となるデータソースが更新されるたびに、Audit Manager は関連するすべての標準コントロールに同じ更新を自動的に適用します。

これらの AWS マネージドソースを活用するには、更新されたフレームワークから新しい評価を作成することをお勧めします。これを行うと、古い評価ステータスを非アクティブな に変更できます。このアクションは、新しい評価が AWS マネージドソースから入手可能な最も正確で包括的な証拠を確実に収集できるようにするのに役立ちます。何もしない場合、評価では引き続き古いフレームワークとコントロール定義を使用して、以前とまったく同じように証拠を収集します。

データソースと証拠ソースの違いは何ですか？

証拠ソースは、証拠の収集元を決定します。これは、個々のデータソースでも、コアコントロールまたは共通コントロールにマッピングされるデータソースの事前定義されたグループでもかまいません。

データソースは、最も詳細なタイプの証拠ソースです。データソースには、証拠データを収集する正確な場所を Audit Manager に伝える以下の詳細が含まれています。

- データソースタイプ (例： AWS Config)
- データソースマッピング (などの特定の AWS Config ルールなど`s3-bucket-public-write-prohibited`)

評価の作成に失敗した

アセスメントの作成に失敗した場合は、評価範囲で選択した AWS アカウント が多すぎることが原因である可能性があります。を使用している場合 AWS Organizations、Audit Manager は 1 つの評価の範囲内で最大 200 のメンバーアカウントをサポートできます。この数を超えると、評価の作成が失敗する可能性があります。回避策として、各評価の範囲内で異なるアカウントを使用して複数の評価を実行できます。

対象範囲内のアカウントを組織から削除するとどうなりますか?

範囲内のアカウントが組織から削除されると、Audit Manager は、それ以降、そのアカウントの証拠を収集しなくなります。ただし、アカウントは引き続き [AWS アカウント] タブの評価に表示されます。範囲内のアカウントのリストからアカウントを削除するには、評価を編集を実行します。削除されたアカウントは編集中にリストに表示されなくなります。また、そのアカウントが範囲に含まれていなくても変更を保存できます。

評価の対象となるサービスが表示されない

AWS のサービス タブが表示されない場合は、対象範囲内のサービスが Audit Manager によって管理されることを意味します。新しい評価を作成すると、Audit Manager はその時点から対象範囲内のサービスを管理します。

古い評価がある場合、評価でこのタブが以前に表示された可能性があります。ただし、Audit Manager は、評価からこのタブを自動的に削除し、次のいずれかのイベントが発生したときに、範囲内のサービスの管理を引き継ぎます。

- 評価を編集する
- 評価で使用されるカスタムコントロールの 1 つを編集する

Audit Manager は、評価コントロールとそのデータソースを調べ、この情報を対応する にマッピングすることで、範囲内のサービスを推測します AWS のサービス。評価の基盤となるデータソースが変更された場合、適切なサービスを反映するために、必要に応じてスコープが自動的に更新されます。これにより、評価によって AWS 、環境内のすべての関連サービスに関する正確で包括的な証拠が収集されます。

評価の範囲内のサービスを編集できません

での評価の編集 AWS Audit Manager ワークフローにサービスの編集ステップがなくなりました。これは、Audit Manager AWS のサービス が評価の対象となる を管理するようになったためです。

古い評価がある場合は、その評価の作成時に対象範囲内のサービスを手動で定義している可能性があります。ただし、これらのサービスを今後編集することはできません。Audit Manager は、次のいずれかのイベントが発生すると、評価の対象となるサービスの管理を自動的に引き継ぎます。

- 評価を編集する
- 評価で使用されるカスタムコントロールの 1 つを編集する

Audit Manager は、評価コントロールとそのデータソースを調べ、この情報を対応する にマッピングすることで、範囲内のサービスを推測します AWS のサービス。評価の基盤となるデータソースが変更された場合、適切なサービスを反映するために、必要に応じてスコープが自動的に更新されます。これにより、評価によって AWS 、環境内のすべての関連サービスに関する正確で包括的な証拠が収集されます。

サービスの対象範囲とデータソースタイプにはどのような違いがありますか?

service in scope は AWS のサービス 、評価の範囲に含まれる です。サービスが対象範囲内にある場合、Audit Manager は対象サービスとそのリソースの使用状況に関する証拠を収集します。

> **Note**
>
> Audit Manager AWS のサービス は、評価の対象となる を管理します。古い評価がある場合は、過去にスコープ内のサービスを手動で指定している可能性があります。今後は、範囲内のサービスを指定または編集することはできません。

データソースタイプは、証拠が正確にどこから収集されたかを示します。独自のエビデンスをアップロードする場合、データソースタイプは手動です。Audit Manager が証拠を収集する場合、データソースは 4 つのタイプのいずれかになります。

1. AWS Security Hub – Security Hub から検出結果を報告することで、リソースのセキュリティ体制のスナップショットを取得します。
2. AWS Config – から結果を報告することで、リソースのセキュリティ体制のスナップショットを取得します AWS Config。
3. AWS CloudTrail – リソースの特定のユーザーアクティビティを追跡します。
4. AWS API コール – 特定の への API コールを通じて、リソース設定のスナップショットを直接取得します AWS のサービス。

対象範囲のサービスとデータソースタイプの違いを説明する 2 つの例を次に示します。

例 1

例えば、4.1.2 - S3 バケットへのパブリック書き込みアクセスを許可しないという名前のコントロールの証拠を収集するとします。このコントロールは S3 バケットポリシーのアクセスレベルをチェックします。このコントロールでは、Audit Manager は特定の AWS Config ルール (s3-bucket-public-write-prohibited) を使用して S3 バケットの評価を検索します。この例では、以下のことが当てはまります。

- service in scope は Amazon S3 です
- 評価対象のリソースが S3 バケットである
- データソースタイプは です。 AWS Config
- データソースマッピングは特定の AWS Config ルールです (`s3-bucket-public-write-prohibited`)

例 2

164.308(a)(5)(ii)(C)という名前の HIPAA コントロールの証拠を収集するとします。このコントロールは、不適切なサインインを検出するためのモニタリング手順を要求します。このコントロールでは、Audit Manager は CloudTrail ログを使用して、すべての AWS マネジメントコンソールのサインインイベントを検索します。この例では、以下のことが当てはまります。

- service in scope は IAM
- 評価対象のリソースがお客様のユーザーである
- データソースタイプは です。 CloudTrail
- データソースマッピングは特定の CloudTrail イベントです (`ConsoleLogin`)

評価レポートの問題のトラブルシューティング

このページの情報を参照して、Audit Manager での一般的な評価レポートに関する問題を解決できます。

トピック

- 評価レポートの生成が失敗しました
- 上記のチェックリストに従いましたが、評価レポートを生成できませんでした

評価レポートの生成が失敗しました

評価レポートの生成が失敗した場合、いくつかの理由が考えられます。この問題のトラブルシューティングは、最もよく生じる原因を確認することから開始できます。開始するには、次のチェックリストに従います。

1. いずれかの AWS リージョン 情報が一致しないかどうかを確認します。
   a. カスタマーマネージドキー AWS リージョン の は、評価 AWS リージョン の と一致していますか？

      Audit Manager のデータ暗号化に独自の KMS キーを指定した場合、そのキーは評価 AWS リージョン と同じ にある必要があります。この問題を解決するには、KMS キーを評価と同じリージョンにあるものに変更してください。KMS キーを変更する方法については、「」を参照してくださいデータ暗号化設定の構成。

   b. カスタマーマネージドキー AWS リージョン の は S3 バケット AWS リージョン の と一致していますか？

      Audit Manager のデータ暗号化に独自の KMS キーを指定した場合、そのキーは評価レポートの宛先として使用する S3 バケット AWS リージョン と同じ にある必要があります。この問題を解決するには、KMS キーと S3 バケットのどちらかを変更して、両方が評価と同じリージョンになるようにします。KMS キーを変更する方法については、「」を参照してくださいデータ暗号化設定の構成。S3 バケットを変更する方法については、「」を参照してくださいデフォルトの評価レポートの送信先の設定。
2. 評価レポートの宛先として使用している S3 バケットの許可を確認します。
   a. 評価レポートを生成している IAM エンティティには、S3 バケットについての必要な許可がありますか?

      IAM エンティティには、そのバケットでレポートを発行するために必要な S3 バケットの許可が付与されている必要があります。ご利用いただけるサンプルポリシーが用意されています。

b. S3 バケットには、SSE-KMS を使用したサーバー側の暗号化 (SSE) を必要とするバケットポリシーがありますか?

「はい」の場合、そのバケットポリシーで使用される KMS キーは、Audit Manager のデータ暗号化設定で指定されている KMS キーと一致する必要があります。Audit Manager の設定で KMS キーを設定しておらず、S3 バケットポリシーで SSE が必要な場合は、バケットポリシーで SSE-S3 が許可されているようにしてください。KMS キーを変更する方法については、「」を参照してくださいデータ暗号化設定の構成。S3 バケットを変更する方法については、「」を参照してくださいデフォルトの評価レポートの送信先の設定。

それでも評価レポートを正常に生成できない場合は、このページで次の問題を確認してください。

上記のチェックリストに従いましたが、評価レポートを生成できませんでした

Audit Manager は、評価レポートに追加できる証拠の量を制限します。この制限は、評価 AWS リージョン の 、評価レポートの宛先として使用される S3 バケットのリージョン、および評価でカスタマー管理の を使用しているかどうかに基づきます AWS KMS key。

1. 同じリージョンのレポートの制限は 22,000 件です (S3 バケットと評価が同じ AWS リージョンにある場合)
2. クロスリージョンレポートの制限は 3,500 件です (S3 バケットと評価が異なる AWS リージョンにある場合)
3. 評価でカスタマーマネージドの KMS キーを使用する場合の制限は 3,500 件です

これよりも多くの証拠を含むレポートを生成しようとすると、操作が失敗する可能性があります。

回避策として、1 つの大きな評価レポートではなく、複数の評価レポートを生成することが考えられます。このようにすることで、評価の証拠をより管理しやすいサイズのバッチにエクスポートできます。

レポートを生成しようとすると、アクセス拒否エラーが発生します

Audit Manager の設定で指定された KMS キーが属していない委任された管理者アカウントによって評価が作成された場合、`access denied` エラーが発生します。このエラーを回避するには、Audit Manager の委任された管理者を指定するときに、委任された管理者アカウントが Audit Manager の設定時に指定した KMS キーにアクセスできることを確認してください。

評価レポートの宛先として使用している S3 バケットの書き込み許可がない場合にも、access denied エラーが発生する可能性があります。

access denied エラーが発生したら、以下の前提条件を満たしていることを確認してください。

- Audit Manager の設定の KMS キーが、委任された管理者に許可を付与していること。これを設定するには、AWS Key Management Service デベロッパーガイドの他のアカウントのユーザーに KMS キーの使用を許可するの手順に従います。Audit Manager で暗号化設定を確認および変更する方法については、「」を参照してくださいデータ暗号化設定の構成。
- 評価レポートの宛先として使用している S3 バケットへの書き込みアクセス権を付与する許可ポリシーが付与されていること。より具体的には、許可ポリシーが s3:PutObject アクションを含み、S3 バケットの ARN を指定し、評価レポートの暗号化に使用される KMS キーを含んでいること。使用できるポリシーの例については、「」を参照してください例2 (評価レポートの宛先の許可)。

> **Note**
>
> Audit Manager のデータ暗号化の設定を変更した場合、これらの変更は、今後作成する新しい評価に適用されます。ここで言う新しい評価には、新しい評価から作成する評価レポートが含まれます。
> この変更は、暗号化の設定を変更する前に作成した既存の評価には適用されません。ここで言う既存の評価には、既存の評価レポートに加え、既存の評価から作成する新しい評価レポートも含まれます。既存の評価 (およびそれらのすべての評価レポート) は、引き続き古い KMS キーを使用します。評価レポートを生成する IAM アイデンティティに、古い KMS キーを使用するための許可が付与されていない場合は、キーポリシーレベルで許可を付与できます。

評価レポートを展開できません

Windows で評価レポートを展開できない場合、ファイルパスにいくつかのネストされたフォルダまたは長い名前が含まれているため、Windows エクスプローラーで評価レポートを抽出できない可能性があります。これは、Windows のファイル命名システムでは、フォルダパス、ファイル名、およびファイル拡張子が 259 文字を超えることができないためです。このルールから逸脱すると、Destination Path Too Long エラーが発生します。

この問題を解決するには、zip ファイルを現在の場所の親フォルダに移動してみてください。その後、そこから再度展開を試みてください。または、zip ファイルの名前を短くするか、ファイルパスが短い別の場所にファイルを抽出することもできます。

レポートで証拠名を選択しても、証拠の詳細にリダイレクトされません

この問題は、ブラウザで評価レポートを操作している場合や、オペレーティングシステムにインストールされているデフォルトの PDF リーダーを使用している場合に発生することがあります。一部のブラウザおよびシステムのデフォルトの PDF リーダーでは、相対リンクを開くことができません。つまり、評価レポートの要約 PDF 内ではハイパーリンク (目次のハイパーリンクされたコントロール名など) は機能する可能性がありますが、評価サマリー PDF から別の証拠詳細 PDF に移動しようとすると、ハイパーリンクは無視されます。

この問題が発生した場合は、専用の PDF リーダーを使用して評価レポートを操作することをお勧めします。信頼性の高いエクスペリエンスを得るには、Adobe Acrobat Reader をインストールして使用することをお勧めします。このリーダーでAdobe のウェブサイトからダウンロードができます。他の PDF リーダーも使用できますが、Adobe Acrobat Reader は Audit Manager の評価レポートと一貫して確実に動作することが証明されています。

評価レポートの生成が [In progress] (進行中) のステータスのままであり、これが請求にどのように影響するかわかりません

評価レポートの生成は請求に影響しません。評価が収集した証拠に基づいてのみ請求されます。料金の詳細については、「AWS Audit Manager 料金表」を参照してください。

追加リソース

次のページには、証拠ファインダーからの評価レポートの生成に関するトラブルシューティングのガイダンスが含まれています。

- 検索結果から複数の評価レポートを生成できません
- 検索結果から特定の証拠を含めることができません
- 証拠ファインダーの結果がすべて評価レポートに含まれているわけではありません
- 検索結果から評価レポートを生成したいのですが、クエリステートメントが失敗します

コントロールとコントロールセットの問題のトラブルシューティング

このページの情報を参照して、Audit Manager での一般的なコントロールに関する問題を解決できます。

一般的な問題

- 評価にコントロールまたはコントロールセットが表示されません
- コントロールに手動証拠をアップロードできません
- コントロールに「交換可能」と表示されている場合の意味は何ですか？

AWS Config 統合の問題

- 1 つのコントロールのデータソースとして複数の AWS Config ルールを使用する必要があります
- コントロールデータソースを設定しているときは、カスタムルールオプションは使用できません
- カスタムルールオプションも使用できますが、ドロップダウンリストにルールは表示されません
- カスタムルールはいくつか使用できますが、使用したいルールが見当たりません
- 使用したいマネージドルールが表示されません
- カスタムフレームワークを共有したいが、カスタム AWS Config ルールをデータソースとして使用するコントロールがある。受信者はこれらのコントロールを収集することができますか?
- カスタムルールが AWS Configで更新されるとどうなりますか? Audit Manager で何かアクションを実行する必要がありますか?

評価にコントロールまたはコントロールセットが表示されません

簡単に述べると、評価のコントロールを表示するには、ユーザーは、その評価の監査所有者として指定される必要があります。さらに、関連する Audit Manager リソースを表示および管理するために必要な IAM 許可が必要です。

評価のコントロールにアクセスする必要がある場合は、その評価について、自分を監査所有者として指定するよういずれかの監査所有者に依頼します。評価を作成または編集するときに、監査所有者を指定できます。

また、評価を管理するために必要な許可が付与されていることも確認してください。監査所有者は AWSAuditManagerAdministratorAccessポリシーを使用することをお勧めします。IAM 許可につい

てサポートが必要な場合は、管理者または AWS Support までお問い合わせください。IAM アイデンティティにポリシーをアタッチする方法の詳細については、IAM ユーザーガイドの「ユーザーへの許可の追加」および「IAM アイデンティティ許可の追加と削除」を参照してください。

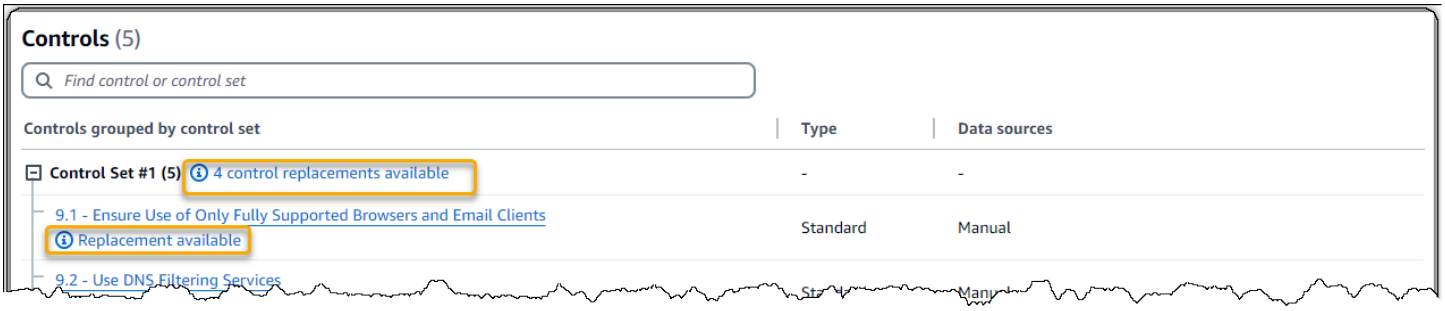
コントロールに手動証拠をアップロードできません

コントロールに証拠を手動でアップロードできない場合は、コントロールのステータスが [inactive] (非アクティブ) であることが原因である可能性があります。

手動証拠をコントロールにアップロードするには、最初にコントロールのステータスを [Under review] (レビュー中) または [Reviewed] (レビュー済み) に変更する必要があります。手順については、「での評価コントロールのステータスの変更 AWS Audit Manager」を参照してください。

> **Important**
>
> 各 AWS アカウント は、1 日あたり最大 100 個の証拠ファイルをコントロールに手動でアップロードできます。この 1 日あたりのクォータを超えると、そのコントロールについては追加の手動アップロードが失敗します。単一のコントロールに手動証拠を大量にアップロードする必要がある場合は、証拠を数日にわたってバッチでアップロードします。

コントロールに「交換可能」と表示されている場合の意味は何ですか？



このメッセージが表示された場合は、カスタムフレームワークの 1 つ以上の標準コントロールで更新されたコントロール定義が使用可能であることを意味します。Audit Manager が提供する改善された証拠ソースを活用できるように、これらのコントロールを置き換えることをお勧めします。

手順については、「」を参照してくださいカスタムフレームワークの詳細ページで、カスタムフレームワークを再作成するように求められます。。

1 つのコントロールのデータソースとして複数の AWS Config ルールを使用する必要があります

マネージドルールとカスタムルールを組み合わせて 1 つのコントロールに使用できます。これを行うには、コントロールに複数の証拠ソースを定義し、それぞれに優先するルールタイプを選択します。1 つのカスタムコントロールに対して最大 100 のカスタマーマネージドデータソースを定義できます。

コントロールデータソースを設定しているときは、カスタムルールオプションは使用できません

つまり、自分の AWS アカウント または組織のカスタムルールを表示するためのアクセス権限がないことを意味します。具体的には、Audit Manager コンソールでDescribeConfigRulesオペレーションを実行するアクセス許可はありません。

この問題を解決するには、 AWS 管理者にお問い合わせください。ご自身が AWS 管理者の場合は、IAM ポリシーを管理することでユーザーまたはグループにアクセス権限を付与できます。

カスタムルールオプションも使用できますが、ドロップダウンリストにルールは表示されません

つまり、ご自身の AWS アカウント や組織ではカスタムルールが有効になっておらず、使用できないことを意味します。

にまだカスタムルールがない場合は AWS Config、作成できます。手順については、AWS Config デベロッパーガイドの AWS Config カスタム ルール を参照してください。

カスタムルールが表示されることが予想される場合は、次のトラブルシューティング項目を確認してください。

カスタムルールはいくつか使用できますが、使用したいルールが見当たりません

目的のカスタムルールが表示されない場合は、次のいずれかの問題が原因である可能性があります。

アカウントがルールから除外されています

使用している委任管理者アカウントがルールから除外されている可能性があります。

組織の管理アカウント (または委任された管理者アカウントの 1 つ) は、 AWS Config AWS Command Line Interface () を使用してカスタム組織ルールを作成できますAWS CLI。その際、ルールから除外するアカウントのリストを指定できます。アカウントがこのリストに含まれている場合、ルールは Audit Manager では使用できません。

この問題を解決するには、 AWS Config 管理者にお問い合わせください。 AWS Config 管理者の場合は、 put-organization-config-rule コマンドを実行して除外されたアカウントのリストを更新できます。

ルールが正常に作成されず、 AWS Configで有効になりませんでした

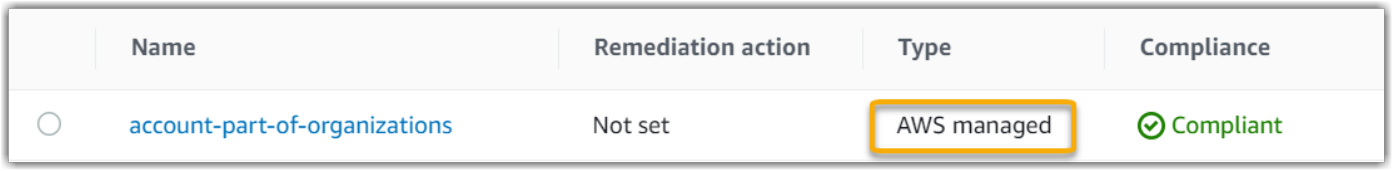
カスタムルールが正常に作成および有効化されなかった可能性もあります。ルールの作成時にエラーが発生した場合、またはルールが有効になっていない場合、そのルールは Audit Manager の使用可能なルールのリストに表示されません。

この問題については、 AWS Config 管理者に問い合わせることをお勧めします。

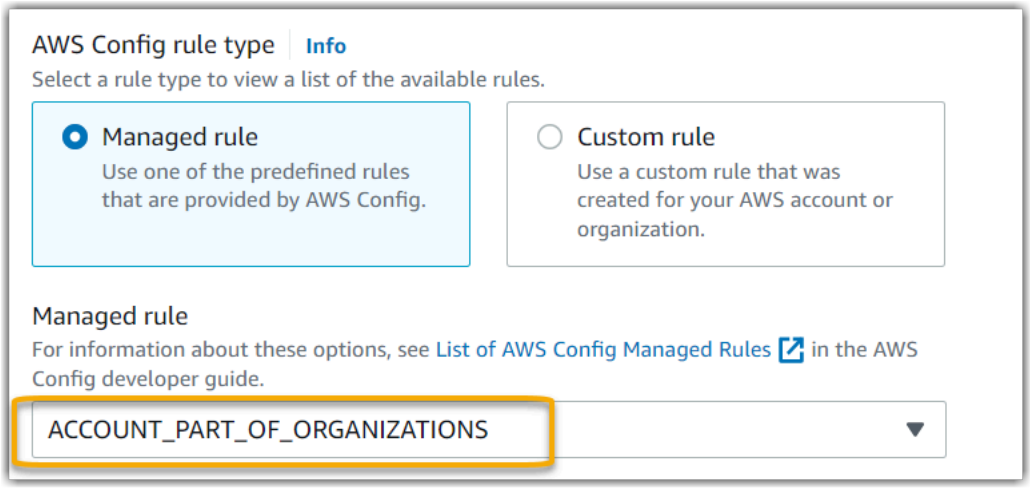
このルールはマネージドルールです

探しているルールがカスタムルールのドロップダウンリストに見つからない場合は、そのルールがマネージドルールである可能性があります。

AWS Config コンソールを使用して、ルールがマネージドルールであるかどうかを確認できます。そのためには、左側のナビゲーションメニューでルールを選択し、表でルールを探します。ルールがマネージドルールの場合、タイプ列にはAWS マネージドと表示されます。

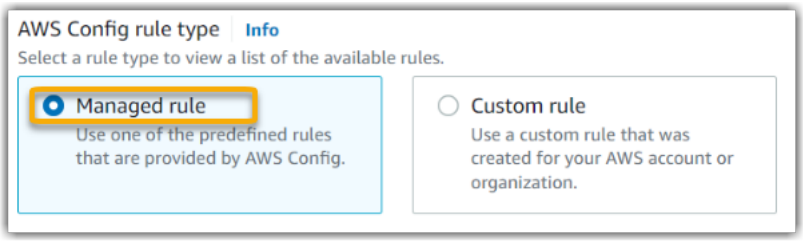


マネージドルールであることを確認したら、Audit Manager に戻り、ルールタイプとしてマネージドルールを選択します。次に、マネージドルールのドロップダウンリストでマネージドルール識別子のキーワードを探します。



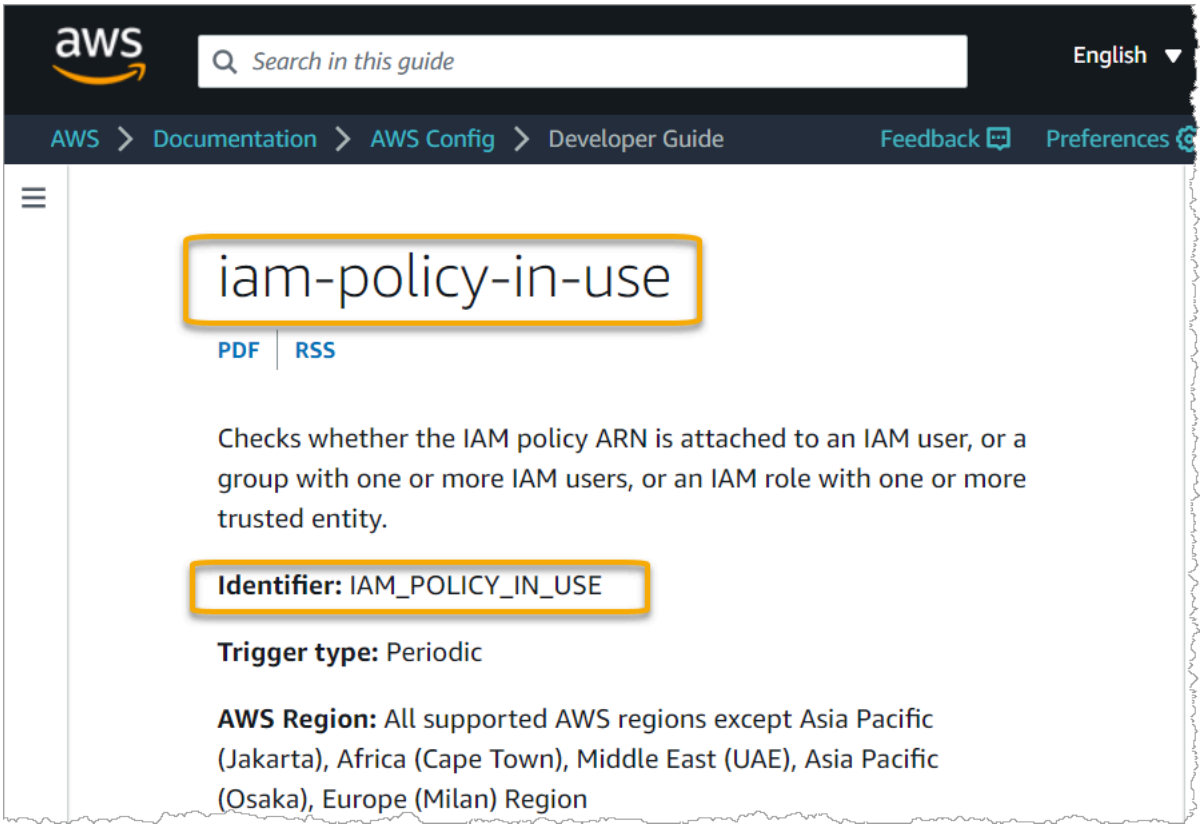
使用したいマネージドルールが表示されません

Audit Manager コンソールのドロップダウンリストからルールを選択する前に、ルールタイプとしてマネージドルールを選択したことを確認してください。

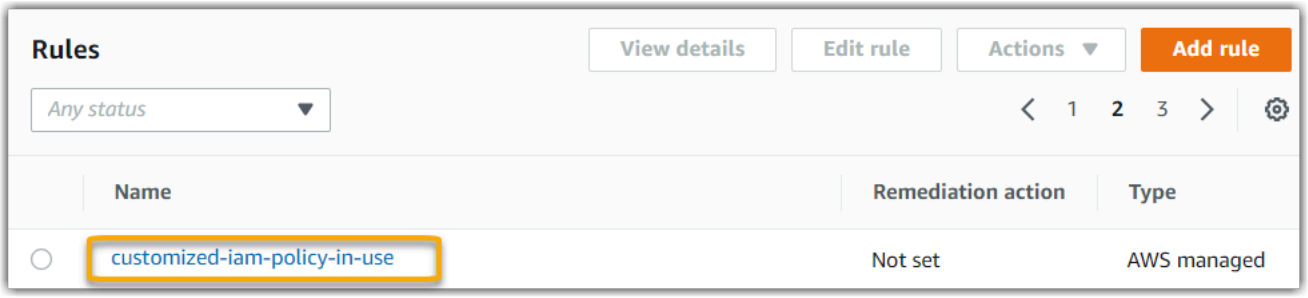


それでも期待していたマネージドルールが表示されない場合は、ルール名を探している可能性があります。代わりに、ルール識別子を探す必要があります。

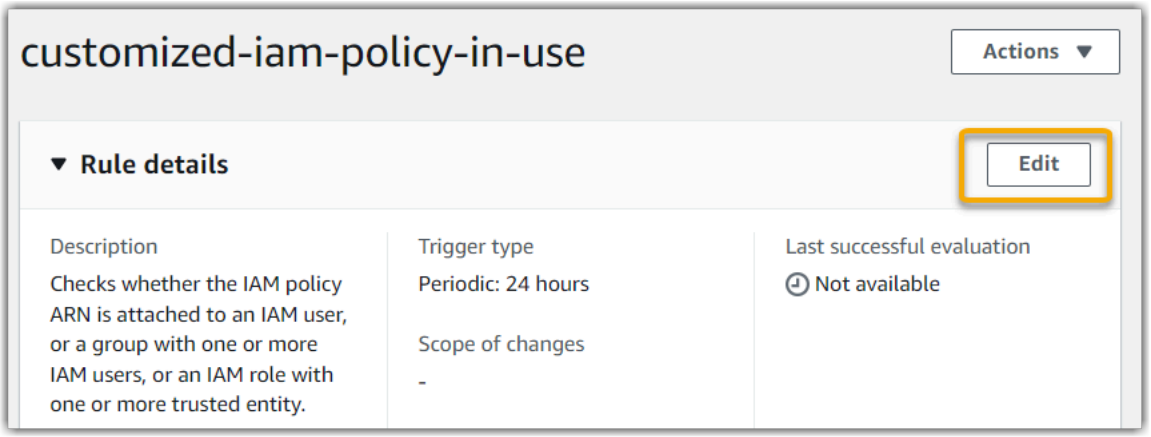
デフォルトのマネージドルールを使用している場合、名前と識別子は似ています。名前は小文字で、ダッシュが使用されています (例: `iam-policy-in-use`)。識別子は大文字で、アンダースコアが使用されます (例: `IAM_POLICY_IN_USE`)。デフォルトのマネージドルールの識別子を見つけるには、サポートされている AWS Config マネージドルールキーワードのリストを確認し、使用するルールのリンクに従います。これにより、そのマネージドルールの AWS Config ドキュメントが表示されます。ここから、名前と識別子の両方を確認できます。「Audit Manager」のドロップダウンリストで識別キーワードを探します。



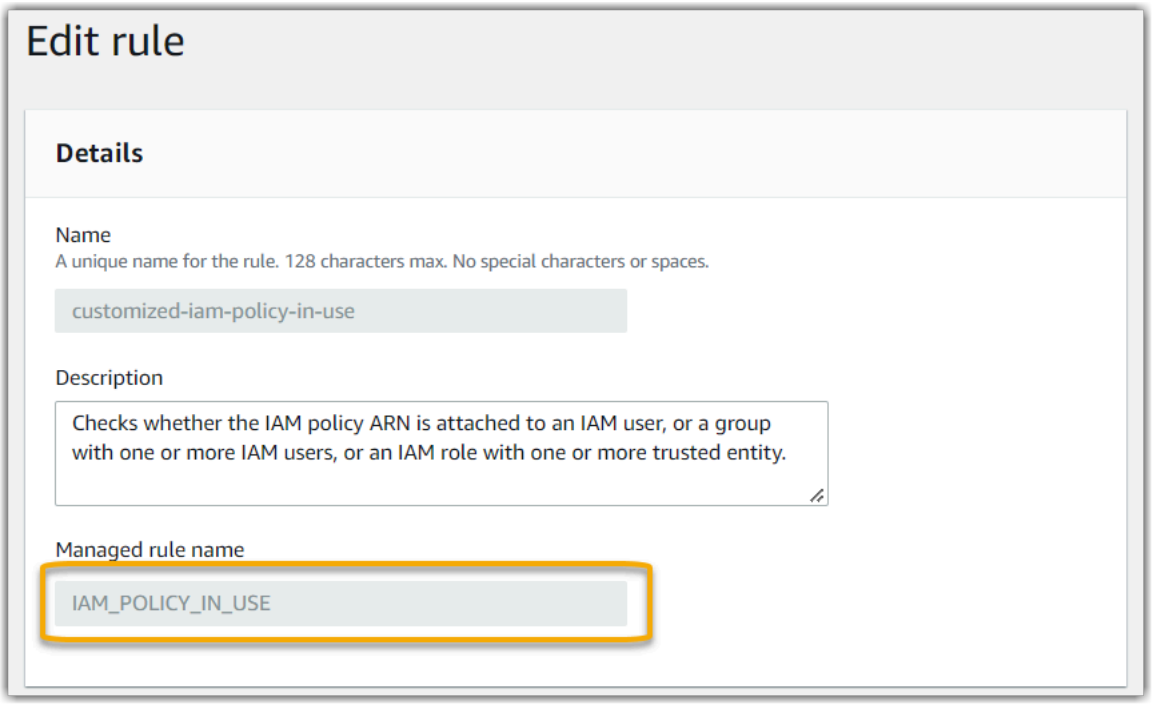
カスタムマネージドルールを使用している場合は、AWS Config コンソールを使用してルール識別子を検索できます。例えば、`customized-iam-policy-in-use`というマネージドルールを使用するとします。このルールの識別子を見つけるには、 AWS Config コンソールに移動し、左側のナビゲーションメニューでルールを選択し、テーブルでルールを選択します。



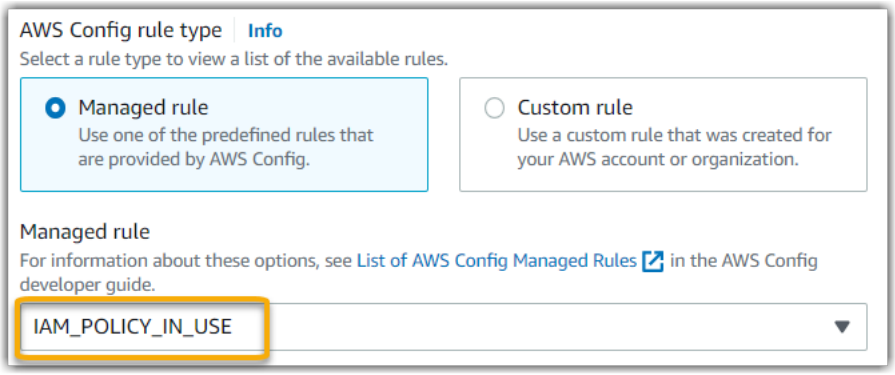
編集を選択すると、マネージドルールの詳細が開きます。



詳細セクションで、マネージドルールの作成元のソース識別子 (IAM_POLICY_IN_USE) を見つけることができます。



これで Audit Manager コンソールに戻り、ドロップダウンリストから同じ識別子キーワードを選択できます。



カスタムフレームワークを共有したいが、カスタム AWS Config ルールをデータソースとして使用するコントロールがある。受信者はこれらのコントロールを収集することができますか?

はい、受信者はこれらのコントロールの証拠を収集できますが、そのためにはいくつかの手順が必要です。

Audit Manager が AWS Config ルールをデータソースマッピングとして使用して証拠を収集するには、次の条件が満たされている必要があります。これは、マネージドルールとカスタムルールの両方に当てはまります。

1. ルールは受信者の AWS 環境に存在する必要があります
2. ルールは受信者の AWS 環境で有効にする必要があります

アカウントのカスタム AWS Config ルールが受信者の AWS 環境にまだ存在しない可能性があることに注意してください。さらに、受信者が共有リクエストを受け入れるとき、Audit Manager は受信者のアカウントにカスタムルールを再作成しません。受信者がデータソースマッピングとしてカスタムルールを使用して証拠を収集するには、 のインスタンスに同じカスタムルールを作成する必要があります AWS Config。受信者がルールを作成して有効にすると、Audit Manager はそのデータソースから証拠を収集できます。

受信者に連絡して、 AWS Configのインスタンスでカスタムルールを作成する必要があるかどうかを知らせることをお勧めします。

カスタムルールが AWS Configで更新されるとどうなりますか? Audit Manager で何かアクションを実行する必要がありますか?

AWS 環境内のルール更新の場合

AWS 環境内のカスタムルールを更新する場合、Audit Manager でアクションは必要ありません。Audit Manager は、次の表で説明されているように、ルールの更新を検出して処理します。Audit Manager は、ルールの更新が検出されても通知しません。

シナリオ	Audit Manager の機能	必要な作業
のインスタンスでカスタムルールが更新されます。 AWS Config	Audit Manager は、更新されたルール定義を使用して、そのルールに関する検出結果を引き続き報告します。	アクションは不要です。
のインスタンスでカスタムルールが削除されます AWS Config	Audit Manager は、削除されたルールに関する検出結果の報告を停止します。	アクションは不要です。 必要に応じて、削除されたルールをデータソースマッピングとして使用していたカスタムコントロールを編集することができます。これにより、削除されたルールが取り除かされ、データ ソース設定が整理されます。そうしない場合、削除されたルール名は未使用のデータソースマッピングとして残ります。

AWS 環境外のルール更新の場合

カスタムルールが AWS 環境外で更新された場合、Audit Manager はルールの更新を検出しません。共有カスタムフレームワークを使用している場合は、この点を考慮する必要があります。これは、このシナリオでは、送信者と受信者がそれぞれ別々の AWS 環境で作業するためです。次の表は、このシナリオの推奨アクションを示しています。

役割	シナリオ	推奨されるアクション
送信者	• カスタムルールをデータソースマッピングとして使用するフレームワークを共有しました。	受信者に更新内容を知らせてください。そうすれば、受信者は同じ更新を

役割	シナリオ	推奨されるアクション
	• フレームワークを共有した後、 でこれらのルールのいずれかを更新または削除しました AWS Config。	適用し、最新のルール定義と同期した状態を保つことができます。
受取人	• カスタムルールをデータソースマッピングとして使用する共有フレームワークを受け入れました。 • のインスタンスでカスタムルールを再作成すると AWS Config、送信者はそれらのルールの 1 つを更新または削除します。	AWS Configのインスタンスで、対応するルールを更新してください。

ダッシュボードに関する問題のトラブルシューティング

このページの情報を参照して、Audit Manager での一般的なダッシュボードの問題を解決できます。

トピック

ダッシュボードにデータがありません

日次スナップショット ウィジェット内の数字にハイフン (-) が表示されている場合は、使用可能なデータがないことを示します。ダッシュボードにデータを表示するには、少なくとも 1 つのアクティブな評価が必要です。使用を開始するには、評価を作成します。24 時間後から、評価データがダッシュボードに表示され始めます。

> **Note**
>
> 日次スナップショットウィジェットの数値にゼロ (0) が表示されている場合、これは、アクティブな評価 (または選択した評価) に非準拠の証拠がないことを示しています。

評価のダッシュボードデータが表示されなくなりました

Audit Manager は、古いバージョンの標準フレームワークを使用して作成された評価のダッシュボードデータを表示しません。この問題を解決するには、標準フレームワークの最新バージョンから評価を再作成します。

Audit Manager が 2024 年 6 月 6 日に共通コントロールライブラリを起動したとき、すべての標準フレームワークが更新されました。新しいフレームワーク定義では、フレームワークのすべての標準コントロールが から証拠AWS managed sourceを収集できるようになりました。つまり、共通コントロールまたはコアコントロールの基盤となるデータソースが更新されるたびに、Audit Manager は関連するすべての標準コントロールに同じ更新を自動的に適用します。

これらのデータソースマッピングが自動的に更新されるたびに、新しい評価を作成する必要はありません。新しい評価の作成は 1 回限りのアクティビティであり、一般的なコントロールの起動後に完了することをお勧めします。

ダッシュボードのインサイトデータを表示するには、標準フレームワークの更新バージョンから新しい評価を作成します。新しい評価が作成されたら、古い評価のステータスを非アクティブな に変更できます。

CSV のダウンロードオプションが使用できません

このオプションは、個別の評価でのみ使用できます。ダッシュボードに 評価フィルター を適用したことを確認してから、再試行してください。一度にダウンロードできる CSV ファイルは 1 つだけであることに注意してください。

CSV ファイルのダウンロードを試みても、ダウンロードしたファイルが表示されません

コントロールドメインに多数のコントロールが含まれている場合、Audit Manager が CSV ファイルを生成するまでに少し時間がかかることがあります。ファイルが生成されると、自動的にダウンロードされます。

それでもダウンロードしたファイルが表示されない場合は、インターネット接続が正常に機能しており、最新バージョンのウェブブラウザを使用していることを確認してください。さらに、最近のダウンロードフォルダを確認します。ファイルは、ブラウザによって決定されるデフォルトの場所にダウンロードされます。それでも問題が解決しない場合は、別のブラウザを使用してファイルのダウンロードを試みてください。

特定のコントロールまたはコントロールドメインがダッシュボードにありません

これは、アクティブな評価 (または指定された評価) に、そのコントロールまたはコントロールドメインに関連するデータがないことを意味している可能性があります。

コントロールドメインは、次の 2 つの基準の両方が満たされた場合にのみダッシュボードに表示されます。

- アクティブな評価 (または指定された評価) に、そのドメインに関連するコントロールが少なくとも 1 つ含まれています
- そのドメイン内の少なくとも 1 つのコントロールが、ダッシュボードの上部に表示されている日付に証拠を収集しました

コントロールは、ダッシュボードの上部にある日付に証拠を収集した場合にのみ、ドメイン内に表示されます。

毎日のスナップショットには、日によって異なる量の証拠が示されます。これは正常ですか?

すべての証拠が毎日収集されるわけではありません。Audit Manager の評価のコントロールは、さまざまなデータソースにマッピングされており、それぞれの証拠収集スケジュールが異なっていることがあります。その結果、日々のスナップショットの証拠の量は、各日において異なることが想定されます。詳細については、「証拠収集の頻度」を参照してください。

委任された管理者と AWS Organizations 問題のトラブルシューティング

このページの情報を参照して、Audit Manager での委任された管理者に関する問題を解決できます。

トピック

委任された管理者アカウントで Audit Manager を設定できません

では複数の委任された管理者がサポートされていますが AWS Organizations、Audit Manager では委任された管理者は 1 人しか許可されません。Audit Manager で複数の委任された管理者を指定しようとすると、次のエラーメッセージが表示されます。

- コンソール: `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`

Audit Manager で委任された管理者として使用する個別のアカウントを 1 つ選択します。委任された管理者アカウントを最初に Organizations に登録してから、Audit Manager で委任された管理者と同じアカウントを追加してください。

評価を作成しても、[Accounts in scope] (対象アカウント) の下に組織のアカウントが表示されません

Audit Manager の評価に組織の複数のアカウントを含める場合は、委任された管理者を指定する必要があります。

Audit Manager の委任された管理者アカウントを設定したことを確認してください。手順については、「委任された管理者の追加」を参照してください。

留意すべきいくつかの問題:

- Audit Manager では AWS Organizations 、管理アカウントを委任された管理者として使用することはできません。
- 複数の で Audit Manager を有効にする場合は AWS リージョン、リージョンごとに委任管理者アカウントを個別に指定する必要があります。Audit Manager の設定で、すべてのリージョンで同じ委任された管理者アカウントを指定します。
- 委任された管理者を指定する際には、委任された管理者アカウントが、Audit Manager の設定時に指定した KMS キーにアクセスできることを確認してください。暗号化設定を確認および変更する方法については、「」を参照してくださいデータ暗号化設定の構成。

委任された管理者アカウントを使用して評価レポートを生成しようとすると、アクセス拒否エラーが発生します

Audit Manager の設定で指定された KMS キーが属していない委任された管理者アカウントによって評価が作成された場合、`access denied` エラーが発生します。このエラーを回避するには、Audit Manager の委任された管理者を指定するときに、委任された管理者アカウントが Audit Manager の設定時に指定した KMS キーにアクセスできることを確認してください。

評価レポートの宛先として使用している S3 バケットの書き込み許可がない場合にも、`access denied` エラーが発生する可能性があります。

`access denied` エラーが発生したら、以下の前提条件を満たしていることを確認してください。

- Audit Manager の設定の KMS キーが、委任された管理者に許可を付与していること。これを設定するには、AWS Key Management Service デベロッパーガイドの他のアカウントのユーザーに KMS キーの使用を許可するの手順に従います。Audit Manager で暗号化設定を確認および変更する方法については、「」を参照してくださいデータ暗号化設定の構成。
- 評価レポートの宛先への書き込みアクセス権を付与する許可ポリシーがあること。より具体的には、許可ポリシーが `s3:PutObject` アクションを含み、S3 バケットの ARN を指定し、評価レポートの暗号化に使用される KMS キーを含んでいること。使用できるポリシーの例については、「」を参照してください例2 (評価レポートの宛先の許可)。

> **Note**
>
> Audit Manager のデータ暗号化の設定を変更した場合、これらの変更は、今後作成する新しい評価に適用されます。ここで言う新しい評価には、新しい評価から作成する評価レポートが含まれます。

この変更は、暗号化の設定を変更する前に作成した既存の評価には適用されません。ここで言う既存の評価には、既存の評価レポートに加え、既存の評価から作成する新しい評価レポートも含まれます。既存の評価 (およびそれらのすべての評価レポート) は、引き続き古い KMS キーを使用します。評価レポートを生成する IAM アイデンティティに、古い KMS キーを使用するための許可が付与されていない場合は、キーポリシーレベルで許可を付与できます。

メンバーアカウントを組織からリンク解除すると、Audit Manager はどうなりますか?

メンバーアカウントを組織からリンク解除すると、Audit Manager はこのイベントに関する通知を受け取ります。その後、Audit Manager は既存の評価の範囲リスト内のアカウントからその AWS アカウント を自動的に削除します。今後新しい評価の範囲を指定すると、リンクされていないアカウントは対象となる AWS アカウントのリストに表示されなくなります。

Audit Manager が評価の範囲リスト内のアカウントからリンクされていないメンバーアカウントを削除しても、この変更は通知されません。さらに、リンクされていないメンバーアカウントには、そのアカウントで Audit Manager が有効でなくなったことは通知されません。

メンバーアカウントを自分の組織に再リンクするとどうなりますか?

メンバーアカウントを組織に再リンクしても、そのアカウントは既存のAudit Manager 評価の範囲には自動的に追加されません。ただし、評価の範囲内でアカウント AWS アカウント を指定すると、再リンクされたメンバーアカウントが 対象として表示されるようになりました。

- 既存の評価については、評価範囲を手動で編集して、再リンクされたメンバーアカウントを追加できます。手順については、「ステップ 2: 範囲内 AWS アカウント で を編集する」を参照してください。
- 新しい評価では、評価の設定中に再リンクされたアカウントを追加できます。手順については、「ステップ 2: 範囲内 AWS アカウント で を指定する」を参照してください。

メンバーアカウントをある組織から別の組織に移行するとどうなりますか?

メンバーアカウントで組織 1 でAudit Manager が有効になってから組織 2 に移行した場合、その結果、組織 2 ではAudit Manager が有効になりません。

証拠ファインダーの問題のトラブルシューティング

このページの情報を使用して、Audit Manager での一般的な証拠収集の問題を解決できます。

証拠ファインダーに関する一般的な問題

- 証拠ファインダーを有効にできません
- 証拠ファインダーを有効にしたが、検索結果に過去の証拠が表示されない
- 証拠ファインダーを無効にできません
- 検索クエリが失敗しました

証拠ファインダーの評価レポートの問題

- 検索結果から複数の評価レポートを生成できません
- 検索結果から特定の証拠を含めることができません
- 証拠ファインダーの結果がすべて評価レポートに含まれているわけではありません
- 検索結果から評価レポートを生成したいのですが、クエリステートメントが失敗します
- 追加リソース

証拠ファインダー CSV エクスポートの問題

- CSV をエクスポートできませんでした
- 検索結果から特定の証拠をエクスポートできません
- 複数の CSV ファイルを一度にエクスポートできません

証拠ファインダーを有効にできません

証拠ファインダーを有効にできない一般的な理由には、次のような状況があります。

権限がありません

> 証拠ファインダーを初めて有効にする場合は、証拠ファインダー を有効にするために必要なアクセス許可があることを確認してください。これらのアクセス許可により、証拠ファインダー検索クエリをサポートするために必要なイベントデータストアを CloudTrail Lake で作成および管理できます。この権限により、証拠ファインダーで検索クエリを実行することもできます。

アクセス許可に関するヘルプが必要な場合は、 AWS 管理者にお問い合わせください。 AWS 管理者の場合は、必要なアクセス許可ステートメントをコピーし、IAM ポリシー にアタッチできます。

組織の管理アカウントの使用

管理アカウントを使用して証拠ファインダーを有効にすることはできませんので、ご注意ください。委任管理者アカウントとしてサインインし、再試行してください。

以前に証拠ファインダーを無効にした

現在、証拠ファインダーの再有効化には対応されません。以前に証拠ファインダーを無効にした場合は、再度有効にすることはできません。

証拠ファインダーを有効にしたが、検索結果に過去の証拠が表示されない

証拠ファインダーを有効にすると、過去の証拠データがすべて利用可能になるまでに最大 7 日かかります。

この 7 日間、イベントデータストアに過去 2 年分の証拠データがバックフィルされます。つまり、有効にした直後に証拠ファインダーを使用しても、バックフィルが完了するまですべての結果が表示されるわけではありません。

データバックフィルのステータスを確認する方法については、「」を参照してください証拠ファインダーのステータスの確認。

証拠ファインダーを無効にできません

これは、次のいずれかの理由によって発生する可能性があります。

権限がありません

証拠ファインダーを無効にする場合は、証拠ファインダー を無効にするために必要なアクセス許可があることを確認してください。これらのアクセス許可により、証拠ファインダーを無効にするために必要な Lake の CloudTrailイベントデータストアを更新および削除できます。

アクセス許可に関するヘルプが必要な場合は、 AWS 管理者にお問い合わせください。 AWS 管理者の場合は、必要なアクセス許可ステートメントをコピーし、IAM ポリシー にアタッチできます。

証拠ファインダーを有効にするリクエストはまだ進行中

証拠ファインダーの有効化をリクエストすると、証拠ファインダーのクエリをサポートするイベントデータストアが作成されます。イベントデータストアの作成中は、証拠ファインダーを無効にすることはできません。

続行するには、イベントデータストアが作成されてから、もう一度試してください。詳細については、「証拠ファインダーのステータスの確認」を参照してください。

証拠ファインダーを無効にするリクエストを既に行っています

証拠ファインダーの無効化をリクエストすると、証拠ファインダーのクエリに使用されていたイベントデータストアが削除されます。イベントデータストアの削除中に証拠ファインダーを再度無効にしようとすると、エラーメッセージが表示されます。

この場合、アクションは不要です。イベントデータストアが削除されるまでお待ちください。これが完了すると、証拠ファインダーはすぐに無効になります。詳細については、「証拠ファインダーのステータスの確認」を参照してください。

検索クエリが失敗しました

検索クエリが失敗する場合は、次のいずれかの理由が考えられます。

権限がありません

ユーザーが検索クエリの実行と検索結果へのアクセスに必要な権限を持っていることを確認してください。具体的には、以下の CloudTrail アクションに対するアクセス許可が必要です。

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

アクセス許可に関するヘルプが必要な場合は、 AWS 管理者にお問い合わせください。 AWS 管理者の場合は、必要なアクセス許可ステートメントをコピーし、IAM ポリシー にアタッチできます。

実行しているクエリの数が最大数です。

一度に最大 5 つのクエリを実行できます。同時に実行するクエリの数が最大数に達すると、`MaxConcurrentQueriesException`エラーになります。このエラーメッセージが表示され

る場合は、いくつかのクエリが終了するまでしばらくお待ちください。 その後、クエリを再実行してください。

クエリステートメントに検証エラーがあります

API または CLI を使用して CloudTrail Lake StartQueryオペレーションを実行する場合は、 が有効queryStatementであることを確認してください。クエリステートメントに検証エラー、不正な構文、サポートされていないキーワードがある場合は、InvalidQueryStatementExceptionという結果になります。

クエリの記述についての詳細は、AWS CloudTrail ユーザーガイドのクエリの作成または編集を参照してください。

有効な構文の例については、Audit Manager イベントデータストアへのクエリに使用できる次のクエリステートメントの例を参照してください。

例 1: 証拠とそのコンプライアンス状況を調査する

この例では、指定された日付範囲内で、アカウント内のすべての評価にわたってコンプライアンスステータスを持つ証拠を検索します。

```
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'
```

例 2: コントロールの非準拠証拠を特定する

この例では、特定の評価とコントロールについて、指定された日付範囲内のすべての非準拠証拠を検索します。

```
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')
```

例 3: 証拠を名前で数える

この例では、指定された日付範囲内で、評価の証拠の総数を名前でグループ化し、証拠数の順に一覧表示します。

```
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
```

例 4: データソースとサービスごとに証拠を調べる

この例では、特定のデータソースとサービスについて、指定された日付範囲内のすべての証拠を検索します。

```
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')
```

例 5: データソースとコントロールドメインごとに準拠している証拠を調べる

この例では、AWS Config ではないデータソースから証拠が得られる、特定の制御ドメインの準拠証拠を検索します。

```
 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')
```

その他の API 例外

StartQuery API は、他のいくつかの理由で失敗することがあります。考えられるエラーと説明の完全なリストについては、 API リファレンスのStartQuery 「エラー」を参照してください。 AWS CloudTrail

検索結果から複数の評価レポートを生成できません

このエラーは、同時に実行する CloudTrail Lake クエリが多すぎることが原因です。

このエラーは、検索結果をグループ化し、グループ化された結果の各項目の評価レポートをすぐに生成しようとした場合に発生する可能性があります。検索結果を取得して評価レポートを生成すると、各アクションによってクエリが呼び出されます。一度に実行できるクエリは最大 5 つまでです。同時に実行するクエリの数が最大数に達すると、MaxConcurrentQueriesException エラーが返されます。

このエラーを防ぐには、一度に生成する評価レポートの数が多すぎないようにしてください。同時に実行するクエリの数が最大数に達すると、MaxConcurrentQueriesException工ラーが返されます。このエラーメッセージが表示される場合は、進行中の評価レポートが完成するまで数分お待ちください。

Audit Manager コンソールのダウンロードセンターページから、評価レポートのステータスを確認できます。レポートが完成したら、証拠ファインダーでグループ化された結果に戻ります。その後、引き続き結果を取得し、各項目の評価レポートを生成できます。

検索結果から特定の証拠を含めることができません

検索結果はすべて評価レポートに含まれます。検索結果のセットから個々の行を選択して追加することはできません。

特定の検索結果のみを評価レポートに含めたい場合は、現在の検索フィルターを編集することをお勧めします。この方法により、レポートに含める証拠のみを対象とするように結果を絞り込むことができます。

証拠ファインダーの結果がすべて評価レポートに含まれているわけではありません

評価レポートを生成する場合、追加できる証拠の量には制限があります。この制限は、評価 AWS リージョン の 、評価レポートの宛先として使用される S3 バケットのリージョン、および評価でカスタマー管理の を使用しているかどうかに基づきます AWS KMS key。

1. 同じリージョンのレポートの制限は 22,000 件です (S3 バケットと評価が同じ AWS リージョンにある場合)
2. クロスリージョンレポートの制限は 3,500 件です (S3 バケットと評価が異なる AWS リージョンにある場合)
3. 評価でカスタマーマネージドの KMS キーを使用する場合の制限は 3,500 件です

この制限を超えた場合でも、レポートは作成されます。ただし、Audit Manager がレポートに追加するのは、最初の 3,500 件または 22,000 件の証拠項目だけです。

この問題を防ぐには、現在の検索フィルターを編集することをお勧めします。この方法では、対象とする証拠の量を減らすことで、検索結果を絞り込むことができます。必要に応じて、この方法を繰り返して、1 つの大きなレポートの代わりに複数の評価レポートを生成できます。

検索結果から評価レポートを生成したいのですが、クエリステートメントが失敗します

CreateAssessmentReport API を使用していて、クエリステートメントが検証例外を返す場合は、次の表で修正方法のガイダンスを確認してください。

> **Note**
>
> クエリステートメントが で機能する場合でも CloudTrail、同じクエリが Audit Manager での評価レポートの生成に有効でない可能性があります。これは、2 つのサービスのクエリの検証に多少の違いがあるためです。

句	問題	ソリューション	メモ
`SELECT`	SELECT句には列名が含まれています	`SELECT` 句を削除し、`SELECT eventJson` に置き換えます。	`SELECT eventJson` のみサポートされています。 この検証はAudit Manager によって処理されます。
`FROM`	FROM句には無効なイベントデータストア ID が含まれています または 指定されたイベントデータストア ID は、Audit Manager 設定のイベントデータストア ID と一致しません	`FROM` 句を削除して`FROM` *`edsID`*に置き換えます。この場合、`edsID`の値は Audit Manager 設定で指定されているイベントデータストア ID と一致します。 イベントデータストアの ARN は、Audit Manager の設定から取得できます。詳細については、 API リファレンスGetSettingsの「」を参照してください。AWS Audit Manager	この検証はAudit Manager によって処理されます。
`GROUP BY`	クエリ内に`GROUP BY`句が存在します	`GROUP BY` 句を削除してください。	この検証はAudit Manager によって処理されます。

句	問題	ソリューション	メモ
HAVING	クエリ内にHAVING句が存在します	HAVING 句を削除してください。	この検証はAudit Manager によって処理されます。
LIMIT	LIMIT句に最大許容値を超える値が含まれています	LIMIT句が存在する場合は、その値がサポートされている最大制限以下であることを確認してください。 • 同じリージョンレポートの場合、上限は 22,000 件です • クロスリージョンレポートの場合、上限は 3,500 件です • 関連する評価がカスタマー管理の を使用するレポートの場合 AWS KMS key、制限は 3,500 です。	コンソールでは、返される証拠結果の数に制限はありません。ただし、評価レポートを生成する場合、含めることができる証拠の量には制限があります。 クエリステートメントにLIMIT値が指定されていない場合は、デフォルトの最大制限が適用されます。 この検証はAudit Manager によって処理されます。
ORDER BY	ORDER BY句に、SELECT句に存在しない集計関数またはエイリアスが含まれています	集計関数やエイリアスを使用する条件がORDER BY句に含まれていないことを確認してください。	この検証は API によって処理されます CloudTrail StartQuery 。

句	問題	ソリューション	メモ
WHERE	WHERE句には 1 つ以上のassessmentId が含まれています または WHERE句に、createAssessmentReport リクエストのassessmentId と一致しないassessmentId が含まれています または WHERE句に対応されない列名が含まれています	評価 ID が 1 つだけ指定されていることと、createAssessmentReport API リクエストで指定した評価 ID パラメータと一致することを確認してください。 対応されない列名を削除します。	この検証は CloudTrail StartQuery API によって処理されます。

例

次の例は、 CreateAssessmentReportオペレーションを呼び出すときに queryStatementパラメータを使用する方法を示しています。これらのクエリを使用する前に、############を独自のedsIdおよびassessmentId値に置き換えてください。

例 1: レポートを作成する (同じリージョンの制限が適用されます)

この例では、2022 年 1 月 22 日 ~ 23 日の間に作成された S3 バケットの結果を含むレポートを作成します。

```
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
```

例 2: レポートを作成する (クロスリージョンの制限が適用されます)

この例では、日付範囲を指定せずに、指定されたイベントデータストアと評価のすべての結果を含むレポートを作成します。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

例 3: レポートを作成する (デフォルトの制限内)

この例では、指定されたイベントデータストアと評価のすべての結果を含むレポートを、デフォルトの最大値を下回る制限付きで作成します。

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

追加リソース

次のページには、評価レポートに関する一般的なトラブルシューティングのガイダンスが含まれています

- 評価レポートの問題のトラブルシューティング

CSV をエクスポートできませんでした

CSV エクスポートは、いくつかの理由で失敗する可能性があります。この問題は、最もよく生じる原因を確認することで解決できます。

まず、CSV エクスポート機能を使用するための前提条件を満たしていることを確認してください。

証拠ファインダーが正常に有効化されました

> 証拠ファインダーを有効にしていない場合、検索クエリを実行して検索結果をエクスポートすることはできません。

イベントデータストアのバックフィルが完了しました

有効にした直後に証拠ファインダーを使用し、証拠バックフィルがまだ進行中の場合は、結果が表示されない可能性があります。バックフィルステータスを確認するには、「」を参照してください証拠ファインダーのステータスの確認。

検索クエリは成功しました

Audit Manager は失敗したクエリの結果をエクスポートできません。失敗したクエリに対処するには、検索クエリが失敗しましたを参照してください。

前提条件を満たしていることを確認したら、次のチェックリストを使用して潜在的な問題がないか確認します。

1. 検索クエリのステータスを確認する。
   a. クエリはキャンセルされましたか? 証拠ファインダーでは、クエリがキャンセルされる前に処理された部分的な結果が表示されます。ただし、Audit Manager は部分的な結果を S3 バケットやダウンロードセンターにエクスポートしません。
   b. クエリの実行時間が 1 時間を超えていますか? 1 時間以上実行するクエリは、タイムアウトすることがあります。証拠ファインダーでは、クエリがタイムアウトになる前に処理された部分的な結果が表示されます。ただし、Audit Manager は、部分的な結果をエクスポートしません。タイムアウトを回避するには、 によってスキャンされる証拠の量を減らし検索フィルターの編集て、より狭い時間範囲を指定できます。
2. エクスポート先の S3 バケットの名前と URI を確認してください。
   a. 指定されたバケットは存在しますか？ バケット URI を手動で入力した場合は、入力ミスがないことを確認してください。Audit Manager が CSV ファイルを Amazon S3 にエクスポートしようとしたときに、タイプミスまたは誤った URI によってRESOURCE_NOT_FOUNDエラーが発生する可能性があります。
3. エクスポート先の S3 バケットの権限を確認してください。
   a. S3 バケットへの書き込み権限はありますか? エクスポート先として使用している S3 バケットへの書き込み権限が必要です。具体的には、IAM アクセス許可ポリシーに s3:PutObjectアクションとバケット ARN が含まれ、サービスプリンシパル CloudTrail としてリストされている必要があります。ご利用いただけるサンプルポリシーが用意されています。
4. いずれかの AWS リージョン 情報が一致しないかどうかを確認します。
   a. カスタマーマネージドキー AWS リージョン の は、評価 AWS リージョン の と一致していますか？ データ暗号化用にカスタマーマネージドキーを提供した場合、それは評価と同じ AWS

リージョン にある必要があります。KMS キーを変更する方法については、「」を参照してくださいデータ暗号化設定の構成。

5. 委任管理者アカウントの権限を確認してください。

   a. Audit Manager の設定のカスタマーマネージドキーが、委任された管理者に許可を付与していること。委任管理者アカウントを使用していて、データ暗号化にカスタマーマネージドキーを指定した場合は、委任管理者がその KMS キーにアクセスできることを確認してください。詳細については、「AWS Key Management Service 開発者ガイド」の「他のアカウントのユーザーに KMS キーの使用を許可する」を参照してください。Audit Manager で暗号化設定を確認および変更するには、「」を参照してくださいデータ暗号化設定の構成。

> **Note**
>
> Audit Manager のデータ暗号化の設定を変更した場合、これらの変更は、今後作成する新しい評価に適用されます。これには、新しい評価からエクスポートするすべての CSV ファイルが含まれます。
> この変更は、暗号化の設定を変更する前に作成した既存の評価には適用されません。これには、既存の CSV エクスポートに加えて、既存の評価からの新しい CSV エクスポートが含まれます。既存の評価 およびそれらのすべてのエクスポートは、引き続き古い KMS キーを使用します。評価レポートを生成する IAM ID に、古い KMS キーを使用するための許可が付与されていない場合は、キーポリシーレベルで許可を付与できます。

検索結果から特定の証拠をエクスポートできません

検索結果はすべて結果に含まれます。

CSV ファイルに特定の証拠のみを含めたい場合は、現在の検索フィルターを編集することをお勧めします。これにより、エクスポートしたい証拠だけをターゲットにするように結果を絞り込むことができます。

複数の CSV ファイルを一度にエクスポートできません

このエラーは、同時に実行する CloudTrail Lake クエリが多すぎることが原因です。

これは、検索結果をグループ化した後、その結果の各項目の CSV ファイルをすぐにエクスポートしようとした場合に発生する可能性があります。検索結果を取得して CSV ファイルをエクスポートすると、これらの各アクションによってクエリが呼び出されます。一

度に実行できるクエリは最大 5 つまでです。同時に実行するクエリの数が最大数に達すると、`MaxConcurrentQueriesException`エラーが返されます。

このエラーを防ぐには、一度にエクスポートする CSV ファイルの数が多すぎないようにしてください。

このエラーを解決するには、進行中の CSV エクスポートが完了するまでお待ちください。ほとんどのエクスポートには数分かかる場合があります。ただし、極めて大量のデータをエクスポートする場合、エクスポートが完了するまでに最大 1 時間かかることがあります。エクスポート中は、証拠ファインダーから自由に離れることができます。

Audit Manager コンソールのダウンロードセンターから、エクスポートステータスを確認できます。エクスポートしたファイルの準備ができたら、証拠ファインダーでグループ化された結果に戻ります。その後、引き続き結果を取得し、各項目の CSV ファイルをエクスポートできます。

フレームワークの問題のトラブルシューティング

このページの情報を使用して、Audit Manager の一般的なフレームワークの問題を解決できます。

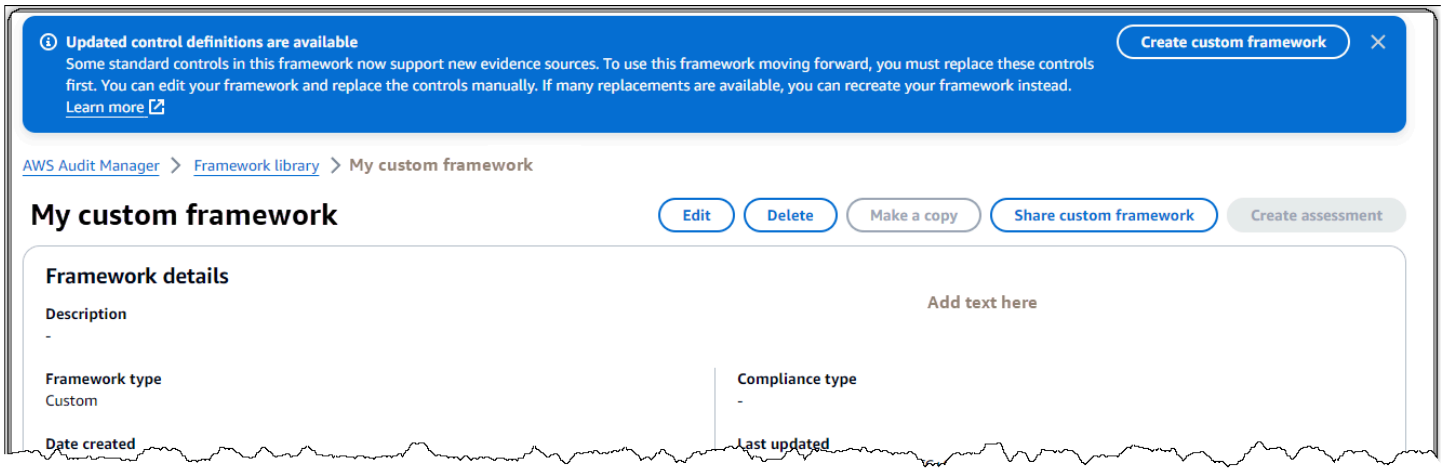
フレームワークの一般的な問題

- カスタムフレームワークの詳細ページで、カスタムフレームワークを再作成するように求められます。
- カスタムフレームワークのコピーを作成したり、それを使用して評価を作成したりすることはできません

フレームワークの共有に関する問題

- 送信済みの共有リクエストのステータスは失敗として表示されます
- 共有リクエストの横に青いドットがあります。これは何を意味するのでしょうか?
- 共有フレームワークには、データソースとしてカスタム AWS Config ルールを使用するコントロールがあります。受信者はこれらのコントロールを収集することができますか?
- 共有フレームワークで使用されているカスタムルールを更新しました。何かアクションを起こす必要がありますか?

カスタムフレームワークの詳細ページで、カスタムフレームワークを再作成するように求められます。



「更新されたコントロール定義が利用可能」というメッセージが表示された場合は、Audit Manager がカスタムフレームワークにある一部の標準コントロールの新しい定義を提供するようになったことを示します。

標準コントロールが から証拠を収集できるようになりましたAWS managed source。つまり、Audit Manager が共通コントロールまたはコアコントロールの基盤となるデータソースを更新するたびに、関連する標準コントロールに同じ更新が自動的に適用されます。これにより、クラウドコンプライアンス環境の変化に応じて継続的なコンプライアンスを確保できます。これらの AWS マネージドソースのメリットを確実に享受するには、カスタムフレームワークのコントロールを置き換えることをお勧めします。

カスタムフレームワークでは、Audit Manager はどのコントロールで置換が利用可能かを示します。カスタムフレームワークのコピーを作成したり、そこから評価を作成したりする前に、これらのコントロールを置き換える必要があります。次回カスタムフレームワークを編集するときに、これらのコントロールを他の編集内容に置き換えるよう求められます。

カスタムフレームワークのコントロールを置き換えるには、次の 2 つの方法があります。

1. カスタムフレームワークを再作成する

多数のコントロールで置換が可能な場合は、カスタムフレームワークを再作成することをお勧めします。これは、カスタムフレームワークが標準フレームワークに基づいている場合に最適なオプションである可能性があります。

- 例えば、 を出発点NIST SP 800-53 Rev 5として使用してカスタムフレームワークを作成したとします。この標準フレームワークには 1007 個の標準コントロールがあり、20 個のカスタムコントロールを追加しました。
- この場合、最も効率的なオプションは、フレームワークライブラリNIST 800-53 (Rev. 5) Low-Moderate-Highで を見つけ、そのフレームワークの編集可能なコピーを作成することです。このプロセス中に、以前に使用したものと同じ 20 個のカスタムコントロールを追加できます。標準フレームワークの最新の定義を開始点として使用しているため、カスタムフレームワークは 1007 のすべての標準コントロールの最新の定義を自動的に継承します。

2. カスタムフレームワークを編集する

少数のコントロールで置換が可能な場合は、カスタムフレームワークを編集し、コントロールを手動で置換することをお勧めします。

- 例えば、カスタムフレームワークをゼロから作成したとします。カスタムフレームワークでは、自分で作成した 20 個のカスタムコントロールと、標準フレームワークの 8 個のACSC Essential Eight 標準コントロールを追加しました。
- この場合、最大 8 つのコントロールで更新が使用可能になるため、最も効率的なオプションは、カスタムフレームワークを編集し、それらのコントロールを 1 つずつ置き換えることです。詳細については、以下の手順を参照してください。

カスタムフレームワークのコントロールを手動で置き換えるには

カスタムフレームワークのコントロールを手動で置き換えるには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 左側のナビゲーションペインで、フレームワークライブラリ を選択し、カスタムフレームワークタブを選択します。
3. 編集するフレームワークを選択し、[アクション]、[編集] の順に選択します。
4. フレームワークの詳細の編集ページで、次へ を選択します。
5. 「コントロールセットの編集」ページで、各コントロールセットの名前を確認して、そのコントロールのいずれかに代替のものがあるかどうかを確認します。
6. 影響を受けるコントロールセットを選択して展開し、置き換える必要があるコントロールを特定します。

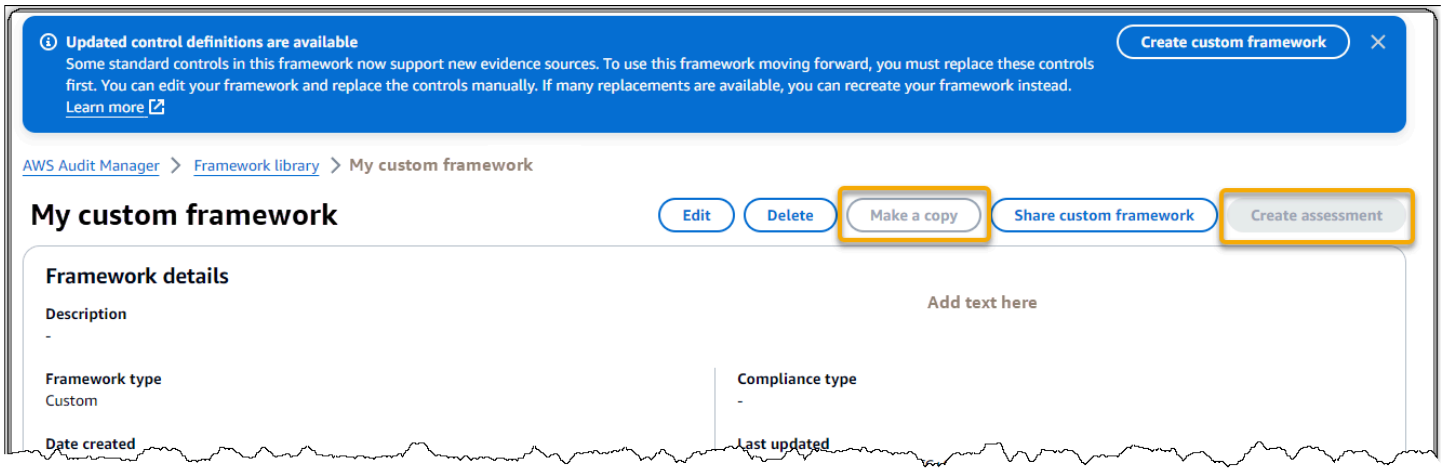
> **Tip**
>
> コントロールをより迅速に識別するには、検索ボックスに **`Replacement available`** と入力します。

7. 影響を受けたコントロールを削除するには、チェックボックスを選択し、コントロールセットから削除を選択します。
8. 同じコントロールを再追加します。このアクションは、先ほど削除したコントロールを最新のコントロール定義に置き換えます。
   a. 「コントロールの追加」で、コントロールタイプのドロップダウンリストを使用して、「標準コントロール」を選択します。
   b. 削除したコントロールの置き換えを見つけます。

      > **Tip**
      >
      > 場合によっては、置換コントロール名は元のコントロール名とまったく同じではない場合があります。この場合、置換コントロール名は元のものと非常によく似ています。まれに、1 つのコントロールが 2 つのコントロール (または逆) に置き換えられることがあります。
      > 代替コントロールが見つからない場合は、部分検索を行うことをお勧めします。これを行うには、元のコントロール名の一部、または探しているものを表すキーワードを入力します。コンプライアンスタイプで検索して、結果のリストをさらに絞り込むこともできます。

   c. コントロールの横にあるチェックボックスを選択し、コントロールセット に追加 を選択します。
   d. 表示されるポップアップウィンドウで、追加 を選択して確認します。
9. すべてのコントロールを置き換えるまで、必要に応じてステップ 6~8 を繰り返します。
10. [次へ] をクリックします。
11. 確認と保存ページで、変更を保存 を選択します。

カスタムフレームワークのコピーを作成したり、それを使用して評価を作成したりすることはできません



フレームワークの詳細ページで「コピーの作成」ボタンと「評価の作成」ボタンが使用できない場合は、カスタムフレームワークのコントロールの一部を置き換える必要があります。

手順については、「」を参照してください[カスタムフレームワークの詳細ページで、カスタムフレームワークを再作成するように求められます。](#)。

送信済みの共有リクエストのステータスは失敗として表示されます

カスタムフレームワークを共有しようとして操作が失敗した場合は、次の事項を確認することをお勧めします。

1. Audit Manager が受信者の AWS アカウント および指定されたリージョンで有効になっていることを確認します。サポートされている AWS Audit Manager リージョンのリストについては、アマゾン ウェブ [AWS Audit Manager サービス全般のリファレンスの「 エンドポイントとクォータ](#)」を参照してください。
2. 受信者アカウントを指定したときに、正しい AWS アカウント ID を入力していることを確認してください。
3. AWS Organizations 管理アカウントを受信者として指定していないことを確認してください。委任された管理者とカスタムフレームワークを共有できますが、管理アカウントとカスタムフレームワークを共有しようとすると、操作は失敗します。
4. Audit Manager データを暗号化するためにカスタマーマネージドキーを使用する場合は、KMS キーが有効になっていることを確認します。KMS キーが無効になっているときにカスタムフレームワークを共有しようとすると、操作は失敗します。無効になっている KMS キーを有効にする手

順については、AWS Key Management Service 開発者ガイドのキーの有効化と無効化を参照してください。

共有リクエストの横に青いドットがあります。これは何を意味するのでしょうか?

青いドットの通知は、共有リクエストに注意が必要であることを示唆しています。

送信者向けの青いドットの通知

ステータスが [Expiring] (まもなく期限切れ) の送信済み共有リクエストの横に青い通知ドットが表示されます。Audit Manager は青いドットの通知を表示して、共有リクエストの有効期限が切れる前にアクションを実行するよう受信者に注意喚起できるようにします。

青い通知ドットが表示されないようにするには、受信者は、リクエストを承諾または辞退する必要があります。共有リクエストを取り消すと、青いドットも表示されなくなります。

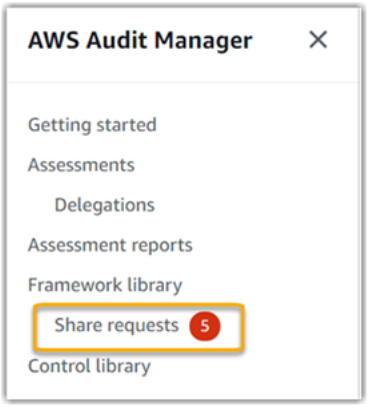
次の手順を実行して、まもなく期限が切れる共有リクエストを確認し、アクションを実行するようオプションのリマインダーを受信者に送信できます。

送信済みリクエストに関する通知を表示するには

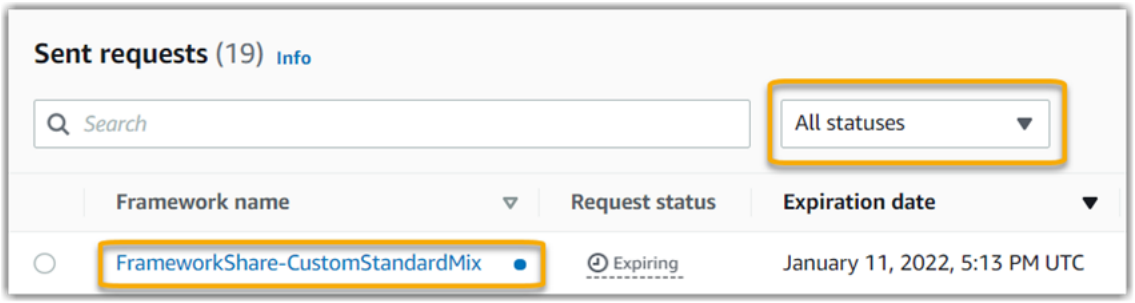
1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 共有リクエスト通知がある場合、Audit Manager は、ナビゲーションメニューのアイコンの横に赤いドットを表示します。

3. ナビゲーションペインを展開し、[Share requests] (共有リクエスト) の横を確認します。通知バッジは、注意が必要な共有リクエストの数を示します。



4. [Share requests] (共有リクエスト) を選択してから、[Sent requests] (送信済みリクエスト) のタブを選択します。
5. 青いドットを探して、今後 30 日以内に期限切れになる共有リクエストを特定します。または、[All statuses] (すべてのステータス) フィルターのドロップダウンから [Expiring] (まもなく期限切れ) を選択して、期限切れになりそうな共有リクエストを表示することもできます。



6. (オプション) 共有リクエストの有効期限が切れる前に、アクションを実行する必要があることを受信者に通知します。共有リクエストがアクティブまたはまもなく期限切れになる場合、Audit Manager は、コンソールで通知を送信して受信者に知らせるため、この手順はオプションです。ただし、希望する通信チャネルを使用して、受信者に独自のリマインダーを送信することもできます。

受信者向けの青いドットの通知

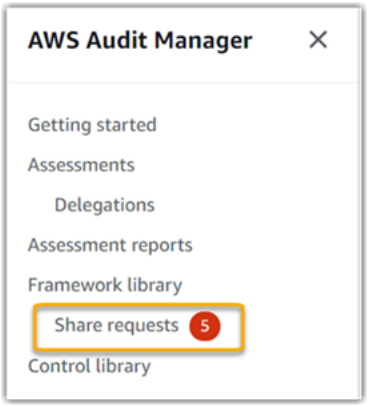
ステータスが [Active] (アクティブ) または [Expiring] (まもなく期限切れ) の受信済み共有リクエストの横に青い通知ドットが表示されます。Audit Manager は青いドットの通知を表示して、共有リクエストの有効期限が切れる前にアクションを実行するようユーザーに注意喚起します。青い通知ドットが表示されないようにするには、リクエストを承諾または辞退する必要があります。送信者が共有リクエストを取り消すと、青いドットも表示されなくなります。

次の手順を実行して、アクティブな共有リクエストやまもなく期限切れの共有リクエストを確認できます。

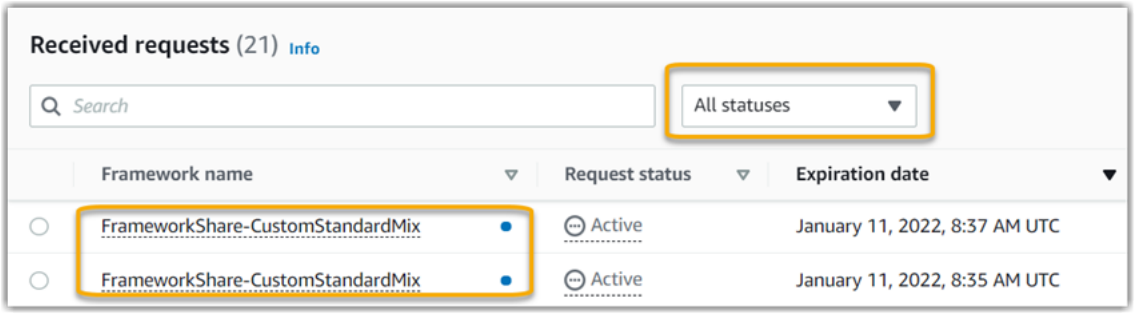
受信したリクエストに関する通知を表示するには

1. AWS Audit Manager コンソール (https://console.aws.amazon.com/auditmanager/home) を開きます。
2. 共有リクエスト通知がある場合、Audit Manager は、ナビゲーションメニューのアイコンの横に赤いドットを表示します。

3. ナビゲーションペインを展開し、[共有リクエスト] の横を確認します。通知バッジは、注意が必要な共有リクエストの数を示します。



4. [共有リクエスト] を選択します。デフォルトでは、このページは [受信したリクエスト] のタブで開きます。
5. 青いドットが表示されている項目を探して、アクションが必要な共有リクエストを特定します。



6. (オプション) 今後 30 日以内に期限切れになるリクエストのみを表示するには、[All statuses] (すべてのステータス) ドロップダウンリストを見つけて、[Expiring] (まもなく期限切れ) を選択します。

共有フレームワークには、データソースとしてカスタム AWS Config ルールを使用するコントロールがあります。受信者はこれらのコントロールを収集することができますか?

はい、受信者はこれらのコントロールの証拠を収集できますが、そのためにはいくつかの手順が必要です。

Audit Manager が AWS Config ルールをデータソースマッピングとして使用して証拠を収集するには、次の条件を満たす必要があります。これらの基準は、マネージドルールとカスタムルールの両方に適用されます。

- ルールは受信者の AWS 環境に存在する必要があります。
- ルールは受信者の AWS 環境で有効にする必要があります。

アカウントの AWS Config ルールが受信者の AWS 環境にまだ存在しない可能性があることに注意してください。さらに、受信者が共有リクエストを受け入れるとき、Audit Manager は受信者のアカウントにカスタムルールを再作成しません。受信者がデータソースマッピングとしてカスタムルールを使用して証拠を収集するには、 のインスタンスに同じカスタムルールを作成する必要があります AWS Config。受信者が でルール[を作成して有効に](#)すると AWS Config、Audit Manager はそのデータソースから証拠を収集できます。

受信者と通信して、 のインスタンスにカスタム AWS Config ルールを作成する必要があるかどうかを知らせることをお勧めします AWS Config。

共有フレームワークで使用されているカスタムルールを更新しました。何かアクションを起こす必要がありますか?

AWS 環境内のルール更新の場合

AWS 環境内のカスタムルールを更新する場合、Audit Manager でアクションは必要ありません。Audit Manager は、次の表で説明されている方法でルールの更新を検出し、処理します。Audit Manager は、ルールの更新が検出されても通知しません。

シナリオ	Audit Manager の機能	必要な作業
カスタムルールは、 のインスタンスで更新されます AWS Config。	Audit Manager は、更新されたルール定義を使用して、そ	アクションは不要です。

シナリオ	Audit Manager の機能	必要な作業
	のルールに関する検出結果を引き続き報告します。	
カスタムルールは、 のインスタンスで削除されます AWS Config。	Audit Manager は、削除されたルールに関する検出結果の報告を停止します。	アクションは不要です。 必要に応じて、削除されたルールをデータソースマッピングとして使用していたカスタムコントロールを編集することができます。その後、削除されたルールを取り除き、コントロールのデータ ソース設定を整理できます。そうしない場合、削除されたルール名は未使用のデータソースマッピングとして残ります。

AWS 環境外のルール更新の場合

受信者の AWS 環境では、Audit Manager はルールの更新を検出しません。これは、送信者と受信者がそれぞれ別々の AWS 環境で作業するためです。次の表は、このシナリオの推奨アクションを示しています。

役割	シナリオ	推奨されるアクション
送信者	• カスタムルールをデータソースマッピングとして使用するフレームワークを共有しました。 • フレームワークを共有した後、 でこれらのルールのいずれかを更新または削除しました AWS Config。	受信者に連絡して、更新について知らせてください。そうすれば、受信者は同じ更新を行い、最新のルール定義と同期した状態を保つことができます。
受取人	• カスタムルールをデータソースマッピングとして使用する共有フレームワークを受け入れました。	AWS Configのインスタンスで、対応するルールを更新してください。

役割	シナリオ	推奨されるアクション
	• のインスタンスでカスタムルールを再作成すると AWS Config、送信者はそれらのルールの 1 つを更新または削除します。	

通知に関する問題のトラブルシューティング

このページの情報を参照して、Audit Manager での一般的な通知の問題を解決できます。

トピック

Audit Manager で Amazon SNS トピックを指定しましたが、通知が届きません

Amazon SNS トピックがサーバー側の暗号化 (SSE) AWS KMS に を使用している場合、 AWS KMS キーポリシーに必要なアクセス許可が不足している可能性があります。エンドポイントをトピックにサブスクライブしなかった場合も、通知を受信できない可能性があります。

通知を受信していない場合は、次の事項を実行したことを確認してください。

- 必要な許可ポリシーを KMS キーにアタッチしたこと。使用できるポリシーの例については、「」を参照してください例 2 (SNS トピックに添付されている KMS キーの許可)。
- 通知が送信されるトピックにエンドポイントをサブスクライブしていること。E メールエンドポイントをトピックにサブスクライブすると、サブスクリプションの確認を求める E メールが届きます。E メール通知の受信を開始するには、サブスクリプションを確認する必要があります。詳細については、Amazon SNS Developer Guide の「開始」を参照してください。

FIFO トピックを指定しましたが、想定した順序で通知が届きません

Audit Manager は FIFO SNS トピックへ通知を送信します。ただし、Audit Manager が FIFO トピックに通知を送信する順序は確約されません。

許可とアクセスの問題のトラブルシューティング

このページの情報を参照して、Audit Manager での一般的な許可の問題を解決できます。

トピック

Audit Manager の設定手順に従いましたが、十分な IAM 権限が付与されていません

Audit Manager にアクセスするユーザー、ロール、またはグループ には、権限が必要です。さらに、アイデンティティベースのポリシーは制限が厳しすぎないようにする必要があります。さもないと、コンソールが意図したとおりに機能しません。このガイドでは、 で使用できるポリシーの例を示しますAudit Managerを有効にするために必要な最小限の許可を与える。ユースケースによっては、より広く、より制限的でない許可が必要になる場合があります。例えば、監査所有者には、管理者アクセス権を付与することが推奨されます。これは、Audit Manager の設定を変更し、評価、フレームワーク、コントロール、評価レポートなどのリソースを管理できるようにするためです。受任者などの他のユーザーに必要なのは、管理アクセスまたは読み取り専用アクセスのみである場合があります。

ユーザー、ロール、またはグループに適切な権限を必ず追加してください。監査所有者の場合、推奨されるポリシーは ですAWSAuditManagerAdministratorAccess。代理人の場合は、IAM ポリシーの例ページで提供されている管理アクセスの例のポリシーを使用できます。https://docs.aws.amazon.com/audit-manager/latest/userguide/security_iam_id-based-policy-examples.htmlこれらのサンプルポリシーを開始点として使用し、要件に合うように必要に応じて変更を加えることができます。

特定の要件を満たせるよう、時間を設けて許可をカスタマイズすることをお勧めします。IAM 許可についてサポートが必要な場合は、管理者または AWS Support までお問い合わせください。

あるユーザーを監査所有者として指定しましたが、そのユーザーは評価に完全にアクセスすることができません。これはなぜですか?

あるユーザーを監査所有者として指定するだけでは、評価への完全なアクセス権は提供されません。監査所有者には、Audit Manager のリソースにアクセスして管理するために必要な IAM 許可も付与されている必要があります。つまり、ユーザーを監査所有者として指定することに加えて、必要な IAM ポリシーをそのユーザーにアタッチする必要もあります。この背後には、両方を要求することにより、Audit Manager が、各評価のすべての詳細を完全に制御できるようにするという考え方があります。

> **Note**
>
> 監査所有者には、 AWSAuditManagerAdministratorAccessポリシーを使用することをお勧めします。詳細については、「 のユーザーペルソナに推奨されるポリシー AWS Audit Manager」を参照してください。

Audit Manager でアクションを実行できません

AWS Audit Manager コンソールまたは Audit Manager API オペレーションを使用するために必要なアクセス許可がない場合は、`AccessDeniedException`エラーが発生する可能性があります。

この問題を解決するには、管理者に問い合わせてサポートを依頼してください。管理者とは、サインイン認証情報を提供した担当者です。

自分の 以外のユーザーに Audit Manager リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- AWS Audit Manager がこれらの機能をサポートしているか確認するには、「が IAM と AWS Audit Manager 連携する方法」を参照してください。

- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

必要な Audit Manager のアクセス許可があるにもかかわらず、アクセス拒否エラーが表示される

アカウントが組織の一部である場合、`Access Denied`エラーはサービスコントロールポリシー (SPC) によって引き起こされる可能性があります。SCPsは、組織のアクセス許可を管理するために使用されるポリシーです。SCP が設定されると、Audit Manager で使用する委任管理者アカウントなど、すべてのメンバーアカウントに対する特定のアクセス許可を拒否できます。

例えば、Control Catalog APIs、 AWS Control Catalog によって提供されるリソースを表示することはできません。これは、AWSAuditManagerAdministratorAccessポリシーなど、Audit Manager に必要なアクセス許可がある場合にも当てはまります。SCP は、Control Catalog APIs。

このような SCP の例を次に示します。この SCP を設定すると、委任された管理者アカウントは、Audit Manager の共通コントロール機能を使用するために必要な共通コントロール、コントロール目標、およびコントロールドメインへのアクセスを拒否されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "controlcatalog:ListCommonControls",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListDomains",
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

この問題を解決するには、次の手順を実行することをお勧めします。

1. SCP が組織にアタッチされているかどうかを確認します。手順については、AWS Organizations ユーザーガイドの「組織のポリシーに関する情報の取得」を参照してください。 AWS Organizations
2. SCP が`Access Denied`エラーの原因となっているかどうかを確認します。
3. SCP を更新して、委任管理者アカウントが Audit Manager に必要なアクセス権を持っていることを確認します。手順については、AWS Organizations ユーザーガイドの「SCP の更新」を参照してください。 AWS Organizations

追加リソース

以下のページには、権限がないことが原因で発生する可能性のあるその他の問題に関するトラブルシューティングのガイダンスが記載されています。

- 評価にコントロールまたはコントロールセットが表示されません
- コントロールデータソースを設定しているときは、カスタムルールオプションは使用できません
- レポートを生成しようとすると、アクセス拒否エラーが発生します
- 委任された管理者アカウントを使用して評価レポートを生成しようとすると、アクセス拒否エラーが発生します
- 証拠ファインダーを有効にできません
- 証拠ファインダーを無効にできません
- 検索クエリが失敗しました
- Audit Manager で Amazon SNS トピックを指定しましたが、通知が届きません

AWS Audit Manager リソースのタグ付け

タグは、 AWS リソースに割り当てるメタデータラベルです AWS 。各タグは、キーと値から構成されます。ユーザーが割り当てるタグでは、ユーザーがキーと値を定義します。たとえば、1 つのリソースのキーを `stage` と定義し、値を `test` と定義します。

タグは、以下のことに役立ちます。

- Audit Manager のリソースを簡単に見つけることができます。フレームワークライブラリとコントロールライブラリを参照する際に、タグを検索条件として使用できます。
- リソースをコンプライアンスタイプに関連付けます。複数のリソースにコンプライアンス固有のタグを付けて、それらのリソースを特定のフレームワークに関連付けることができます。
- AWS リソースを特定して整理します。多くの はタグ付け AWS のサービス をサポートしているため、異なるサービスのリソースに同じタグを割り当てて、リソースが関連していることを示すことができます。
- AWS コストを追跡します。 AWS Billing and Cost Management ダッシュボードでこれらのタグをアクティブ化します。 はタグ AWS を使用してコストを分類し、毎月のコスト配分レポートを配信します。詳細については、「AWS Billing and Cost Management ユーザーガイド」の「コスト配分タグを使用する」を参照してください。

以下のセクションでは、 のタグについて詳しく説明します AWS Audit Manager。

目次

Audit Manager の対応しているリソース

次のネットワーク管理リソースがタグ付けをサポートしています。

- 評価
- コントロール
- フレームワーク

タグの制限

Audit Manager リソースのタグには、次のような基本的な制限があります。

- リソースに割り当てることができるタグの最大数 - 50
- キーの最大長 – 128 文字 (Unicode)
- 値の最大長 – 256 文字 (Unicode)
- キーと値の有効な文字 – a ~ z、A ~ Z、0 ~ 9、スペース、および特殊文字 (_ . : / = + - @)
- キーと値では大文字と小文字が区別されます
- キーのプレフィックス`aws:`として を使用しないでください。 AWS 用に予約されています。

追加リソース

評価、フレームワーク、またはコントロールを作成するときに、タグをプロパティとして設定できます。Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、および Audit Manager API を使用して、タグを追加、編集、削除できます。詳細については、以下のリンクを参照してください。

- タグ付け評価の場合：
  - このガイドの「評価」のセクションの「での評価の作成 AWS Audit Manager」および「での評価の編集 AWS Audit Manager」
  - [Tags (タグ)] タブ このガイドの「評価の確認」ページの「
  - CreateAssessment AWS Audit Manager API リファレンスUpdateAssessmentの および
  - TagResource AWS Audit Manager API リファレンスUntagResourceの および
- フレームワークのタグ付けの場合：
  - このガイドの「フレームワークライブラリ」のセクションの「でのカスタムフレームワークの作成 AWS Audit Manager」および「でのカスタムフレームワークの編集 AWS Audit Manager」
  - このガイドのTags tab「フレームワークの詳細を表示」ページの
  - CreateAssessmentFramework AWS Audit Manager API リファレンスUpdateAssessmentFrameworkの および
  - TagResource AWS Audit Manager API リファレンスUntagResourceの および
- タグ付けコントロールの場合：
  - このガイドの「コントロールライブラリ」のセクションの「でのカスタムコントロールの作成 AWS Audit Manager」および「でのカスタムコントロールの編集 AWS Audit Manager」

- このガイドの「カスタムコントロールの確認」ページのTags「」セクション
- このガイドの「標準コントロールの確認」ページのTags「」セクション
- CreateControl AWS Audit Manager API リファレンスUpdateControlの および
- TagResource AWS Audit Manager API リファレンスUntagResourceの および

のクォータと制限について AWS Audit Manager

AWS アカウント には、各 について、以前は制限 と呼ばれていたデフォルトのクォータがありますAWS のサービス。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについてはリクエストできません。

Audit Manager のほとんどのクォータは、すべてではありませんが、Service Quotas コンソール AWS Audit Manager の名前空間に一覧表示されます。クォータの引き上げをリクエストする方法については、「Audit Manager のクォータの管理」を参照してください。

目次

デフォルトの Audit Manager クォータ

次の AWS Audit Manager クォータは、リージョンごとに AWS アカウント ごとに設定されます。

リソース	クォータ
評価	アカウントあたりのアクティブな評価の数: 100
評価レポート	評価レポートに追加できる証拠項目の数: • 同じリージョンのレポートの場合 (評価と評価レポートの送信先 S3 バケットが同じ AWS リージョンになる場合): 22,000 • クロスリージョンレポートの場合 (評価と評価レポートの送信先 S3 バケットが異なる AWS リージョンにある場合): 3,500 • 関連する評価がカスタマー管理の を使用するレポートの場合 AWS KMS key: 3,500
コントロール	アカウントあたりのカスタムコントロールの数: 500
証拠	単一の手動による証拠ファイルの最大サイズ: 100 MB

リソース	クォータ
	各コントロールあたりの 1 日の手動証拠アップロードの数: 100 **Tip** 単一のコントロールに手動証拠を大量にアップロードする必要がある場合は、証拠を数日にわたってバッチでアップロードすることをお勧めします。
フレームワーク	アカウントあたりのカスタムフレームワークの数: 100 **Note** フレームワークのクォータは、フレームワークの作成者にかかわらず、フレームワークライブラリ内のすべての共有カスタムフレームワークに適用されます。
共有カスタムフレームワークの受信者	アクティブな受信者アカウントの数: 100
API アクセス	すべての API での 1 秒あたりのトランザクション数 (TPS): 20 TPS

Audit Manager のクォータの管理

AWS Audit Manager は Service Quotas と統合されています。 AWS のサービス Service Quotas は、クォータを一元的に表示および管理できる です。Service Quotas を使用すると、Audit Manager クォータの値を簡単に調べることができます。

コンソールを使用して Audit Manager のサービスクォータを表示するには

1. Service Quotas のコンソールを開きます。https://console.aws.amazon.com/servicequotas/
2. ナビゲーションペインで、AWS のサービス を選択します。
3. [AWS のサービス] リストから、[AWS Audit Manager] を探して選択します。

4. サービスクォータリストには、サービスクォータ名、適用されたクォータ値 (使用可能な場合) 、 AWS デフォルトのクォータ値、およびクォータが調整可能かどうかが表示されます。
5. 説明など、Service Quotas に関する追加情報を表示するには、クォータ名を選択します。
6. (オプション) クォータの引き上げをリクエストするには、[Request quota increase (クォータ引き上げリクエスト)] を選択、または必要な情報を入力または選択して、[Request (リクエスト)] を選択します。

追加リソース

クォータの管理方法の詳細については、「Service Quotas ユーザーガイド」の「クォータの引き上げのリクエスト」を参照してください。 Service Quotas

Service Quotas の詳細については、Service Quotasとは Service Quotas」を参照してください。

のセキュリティとデータ保護について AWS Audit Manager

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — クラウド AWS のサービス で実行されるインフラストラクチャを保護する責任 AWS は にあります AWS 。 AWS また、 は、安全に使用できるサービスも提供します。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。に適用されるコンプライアンスプログラムの詳細については AWS Audit Manager、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は AWS のサービス 、使用する によって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Audit Manager。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Audit Manager を設定する方法を示します。また、Audit Manager リソースのモニタリングや保護 AWS のサービス に役立つ他の の使用方法についても説明します。

トピック

- でのデータ保護 AWS Audit Manager
- の Identity and Access Management AWS Audit Manager
- のコンプライアンス検証 AWS Audit Manager
- の耐障害性について AWS Audit Manager
- のインフラストラクチャセキュリティ AWS Audit Manager
- AWS Audit Manager およびインターフェイス VPC エンドポイント (AWS PrivateLink)
- での口グ記録とモニタリング AWS Audit Manager
- での設定と脆弱性の分析について AWS Audit Manager

でのデータ保護 AWS Audit Manager

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Audit Manager。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーのよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿されたAWS 責任共有モデルおよび GDPRのブログ記事を参照してください。

データ保護の目的で、 認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Audit Manager AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

上記の推奨事項に加えて、Audit Manager のお客様には、評価、カスタムコントロール、カスタムフレームワーク、および委任コメントを作成する際に、自由形式のフィールドに機密性の高い識別情報を含めないことを特に推奨します。

Audit Manager のデータの削除

Audit Manager のデータを削除するにはいくつか方法があります。

Audit Manager を無効にする場合のデータ削除

Audit Manager を無効にする場合、Audit Manager のデータをすべて削除するかどうかを決定できます。データを削除することを選択した場合、Audit Manager を無効にしてから 7 日以内に削除されます。データを削除すると、復元することはできません。

データの自動削除

Audit Manager のデータの一部は、特定の期間が経過すると自動的に削除されます。Audit Manager は、以下のように顧客データを保持します。

データ型	データ保持期間	メモ
証拠	データは作成時から 2 年間保存されます	自動証拠と手動証拠が含まれます
顧客が作成したリソース	データは無期限に保持されます	評価、評価レポート、カスタムコントロール、カスタムフレームワークが含まれます

手動データ削除

個々のAudit Manager リソースはいつでも削除できます。手順については、以下を参照してください。

- での評価の削除 AWS Audit Manager
  - AWS Audit Manager API リファレンスDeleteAssessmentの も参照してください。
- でのカスタムフレームワークの削除 AWS Audit Manager
  - AWS Audit Manager API リファレンスDeleteAssessmentFrameworkの も参照してください。
- での共有リクエストの削除 AWS Audit Manager
  - AWS Audit Manager API リファレンスDeleteAssessmentFrameworkShareの も参照してください。
- 評価レポートの削除

  - AWS Audit Manager API リファレンスDeleteAssessmentReportの も参照してください。
- でのカスタムコントロールの削除 AWS Audit Manager
  - AWS Audit Manager API リファレンスDeleteControlの も参照してください。

Audit Manager の使用時に作成した他のリソースデータを削除するには、以下を参照してください

- AWS CloudTrail ユーザーガイドの「イベントデータストアを削除する」
- Amazon Simple Storage Service (Amazon S3)ユーザーガイドのバケットキーを削除する

保管中の暗号化

Audit Manager は、保管中のデータを暗号化するために、すべてのデータストアとログ AWS マネージドキー に対して によるサーバー側の暗号化を使用します。

データは、選択した設定に応じて AWS 所有のキー、カスタマーマネージドキーまたは で暗号化されます。カスタマーマネージドキーを指定しない場合、Audit Manager は AWS 所有のキー を使用してコンテンツを暗号化します。Audit Manager の DynamoDB と Amazon S3 のすべてのサービスメタデータは、 AWS 所有のキーを使用して暗号化されます。

Audit Manager は次のようにデータを暗号化します。

- Amazon S3 に保存されているサービスメタデータは、SSE-KMS AWS 所有のキー を使用して で暗号化されます。
- DynamoDB に保存されているサービスメタデータは、KMS と AWS 所有のキーを使用してサーバー側で暗号化されています。
- DynamoDB に保存されているコンテンツは、カスタマーマネージドキーまたは AWS 所有のキーを使用してクライアント側で暗号化されます。KMS キーは、選択した設定に基づきます。
- Audit Manager の Amazon S3 に保存されているコンテンツは、SSE-KMS を使用して暗号化されます。KMS キーは選択に基づいており、カスタマーマネージドキーまたは AWS 所有のキーのいずれかです。
- S3 バケットに発行された評価レポートは、次のように暗号化されます。
  - カスタマーマネージドキーを提供した場合、データは SSE-KMS を使用して暗号化されます。
  - を使用した場合 AWS 所有のキー、データは SSE-S3 を使用して暗号化されます。

転送中の暗号化

Audit Manager は、転送中のデータを暗号化するための安全なプライベートエンドポイントを提供します。セキュアエンドポイントとプライベートエンドポイントにより AWS 、 は Audit Manager への API リクエストの整合性を保護できます。

サービス間トランジット

デフォルトでは、すべてのサービス間通信は、Transport Layer Security (TLS) 暗号化を使用して保護されます。

キー管理

Audit Manager は AWS 所有のキー 、すべての Audit Manager リソース (アカウント内の S3 バケットに保存された評価、コントロール、フレームワーク、証拠、および評価レポート) を暗号化するための とカスタマーマネージドキーの両方をサポートします。

カスタマーマネージドキーを使用することをお勧めします。これにより、 AWS CloudTrailでの使用のログの表示など、データを保護する暗号化キーを表示および管理できます。カスタマーマネージドキーを選択する際に、Audit Manager は、コンテンツの暗号化に使用できるように、KMS キーの付与を作成します。

> **Warning**
>
> Audit Manager リソースの暗号化に使用される KMS キーを削除または無効にすると、その KMS キーで暗号化されたリソースを復号できなくなります。つまり、データを回復できなくなります。
> AWS Key Management Service （ AWS KMS) で KMS キーを削除すると、破壊的になり、潜在的に危険です。KMS キーの削除の詳細については、AWS Key Management Service ユーザーガイドの「AWS KMS keysの削除」を参照してください。

、Audit Manager API AWS Management Console、または AWS Command Line Interface () を使用して Audit Manager を有効にするときに、暗号化設定を指定できますAWS CLI。手順については、「の有効化 AWS Audit Manager」を参照してください。

暗号化設定はいつでも確認および変更できます。手順については、「データ暗号化設定の構成」を参照してください。

カスタマーマネージドキーの設定方法の詳細については、AWS Key Management Service ユーザーガイドの「キーの作成」を参照してください。

の Identity and Access Management AWS Audit Manager

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に Audit Manager リソースの使用を認可する (許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、Audit Manager で行う作業によって異なります。

サービスユーザー – ジョブを実行するために Audit Manager サービスを使用する場合は、管理者から必要な認証情報と許可が与えられます。さらに多くの Audit Manager 機能を使用して作業を行う場合は、追加の許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Audit Manager の機能にアクセスできない場合は、「AWS Audit Manager ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Audit Manager リソースを担当している場合は、通常、Audit Manager へのフルアクセスがあります。サービスユーザーがどの Audit Manager 機能やリソースにアクセスす

る必要があるかを決めるのは、あなたの仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。お客様の会社で Audit Manager で IAM を利用する方法の詳細については、「が IAM と AWS Audit Manager 連携する方法」を参照してください。

IAM 管理者 – IAM 管理者は、Audit Manager へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Audit Manager のアイデンティティベースのポリシーの例を表示するには、「のアイデンティティベースのポリシーの例 AWS Audit Manager」を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「Multi-factor authentication」(多要素認証) および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドのルートユーザー認証情報が必要なタスクを参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションするを参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。

例えば、IAMAdminsという名前のグループを設定して、そのグループにIAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与するを参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、IAM ユーザーガイドの(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドのJSON ポリシー概要を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、IAM ユーザーガイドのマネージドポリシーとインラインポリシーの比較を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があ

げられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイドのアクセスコントロールリスト (ACL) の概要を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM エンティティのアクセス許可の境界を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を

制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、IAM ユーザーガイドのセッションポリシーを参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

が IAM と AWS Audit Manager 連携する方法

IAM を使用してAudit Manager へのアクセスを管理する前に、Audit Managerで利用できるIAMの機能について学びます。

で使用できる IAM の機能 AWS Audit Manager

IAM 機能	Audit Manager のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	部分的
ACL	なし
ABAC (ポリシー内のタグ)	はい

IAM 機能	Audit Manager のサポート
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	いいえ
サービスリンクロール	あり

AWS Audit Manager およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM AWS と連携する のサービス」を参照してください。

のアイデンティティベースのポリシー AWS Audit Manager

アイデンティティベースポリシーをサポートする	あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、IAM ユーザーガイドのIAM JSON ポリシーの要素のリファレンスを参照してください。

AWS Audit Manager は、Audit Manager 管理者`AWSAuditManagerAdministratorAccess`向けのという名前のマネージドポリシーを作成します。このポリシーは、Audit Manager での完全な管理アクセスを許可します。管理者は、このポリシーを既存のロールまたはユーザーにアタッチするか、このポリシーを使用して新しいロールを作成できます。

のユーザーペルソナに推奨されるポリシー AWS Audit Manager

AWS Audit Manager では、異なる IAM ポリシーを使用して、異なるユーザー間および異なる監査のために職務の分離を維持できます。Audit Manager の 2 つのペルソナとそれらの推奨ポリシーは、次のように定義されています。

ペルソナ	説明と推奨ポリシー
監査所有者	• このペルソナには、 で評価を管理するために必要なアクセス許可が必要です AWS Audit Manager。 • このペルソナに使用する推奨ポリシーは、 という名前の マネージドポリシーですAWSAuditManagerAdministratorAccess。このポリシーを開始点として使用し、要件に合わせて必要に応じてこれらの許可をスコープダウンできます。
受任者	• このペルソナは、評価で委任されたコントロールセットにアクセスできます。このペルソナは、コントロールステータスの更新、コメントの追加、レビューのためのコントロールセットの送信、および評価レポートへの証拠の追加を行うことができます。 • このペルソナで使用が推奨されるポリシーは、ポリシー例 ユーザーには AWS Audit Managerへの管理アクセスを許可します です。このポリシーを開始点として使用し、要件に合うように必要に応じて変更を加えることができます。

のアイデンティティベースのポリシーの例 AWS Audit Manager

Audit Managerでのアイデンティティベースのポリシーの例は、「のアイデンティティベースのポリシーの例 AWS Audit Manager」を参照してください。

内のリソースベースのポリシー AWS Audit Manager

リソースベースのポリシーのサポート	なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーに

よって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

のポリシーアクション AWS Audit Manager

ポリシーアクションに対するサポート	あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

AWS Audit Manager アクションのリストを確認するには、「サービス認証リファレンス」の「AWS Audit Manager で定義されるアクション」を参照してください。

のポリシーアクションは、アクションの前に次のプレフィックス AWS Audit Manager を使用します。

```
auditmanager
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

ワイルドカード *を使用して複数のアクションを指定することができます。例えば、Get という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "auditmanager:Get*"
```

Audit Managerでのアイデンティティベースのポリシーの例は、「のアイデンティティベースのポリシーの例 AWS Audit Manager」を参照してください。

のポリシーリソース AWS Audit Manager

ポリシーリソースに対するサポート	あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

AWS Audit Manager リソースタイプとその ARNs」の「AWS Audit Manager で定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、「AWS Audit Manager で定義されるアクション」を参照してください。

Audit Manager の評価には、次の Amazon リソースネーム (ARN) 形式があります。

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Audit Manager のコントロールセットの ARN 形式は次のとおりです。

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Audit Manager のコントロールの ARN 形式は次のとおりです。

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

ARN の形式の詳細については、「Amazon リソースネーム (ARN)」を参照してください。

例えば、ステートメントで i-1234567890abcdef0 評価を指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

特定のアカウントに属するすべてのインスタンスを指定するには、ワイルドカード *を使用します。

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

リソースの作成など、一部のAudit Manager アクションは、特定のリソースで実行できません。このような場合は、ワイルドカード *を使用する必要があります。

```
"Resource": "*"
```

Audit Manager API アクションの多くが複数のリソースと関連します。例えば、 は、現在 にログインしている からアクセス可能な評価メタデータのリストListAssessmentsを返します AWS アカウント。したがって、ユーザーには、評価を表示するための許可が必要です。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [
      "resource1",
      "resource2"
```

Audit Managerのリソースタイプとその ARN のリストを表示するには、IAM ユーザーガイドの AWS Audit Manager で定義したリソースを参照してください。各リソースの ARN を指定できるアクションについては、AWS Audit Managerで定義されるアクションを参照してください。

複数のリソースをサポートする Audit Manager API アクションもあります。例えば、GetChangeLogs は assessmentID、controlID、および controlSetId にアクセスするため、プリンシパルにはこれらの各リソースにアクセスするための許可が必要です。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

のポリシー条件キー AWS Audit Manager

サービス固有のポリシー条件キーのサポート	部分的

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

ポリシーステートメントのプリンシパルが AWS のサービスプリンシパルになる場合は、aws:SourceArn またはポリシーのaws:SourceAccount グローバル条件キーの使用を強くお勧めします。これらのグローバル条件コンテキストキーを使用すると、混乱した代理シナリオを防ぐことができます。次の文書化されたポリシーでは、Audit Manager の aws:SourceArn と aws:SourceAccount グローバル条件コンテキストキーを使用して、混乱した代理問題を回避する方法を示します。

- Audit Manager の通知に使用される SNS トピックのポリシー例

- SNS トピックで使用される KMS キーのポリシー例

条件を指定する際にプレースホルダー変数も使用できます。例えば、ユーザー名でタグ付けされている場合のみ、リソースにアクセスするユーザーアクセス許可を付与できます。詳細については、IAM ユーザーガイドのIAM ポリシーの要素: 変数およびタグを参照してください。

Audit Manager にはサービス固有条件キーがありませんが、いくつかのグローバル条件キーの使用がサポートされています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

AWS Audit Managerのアクセスコントロールリスト (ACL)

ACL のサポート	なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

を使用した属性ベースのアクセスコントロール (ABAC) AWS Audit Manager

ABAC のサポート (ポリシー内のタグ)	はい

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義するアクセス許可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、IAM ユーザーガイドのABAC とは?を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、IAM ユーザーガイドの属性に基づくアクセスコントロール (ABAC) を使用するを参照してください。

AWS Audit Manager リソースのタグ付けの詳細については、「」を参照してくださいAWS Audit Manager リソースのタグ付け。

での一時的な認証情報の使用 AWS Audit Manager

一時的な認証情報のサポート	あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、IAM ユーザーガイドのロールへの切り替え (コンソール)を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、IAM の一時的セキュリティ認証情報を参照してください。

の転送アクセスセッション AWS Audit Manager

転送アクセスセッション (FAS) をサポート	あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のア

クションを実行するためのアクセス許可が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS Audit Managerのサービスロール

サービスロールのサポート	いいえ

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドのAWS のサービスにアクセス許可を委任するロールの作成を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS Audit Manager の機能が破損する可能性があります。Audit Manager が指示する場合以外は、サービスロールを編集しないでください。

のサービスにリンクされたロール AWS Audit Manager

サービスリンクロールのサポート	あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

のサービスにリンクされたロールの詳細については AWS Audit Manager、「」を参照してくださいのサービスにリンクされたロールの使用 AWS Audit Manager。

のアイデンティティベースのポリシーの例 AWS Audit Manager

デフォルトでは、ユーザーとロールにはAudit Manager リソースを作成または変更するための許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、ま

たは AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドの「IAM ポリシーの作成」を参照してください。

AWS Audit Managerが定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「AWS Audit Managerのアクション、リソース、および条件キー 」が「サービス認証リファレンス」にありますので参照してください。

目次

ポリシーのベストプラクティス

ID ベースのポリシーには、アカウント内で誰かがAudit Managerのリソースを作成、アクセス、または削除できるどうかが定められています。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイドのIAM でのポリシーとアクセス許可を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素:条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイドのIAM Access Analyzer ポリシーの検証を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドのIAM でのセキュリティのベストプラクティスを参照してください。

Audit Managerを有効にするために必要な最小限の許可を与える

この例は、管理者ロールのないアカウントが AWS Audit Managerを有効にできるようにする方法を示しています。

> **Note**
>
> ここでは、Audit Manager を有効にするために必要な最小限の許可を付与する基本的なポリシーを提供します。次のポリシーのすべての権限が必要です。このポリシーの一部を省略すると、Audit Managerを有効にすることができなくなります。
> 特定のニーズを満たせるよう、時間を設けて許可をカスタマイズすることをお勧めします。サポートが必要な場合は、管理者または AWS Support までお問い合わせください。

Audit Manager を使用するために必要な最小限のアクセス権を付与するには、次の許可を使用します。

```
{
    "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"
                }
            }
        }
    ]
}
```

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

AWS Audit Managerへの完全な管理者アクセス権を許可する

次のポリシー例では、 へのフル管理者アクセスを許可します AWS Audit Manager。

- 例1、(マネージドポリシーAWSAuditManagerAdministratorAccess)
- 例2 (評価レポートの宛先の許可)
- 例 3 (エクスポート先のアクセス許可)
- 例 4 (エビデンスファインダーを有効にする許可)
- 例 5 (エビデンスファインダーを無効にする許可)

例1、(マネージドポリシー**AWSAuditManagerAdministratorAccess**)

このAWSAuditManagerAdministratorAccessポリシーには、Audit Manager を有効または無効にする機能、Audit Manager 設定を変更する機能、および評価、フレームワーク、コントロール、評価レポートなどのすべての Audit Manager リソースを管理する機能が含まれます。

例2 (評価レポートの宛先の許可)

このポリシーは、特定の S3 バケットにアクセスし、そのバケットにファイルを追加したり削除したりする権限を付与します。これにより、指定したバケットを Audit Manager の評価レポートの送信先として使用できます。

placeholder text を独自の情報に置き換えます。評価レポートの送信先として使用する S3 バケットと、評価レポートの暗号化に使用するKMSキーを含める必要があります。

```
{
    "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"
        }
    ]
}
```

例 3 (エクスポート先のアクセス許可)

次のポリシーでは CloudTrail 、 が指定された S3 バケットに証拠ファインダークエリ結果を配信できるようにします。セキュリティのベストプラクティスとして、IAM グローバル条件キーは、 がイベントデータストアに対してのみ S3 バケットに CloudTrail 書き込むようにするaws:SourceArnのに役立ちます。

*###########*を以下のように自分の情報に置き換えます。

- DOC-EXAMPLE-DESTINATION-BUCKET を、エクスポート先として使用する S3 バケットに置き換えます。
- *myQueryRunningRegion* を、設定 AWS リージョン に適した に置き換えます。
- *myAccountID* を、 AWS アカウント に使用される ID に置き換えます CloudTrail。これは、S3 バケットの AWS アカウント ID と同じではない可能性があります。これが組織のイベントデータストアである場合は、管理アカウントに AWS アカウント を使用する必要があります。

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

例 4 (エビデンスファインダーを有効にする許可)

エビデンスファインダー機能を有効にして使用するには、以下の許可ポリシーが必要です。このポリシーステートメントにより、Audit Manager は CloudTrail Lake イベントデータストアを作成し、検索クエリを実行できます。

```
{
    "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/*"
         }
    ]
}
```

例 5 (エビデンスファインダーを無効にする許可)

このポリシー例は、Audit Manager のエビデンスファインダー機能を無効にする権限を付与します。これには、この機能を最初に有効にしたときに作成されたイベントデータストアの削除のが含まれます。

このポリシーを使用する前に、*placeholder text* を独自の情報に置き換えます。エビデンスファインダーを有効にしたときに作成されたイベント データ ストアの UUID を指定する必要があります。イベントデータストアの ARN は、Audit Manager の設定から取得できます。詳細については、API リファレンスGetSettingsの「」を参照してください。 AWS Audit Manager

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

ユーザーには AWS Audit Managerへの管理アクセスを許可します

この例は、管理者以外の AWS Audit Managerへの管理アクセスを許可する方法を示しています。

このポリシーは、すべての Audit Manager のリソース (評価、フレームワーク、およびコントロール) を管理できるようにしますが、Audit Manager を有効または無効にしたり、Audit Manager の設定を変更したりできるようにするものではありません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:CreateAssessment",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:CreateControl",
                "auditmanager:DeleteControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:DeleteAssessmentFrameworkShare",
```

```
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAccountStatus",
                "auditmanager:GetAssessment",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:GetControl",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:GetAssessmentReportUrl",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetDelegations",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:GetEvidenceFileUploadUrl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:GetInsights",
                "auditmanager:GetInsightsByAssessment",
                "auditmanager:GetOrganizationAdminAccount",
                "auditmanager:ListAssessments",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListControls",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:ListNotifications",
                "auditmanager:ListAssessmentControlInsightsByControlDomain",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:ListAssessmentFrameworkShareRequests",
                "auditmanager:ListControlDomainInsights",
                "auditmanager:ListControlDomainInsightsByAssessment",
                "auditmanager:ListControlInsightsByControlDomain",
                "auditmanager:ListTagsForResource",
                "auditmanager:StartAssessmentFrameworkShare",
                "auditmanager:TagResource",
                "auditmanager:UntagResource",
                "auditmanager:UpdateControl",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:UpdateAssessmentFrameworkShare",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:ValidateAssessmentReportIntegrity"
            ],
```

```
            "Resource": "*"
        },
        {
    "Sid": "ControlCatalogAccess",
    "Effect": "Allow",
    "Action": [
"controlcatalog:ListCommonControls",
"controlcatalog:ListDomains",
"controlcatalog:ListObjectives"
    ],
    "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

への読み取り専用アクセスをユーザーに許可する AWS Audit Manager

このポリシーは、評価、フレームワーク、コントロールなどの AWS Audit Manager リソースへの読み取り専用アクセスを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
```

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

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

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

```
    ]
}
```

AWS Audit Manager が Amazon SNS トピックに通知を送信することを許可する

このポリシーは、Audit Managerに既存の Amazon SNS トピックに通知を送信するための許可を付与します。

- 例 1 – Audit Manager から通知を受信する場合は、この例を使用して SNS トピックアクセスポリシーにアクセス許可を追加します。
- 例 2 – SNS トピックがサーバー側の暗号化 AWS Key Management Service (SSE AWS KMS) に () を使用している場合は、この例を使用して KMS キーアクセスポリシーにアクセス許可を追加します。

次のポリシーでは、許可を取得するプリンシパルは Audit Managerサービス プリンシパル `auditmanager.amazonaws.com` です。ポリシーステートメントのプリンシパルが AWS のサービスプリンシパルになる場合は、`aws:SourceArn` またはポリシーの`aws:SourceAccount` グローバル条件キーの使用を強くお勧めします。これらのグローバル条件コンテキストキーを使用すると、混乱した代理シナリオを防ぐことができます。

例 1(SNSトピックへの許可)

このポリシーステートメントでは、指定したSNSトピックにイベントを発行することをAudit Managerに許可します。指定したSNSトピックに発行するリクエストは、ポリシー条件を満たす必要があります。

このポリシーを使用する前に、*`placeholder text`* を独自の情報に置き換えます。以下の情報を記録します。

- このポリシーで`aws:SourceArn`条件キーを使用する場合、値は通知の送信元の Audit Manager リソースの ARNにする必要があります。以下の例では、`aws:SourceArn` リソース ID にワイルドカード (*) を使用しています。これにより、Audit Manager からのすべてのリクエストが、すべてのAudit Manager リソースで許可されます。`aws:SourceArn` グローバル条件キーには、`StringLike` または `ArnLike` の条件演算子を使用できます。ベストプラクティスとして、`ArnLike` を使用することをお勧めします。
- `aws:SourceAccount` 条件キーを使用する場合は、`StringEquals` または `StringLike` の条件演算子を使用できます。ベストプラクティスとして、`StringEquals`を使用して最小特権を実装することをお勧めします。

- aws:SourceAccountとaws:SourceArnの両方を使用する場合、アカウント値は同じアカウントIDを示す必要があります。

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

次の代替例では、StringLike 条件演算子とともに aws:SourceArn 条件キーのみを使用します。

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

次の代替例では、StringLike 条件演算子とともに aws:SourceAccount 条件キーのみを使用します。

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

例 2 (SNS トピックに添付されている KMS キーの許可)

このポリシーステートメントでは、Audit ManagerはKMSキーを使用して、証跡の暗号化を利用するデータキーを生成できます。指定されたオペレーションの KMS キーを使用するリクエストでは、ポリシーの条件が満たされている必要があります。

このポリシーを使用する前に、*placeholder text* を独自の情報に置き換えます。以下の情報を記録します。

- このポリシーでaws:SourceArn条件キーを使用する場合、値は暗号化されているリソースのARNにする必要があります。例えば、この場合はアカウントの SNS トピックです。値をARNまたはワイルドカード文字(*)を使用したARNパターンに設定します。StringLikeまたはArnLikeの条件演算子をaws:SourceArn条件キーとともに使用できます。ベストプラクティスとして、ArnLikeを使用することをお勧めします。
- aws:SourceAccount 条件キーを使用する場合は、StringEquals または StringLike の条件演算子を使用できます。ベストプラクティスとして、StringEqualsを使用して最小特権を実装することをお勧めします。SNS トピックのARNが不明の場合はaws:SourceAccountを使用できます。
- aws:SourceAccountとaws:SourceArnの両方を使用する場合、アカウント値は同じアカウントIDを示す必要があります。

```
{
     "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"
```

```
            }
        }
    }
  ]
}
```

次の代替例では、StringLike 条件演算子とともに aws:SourceArn 条件キーのみを使用します。

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

次の代替例では、StringLike 条件演算子とともに aws:SourceAccount 条件キーのみを使用します。

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

ユーザーがエビデンスファインダーで検索クエリを実行できるようにします

次のポリシーは、 CloudTrail Lake イベントデータストアでクエリを実行するアクセス許可を付与します。このアクセス許可ポリシーは、エビデンスファインダー機能を使用する場合に必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

サービス間での不分別な代理処理の防止

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、あるサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスを操作すれば、アクセス許可がない場合に、それ自身のアクセス許可を使用して、別の顧客のリソースに働きかけることができます。これを防ぐために、Amazon Web Servicesでは、顧客のすべてのサービスのデータを保護するのに役立つツールを提供しています。これには、アカウントのリソースへのアクセス許可が付与されたサービスプリンシパルを使用します。

リソースポリシーで `aws:SourceArn`および `aws:SourceAccount` のグローバル条件コンテキストキーを使用して、 がリソースにアクセスするために別のサービスに AWS Audit Manager 付与するアクセス許可を制限することをお勧めします。

- クロスサービスのアクセスにリソースを 1 つだけ関連付けたい場合は、`aws:SourceArn` を使用します。複数のリソースを指定する場合は、`aws:SourceArn`でワイルドカード (*) を使用することもできます。

  例えば、Amazon SNS トピックを使用して、Audit Manager からアクティビティ通知を受け取ることができます。この場合、SNS トピックアクセスポリシーでは、`aws:SourceArn` のARN値は通知の送信元である Audit Manager リソースです。Audit Manager リソースは複数ある可能性が高いため、ワイルドカードで`aws:SourceArn`を使用することをお勧めします。これにより、SNS トピックアクセスポリシーですべての Audit Manager リソースを指定できます。
- そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、`aws:SourceAccount` を使用します。
- Amazon S3 バケットの ARN などのアカウント ID が、`aws:SourceArn` 値に含まれていない場合、アクセス許可を制限するためには、これら両方のグローバル条件コンテキストキーを使用する必要があります。
- 両方の条件を使用する場合、および `aws:SourceArn` の値にアカウント ID が含まれている場合は、`aws:SourceAccount` の値と、`aws:SourceArn` の値のアカウントは、同じポリシーステートメントで使用するとき、同じアカウント ID を示している必要があります。

- 混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの完全な Amazon リソースネーム (ARN)が不明な場合や、複数のリソースを指定する場合には、グローバルコンテキスト条件キー aws:SourceArn で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば arn:aws:*servicename*:*:*123456789012*:* です。

Audit Managerの混乱した代理サポート

Audit Manager は、次のようなシナリオで混乱した代理サポートを提供します。これらのポリシーの例では、aws:SourceArn およびaws:SourceAccountの条件キーを使用して、混乱した代理問題を回避する方法を示します。

- ポリシー例:Audit Manager 通知の受信に使用する SNS トピック
- ポリシー例:SNS トピックの暗号化に使用する KMS キー

Audit Manager は、Audit Manager データ暗号化設定の構成 設定で指定した顧客管理キーについて、混乱した代理サポートを提供しません。独自のカスタマー管理キーを提供した場合、その KMS キーポリシーの aws:SourceAccount または aws:SourceArn 条件は使用できません。

AWS の マネージドポリシー AWS Audit Manager

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 AWS のサービス は、新しい が起動されたとき、または既存のサービスで新しい API AWS オペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

トピック

- AWS マネージドポリシー： AWSAuditManagerAdministratorAccess
- AWS マネージドポリシー： AWSAuditManagerServiceRolePolicy
- AWS Audit ManagerAWS 管理ポリシーの更新

AWS マネージドポリシー： AWSAuditManagerAdministratorAccess

`AWSAuditManagerAdministratorAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、 へのフル管理アクセスを許可する管理アクセス許可を付与します AWS Audit Manager。このアクセスには、 の有効化と無効化 AWS Audit Manager、 の設定の変更 AWS Audit Manager、評価、フレームワーク、コントロール、評価レポートなどのすべての Audit Manager リソースの管理の機能が含まれます。

AWS Audit Manager では、複数の AWS サービスにまたがる広範なアクセス許可が必要です。これは、 が複数の AWS サービスと AWS Audit Manager 統合され、評価の範囲内の AWS アカウント および サービスから証拠を自動的に収集するためです。

許可の詳細

このポリシーには、以下の許可が含まれています。

- `Audit Manager` – プリンシパルに AWS Audit Manager リソースに対する完全な許可を付与します。
- `Organizations` – プリンシパルがアカウントと組織単位を一覧表示し、委任された管理者を登録または登録解除でることを許可します。これは、マルチアカウントサポートを有効にし、 AWS Audit Manager が複数のアカウントで評価を実行し、委任された管理者アカウントに証拠を統合することができるようにするために必要です。
- `iam` – プリンシパルが IAM のユーザーを取得して一覧表示し、サービスにリンクされたロールを作成でることを許可します。これは、評価の監査所有者と受任者を指定できるようにするために必要です。また、このポリシーは、プリンシパルがサービスにリンクされたロールを削除し、削除ステータスを取得することも許可します。これは、 でサービスを無効にすることを選択した場合に AWS Audit Manager 、 がリソースをクリーンアップし、サービスにリンクされたロールを削除できるようにするために必要です AWS Management Console。
- `s3` – プリンシパルが利用可能な Amazon Simple Storage Service (Amazon S3) バケットを一覧表示することを許可します。この機能は、証拠レポートを保存する S3 バケットを指定したり、手動証拠をアップロードしたりするために必要です。

- kms – プリンシパルがキーを一覧表示および説明を記述したり、エイリアスを一覧表示したり、許可を作成したりすることを許可します。これは、データ暗号化用にカスタマーマネージドキーを選択できるようにするために必要です。
- sns – プリンシパルが Amazon SNS のサブスクリプショントピックを一覧表示することを許可します。これは、 AWS Audit Manager による通知の宛先とする SNS トピックを指定できるようにするために必要です。
- events — プリンシパルが からチェックを一覧表示および管理できるようにします AWS Security Hub。これは、 が によってモニタリングされる AWS のサービスの検出 AWS Security Hub 結果 AWS Audit Manager を自動的に収集できるようにするために必要です AWS Security Hub。その後、このデータを証拠に変換して、 AWS Audit Manager 評価に含めることができます。
- tag – プリンシパルがタグ付きリソースを取得することを許可します。これは、 AWS Audit Managerでフレームワーク、コントロール、および評価を参照するときにタグを検索フィルターとして使用できるようにするために必要です。
- controlcatalog – プリンシパルが AWS Control Catalog によって提供されるドメイン、目的、および一般的なコントロールを一覧表示できるようにします。これは、 で一般的なコントロール機能を使用できるようにするために必要です AWS Audit Manager。これらのアクセス許可を設定すると、コントロールライブラリの一般的な AWS Audit Manager コントロールのリストを表示し、ドメインと目標でコントロールをフィルタリングできます。カスタムコントロールを作成するときに、一般的なコントロールを証拠ソースとして使用することもできます。

```
{
    "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": "*"
        },
        {
     "Sid": "ControlCatalogAccess",
     "Effect": "Allow",
     "Action": [
  "controlcatalog:ListCommonControls",
  "controlcatalog:ListDomains",
  "controlcatalog:ListObjectives"
     ],
     "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシー： AWSAuditManagerServiceRolePolicy

IAM エンティティに AWSAuditManagerServiceRolePolicy をアタッチすることはできません。このポリシーは、 がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロール AWSServiceRoleForAuditManager AWS Audit Manager にアタッチされます。詳細については、「のサービスにリンクされたロールの使用 AWS Audit Manager」を参照してください。

ロール許可ポリシー AWSAuditManagerServiceRolePolicy は、 AWS Audit Manager がユーザーに代わって次のことを行うことによる自動証拠の収集を許可します。

- 以下のデータソースからデータを収集します。
  - からの管理イベント AWS CloudTrail
  - からのコンプライアンスチェック AWS Config ルール
  - からのコンプライアンスチェック AWS Security Hub
- API コールを使用して、以下の AWS のサービスのリソース構成を記述します。

> **Tip**
>
> Audit Manager がこれらのサービスから証拠を収集するために使用するAPI コールの詳細については、このガイドのカスタムコントロールデータソースでサポートされるAPI コールを参照してください。

- Amazon API Gateway
- AWS Backup
- Amazon Bedrock
- AWS Certificate Manager
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon Cognito ユーザープール
- AWS Config
- Amazon Data Firehose
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Service
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty

- AWS Identity and Access Management (IAM)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- Amazon OpenSearch サービス
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

許可の詳細

`AWSAuditManagerServiceRolePolicy` は AWS Audit Manager 、指定されたリソースに対して次のアクションを実行できます。

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `apigateway:GET`
- `autoscaling:DescribeAutoScalingGroups`
- `backup:ListBackupPlans`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`

- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses

- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions

- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport

- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices

- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters

- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - この API アクション service-linked-role は、 が利用可能な AWS アカウント の範囲内で動作します。クロスアカウントのバケットポリシーにはアクセスできません。
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains

- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups

- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "autoscaling:DescribeAutoScalingGroups",
    "backup:ListBackupPlans",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListDistributions",
    "cloudtrail:GetTrail",
    "cloudtrail:ListTrails",
    "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:DescribeContinuousBackups",
    "dynamodb:DescribeBackup",
    "dynamodb:DescribeTableReplicaAutoScaling",
```

```
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeInstanceCreditSpecifications",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeVpcEndpointConnections",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:GetLaunchTemplateData",
    "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:GetAccessKeyLastUsed",
    "iam:GetCredentialReport",
    "iam:GetGroupPolicy",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetUserPolicy",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:ListAttachedGroupPolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupsForUser",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "iam:ListPolicyVersions",
    "iam:ListAccessKeys",
    "iam:ListAttachedRolePolicies",
    "iam:ListMfaDeviceTags",
    "iam:ListMfaDevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
```

```
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "logs:GetDataProtectionPolicy",
    "es:DescribeDomains",
    "es:DescribeDomain",
    "es:DescribeDomainConfig",
    "es:ListDomainNames",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDBClusterEndpoints",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBInstances",
    "rds:DescribeDBSecurityGroups",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeLoggingStatus",
    "route53:GetQueryLoggingConfig",
    "sagemaker:DescribeAlgorithm",
    "sagemaker:DescribeFlowDefinition",
    "sagemaker:DescribeHumanTaskUi",
    "sagemaker:DescribeModelBiasJobDefinition",
    "sagemaker:DescribeModelCard",
    "sagemaker:DescribeModelQualityJobDefinition",
    "sagemaker:DescribeDomain",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeLabelingJob",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeTrainingJob",
```

```
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetRule",
        "waf-regional:GetWebAcl",
        "waf:GetRule",
        "waf:GetRuleGroup",
        "waf:ListActivatedRulesInRuleGroup",
        "waf:ListWebAcls",
        "wafv2:ListWebAcls",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf-regional:ListRules",
        "waf:ListRuleGroups",
        "waf:ListRules"
    ],
    "Resource": "*",
    "Sid": "APIsAccess"
```

```
  },
  {
   "Sid": "S3Access",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketAcl",
    "s3:GetBucketLogging",
    "s3:GetBucketOwnershipControls",
    "s3:GetBucketPolicy",
    "s3:GetBucketTagging"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "APIGatewayAccess",
   "Effect": "Allow",
   "Action": [
    "apigateway:GET"
   ],
   "Resource": [
    "arn:aws:apigateway:*::/restapis",
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/restapis/*/stages"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${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 ManagerAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS Audit Manager 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、 AWS Audit Manager ドキュメント履歴ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
AWSAuditManagerServiceRolePolicy - 既存ポリシーへの更新	次のアクセス許可が に追加されましたAWSAuditManagerServiceRolePolicy 。 AWS Audit Manager は次のアクションを実行して、 のリソースに関する自動証拠を収集できるようになりました AWS アカウント。 • sagemaker:DescribeAlgorithm • sagemaker:DescribeDomain • sagemaker:DescribeEndpoint • sagemaker:DescribeFlowDefinition • sagemaker:DescribeHumanTaskUi • sagemaker:DescribeLabelingJob • sagemaker:DescribeModel • sagemaker:DescribeModelBiasJobDefinition • sagemaker:DescribeModelCard • sagemaker:DescribeModelQualityJobDefinition • sagemaker:DescribeTrainingJob • sagemaker:DescribeUserProfile • sagemaker:ListAlgorithms • sagemaker:ListDomains • sagemaker:ListEndpoints • sagemaker:ListFlowDefinitions • sagemaker:ListHumanTaskUis • sagemaker:ListLabelingJobs • sagemaker:ListModels	06/10/2024

変更	説明	日付
	• sagemaker:ListModelBiasJobDefinitions • sagemaker:ListModelCards • sagemaker:ListModelQualityJobDefinitions • sagemaker:ListMonitoringAlerts • sagemaker:ListMonitoringSchedules • sagemaker:ListTrainingJobs • sagemaker:ListUserProfiles	

変更	説明	日付
AWSAuditManagerServiceRolePolicy – 既存ポリシーへの更新	次のアクセス許可が に追加されましたAWSAuditManagerServiceRolePolicy 。 AWS Audit Manager は次のアクションを実行して、 のリソースに関する自動証拠を収集できるようになりました AWS アカウント。 • iam:ListAttachedGroupPolicies • iam:ListAttachedUserPolicies • iam:ListGroupsForUser • es:ListDomainNames また、ポリシー () の APIGatewayAccess セクションに新しいリソースを追加しましたarn:aws:apigateway:*::/restapis 。 このポリシーは、API Gateway REST API のステージとステージリソースだけでなく、REST APIs APIs 自体に対しても、指定されたアクセス許可 (この場合は apigateway:GET アクション) を付与するようになりました。この変更により、ポリシーの範囲が効果的に拡張され、API Gateway REST APIs に関連するステージとステージリソースに加えて、API Gateway REST APIs。	05/17/2024

変更	説明	日付
AWSAuditManagerAdministratorAccess – 既存ポリシーへの更新	次のアクセス許可を`AWSAuditManagerAdministratorAccess` に追加しました。 • `controlcatalog:ListCommonControls` • `controlcatalog:ListDomains` • `controlcatalog:ListObjectives` この更新により、コントロールドメイン、コントロール目標、および AWS Control Catalog によって提供される一般的なコントロールを表示できます。これらのアクセス許可は、 で一般的なコントロール機能を使用する場合に必要です AWS Audit Manager。	05/15/2024

変更	説明	日付
AWSAuditManagerServiceRolePolicy – 既存ポリシーへの更新	次のアクセス許可が に追加されましたAWSAuditManagerServiceRolePolicy 。 AWS Audit Manager は次のアクションを実行して、 のリソースに関する自動証拠を収集できるようになりました AWS アカウント。 • apigateway:GET • autoscaling:DescribeAutoScalingGroups • backup:ListBackupPlans • cloudfront:GetDistribution • cloudfront:GetDistributionConfig • cloudfront:ListDistributions • cloudtrail:GetTrail • cloudtrail:ListTrails • dynamodb:DescribeContinuousBackups • dynamodb:DescribeBackup • dynamodb:DescribeTableReplicaAutoScaling • ec2:DescribeInstanceCreditSpecifications • ec2:DescribeInstanceAttribute • ec2:DescribeSecurityGroupRules • ec2:DescribeVpcEndpointConnections • ec2:DescribeVpcEndpointServiceConfigurations • ec2:GetLaunchTemplateData	05/15/2024

変更	説明	日付
	• es:DescribeDomains • es:DescribeDomain • es:DescribeDomainConfig • iam:GetAccessKeyLastUsed • iam:GetGroupPolicy • iam:GetPolicy • iam:GetPolicyVersion • iam:GetRolePolicy • iam:GetUser • iam:GetUserPolicy • iam:ListAccessKeys • iam:ListAttachedRolePolicies • iam:ListMfaDeviceTags • iam:ListMfaDevices • iam:ListPolicyVersions • logs:GetDataProtectionPolicy • rds:DescribeDBInstanceAutomatedBackups • rds:DescribeDBClusterEndpoints • rds:DescribeDBClusterParameterGroups • redshift:DescribeClusterSnapshots • redshift:DescribeLoggingStatus • s3:GetBucketAcl • s3:GetBucketLogging • s3:GetBucketOwnershipControls • s3:GetBucketTagging • sagemaker:DescribeEndpointConfig	

変更	説明	日付
	• sagemaker:ListEndpointConfigs • secretsmanager:DescribeSecret • secretsmanager:ListSecrets • sns:ListTagsForResource • waf-regional:GetRule • waf-regional:GetWebAcl • waf-regional:ListRules • waf:GetRule • waf:GetRuleGroup • waf:ListRuleGroups • waf:ListRules • waf:ListWebAcls • wafv2:ListWebAcls	
AWSAuditManagerServiceRolePolicy – 既存ポリシーへの更新	サービスにリンクされたロールで、 AWS Audit Manager が s3:GetBucketPolicy アクションを実行できるようになりました。 この API アクションは、AWS 生成 AI ベストプラクティスフレームワーク v1 をサポートするために必要です。これにより、Audit Manager では、生成 AI モデルのトレーニングデータセットに適用されているポリシー制限に関する証拠を自動的に収集できます。 GetBucketPolicy アクション service-linked-role は、 AWS アカウント が利用可能な の範囲内で動作します。クロスアカウントのバケットポリシーにはアクセスできません。	12/06/2023

変更	説明	日付
AWSAuditManagerServiceRolePolicy – 既存ポリシーへの更新	次のアクセス許可が に追加されましたAWSAuditManagerServiceRolePolicy 。 AWS Audit Manager は次のアクションを実行して、 のリソースに関する自動証拠を収集できるようになりました AWS アカウント。 • 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

変更	説明	日付
	• 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	

変更	説明	日付
	• 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	

変更	説明	日付
	• 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 – 既存ポリシーへの更新	次のアクセス許可をAWSAuditManagerServiceRolePolicy に追加しました。 • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

変更	説明	日付
AWSAuditManagerServiceRolePolicy – 既存ポリシーへの更新	サービスにリンクされたロールで、 AWS Audit Manager が `organizations:DescribeOrganization` アクションを実行できるようになりました。 また、`CreateEventsAccess` リソースの範囲をワイルドカード (*) から特定のタイプのリソース (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`) に絞り込みました。 最後に、ソース値が存在し、その値が NULL でないことを確認するための `events:source` 条件キーに `Null` 条件演算子を追加しました。	05/20/2022
AWSAuditManagerAdministratorAccess – 既存ポリシーへの更新	`events:source` のキー条件ポリシーを更新して、これが複数値キーであることを反映しました。	04/29/2022
AWSAuditManagerServiceRolePolicy – 既存ポリシーへの更新	`events:source` のキー条件ポリシーを更新して、これが複数値キーであることを反映しました。	03/16/2022
AWS Audit Manager が変更の追跡を開始しました	AWS Audit Manager が AWS マネージドポリシーの変更の追跡を開始しました。	05/06/2021

AWS Audit Manager ID とアクセスのトラブルシューティング

次の情報は、Audit Manager と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- でアクションを実行する権限がない AWS Audit Manager
- iam を実行する権限がありません。PassRole

- 自分の 以外のユーザーに自分の AWS Audit Manager リソース AWS アカウント へのアクセスを許可したい

でアクションを実行する権限がない AWS Audit Manager

このAccessDeniedExceptionエラーは、ユーザーに AWS Audit Manager または Audit Manager API オペレーションを使用するアクセス許可がない場合に表示されます。

この場合、管理者はポリシーを更新して、ユーザーにアクセスを許可する必要があります。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新してAudit Managerにロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用してAudit Manager でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに自分の AWS Audit Manager リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- AWS Audit Manager がこれらの機能をサポートしているか確認するには、「が IAM と AWS Audit Manager 連携する方法」を参照してください。
- 所有している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの AWS アカウント「所有している別の の IAM ユーザーへのアクセスを提供する」を参照してください。AWS アカウント
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

のサービスにリンクされたロールの使用 AWS Audit Manager

AWS Audit Manager は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、Audit Manager に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、Audit Manager によって事前定義されており、サービスがユーザーに代わって他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、設定 AWS Audit Manager が簡単になります。Audit Manager は、サービスにリンクされたロールの許可を定義します。特に定義されている場合を除き、Audit Manager のみがそのロールを引き受けることができます。定義されたアクセス許可には、信頼ポリシーとアクセス権限ポリシーが含まれ、そのアクセス権限ポリシーを他の IAM エンティティに適用することはできません。

サービスリンクロールをサポートするその他のサービスについては、「IAM と連携する AWS のサービス」を参照のうえ、[Service-Linked Role] (サービスリンクロール) 列が [Yes] (はい) になっているサービスを探してください。そのサービスに関するサービスにリンクされたロールのドキュメントを表示するには、リンクが設定されている Yes] (はい) を選択します。

のサービスにリンクされたロールのアクセス許可 AWS Audit Manager

Audit Manager は、 という名前のサービスにリンクされたロールを使用します。これにより**AWSServiceRoleForAuditManager**、 が使用または管理する AWS のサービスおよびリソースにアクセスできます AWS Audit Manager。

`AWSServiceRoleForAuditManager` サービスにリンクされたロールは、ロールを継承するために `auditmanager.amazonaws.com` のサービスを信頼します。

ロールのアクセス許可ポリシー により`AWSAuditManagerServiceRolePolicy`、Audit Manager は AWS 使用状況に関する自動証拠を収集できます。具体的には、ユーザーに代わって以下のアクションを実行できます。

- Audit Manager は、 を使用してコンプライアンスチェックの証拠 AWS Security Hub を収集できます。この場合、Audit Manager は次のアクセス許可を使用して、セキュリティチェックの結果をから直接報告します AWS Security Hub。次に、その結果を証拠として関連する評価コントロールに添付します。
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Audit Manager が記述できる特定の Security Hub コントロールの詳細については、「AWS Audit ManagerでサポートされているAWS Security Hub コントロール」を参照してください。

- Audit Manager は、 を使用してコンプライアンスチェックの証拠 AWS Config を収集できます。この場合、Audit Manager は次のアクセス許可を使用して、 AWS Config ルール評価の結果を から直接報告します AWS Config。次に、その結果を証拠として関連する評価コントロールに添付します。
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

  > **Note**
  >
  > Audit Manager が記述できる特定の AWS Config ルールの詳細については、「 AWS Config でサポートされているルール AWS Audit Manager」を参照してください。

- Audit Manager は、 を使用してユーザーアクティビティの証拠 AWS CloudTrail を収集できます。この場合、Audit Manager は次のアクセス許可を使用してログからユーザーアクティビティをキャプチャします CloudTrail 。次に、そのアクティビティを証拠として関連する評価コントロールに添付します。
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

  > **Note**
  >
  > Audit Manager が記述できる特定の CloudTrail イベントの詳細については、「AWS CloudTrail でサポートされているイベント名 AWS Audit Manager」を参照してください。

- Audit Manager は AWS API コールを使用してリソース設定の証拠を収集できます。この場合、Audit Manager は次の許可を使用して、以下の AWS のサービスのリソース設定を記述する読み取り専用 API を呼び出します。次に、API レスポンスを証拠として関連する評価コントロールに添付します。
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `apigateway:GET`
  - `autoscaling:DescribeAutoScalingGroups`
  - `backup:ListBackupPlans`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`
  - `bedrock:ListModelCustomizationJobs`
  - `cloudfront:GetDistribution`
  - `cloudfront:GetDistributionConfig`
  - `cloudfront:ListDistributions`
  - `cloudtrail:DescribeTrails`

- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways

- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations

- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser

- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions

- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - この API アクション service-linked-role は、 が利用可能な AWS アカウント の範囲内で動作します。クロスアカウントのバケットポリシーにはアクセスできません。

- s3:GetBucketPublicAccessBlock

- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts

- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

> **Note**
>
> Audit Managerで記述できる特定のAPI コールの詳細についてはカスタムコントロールデータソースでサポートされるAPI コールを参照してください。

サービスにリンクされたロール のアクセス許可の詳細については`AWSServiceRoleForAuditManager`、「 AWS マネージドポリシーリファレンスガイドAWSAuditManagerServiceRolePolicy」の「」を参照してください。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「Service-linked role permissions」を参照してください。

AWS Audit Manager サービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。を有効にすると AWS Audit Manager、サービスにリンクされたロールが自動的に作成されます。Audit Manager は、 のオンボーディングページから AWS Management Console、または API または を使用して有効にできます AWS CLI。詳細については、ユーザーガイドの「の有効化 AWS Audit Manager」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。

AWS Audit Manager サービスにリンクされたロールの編集

AWS Audit Manager では、`AWSServiceRoleForAuditManager`サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、IAM ユーザーガイドの「サービスリンクロールの編集」を参照してください。

: IAM エンティティが **`AWSServiceRoleForAuditManager`** サービスリンクロールの説明を編集することを許可します

サービスにリンクされたロールの説明を編集する必要のある IAM エンティティの許可ポリシーに次のステートメントを追加します。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

AWS Audit Manager サービスにリンクされたロールの削除

Audit Managerを使用する必要がなくなった場合は、AWSServiceRoleForAuditManager サービスリンクロールを削除することをお勧めします。これにより、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスにリンクされたロールのクリーンアップ

IAM を使用して Audit Manager サービスリンクロールを削除するには、まずそのロールにアクティブなセッションがないことを確認し、そのロールで使用されているリソースをすべて削除する必要があります。そのためには、Audit Manager がすべての で登録解除されていることを確認します AWS リージョン。登録を解除すると、Audit Manager はサービスリンクロールを使用しなくなります。

Audit Managerの登録解除の方法については以下のリソースを参照してください。

- このガイドの「無効化 AWS Audit Manager」
- 「DeregisterAccount API リファレンス」の「AWS Audit Manager 」
- AWS CLI のリファレンス AWS Audit Managerの deregister-account

Audit Manager リソースを手動で削除する方法については、本ガイドの「Audit Manager データの削除」を参照してください。

サービスリンクロールの削除

サービスリンクロールは、IAM コンソール、 AWS Command Line Interface (AWS CLI)、または IAM API を使用して削除することができます。

IAM console

以下の手順に従って、IAMコンソールでサービスリンクロールを削除してください。

サービスにリンクされたロールを削除するには (コンソール)

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. IAM コンソールのナビゲーションペインで [ロール] を選択します。AWSServiceRoleForAuditManager の横のチェックボックス (名前または行自体ではなく) を選択します。
3. ページ上部にある [ロールのアクション] で [削除] を選択します。

4. 確認ダイアログボックスで、最終アクセス情報を確認します。これは、選択したそれぞれのロールの AWS のサービスへの最終アクセス時間を示します。これは、そのロールが現在アクティブであるかどうかを確認するのに役立ちます。先に進む場合は、テキスト入力フィールドに **AWSServiceRoleForAuditManager** と入力し、[削除]を選択して、削除するサービスリンクロールを送信します。
5. IAM コンソール通知を見て、サービスにリンクされたロールの削除の進行状況をモニタリングします。IAM サービスにリンクされたロールの削除は非同期であるため、削除するロールを送信すると、削除タスクは成功または失敗する可能性があります。タスクが成功した場合は、ロールがリストから削除され、成功のメッセージがページの上部に表示されます。

AWS CLI

から IAM コマンドを使用して AWS CLI 、サービスにリンクされたロールを削除できます。

サービスにリンクされたロールを削除するには (AWS CLI)

1. 次のコマンドを入力して、アカウント内のロールを一覧表示します。

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. サービスにリンクされているロールは、使用されている、または関連するリソースがある場合は削除できないため、削除リクエストを送信する必要があります。これらの条件が満たされない場合、そのリクエストは拒否される可能性があります。レスポンスから deletion-task-id を取得して、削除タスクのステータスを確認する必要があります。

   サービスにリンクされたロールの削除リクエストを送信するには、次のコマンドを入力します：

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. 削除タスクのステータスを確認するには、次のコマンドを入力します：

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

   削除タスクのステータスは、NOT_STARTED、IN_PROGRESS、SUCCEEDED、または FAILED となります。削除が失敗した場合は、失敗した理由がコールによって返され、トラブルシューティングが可能になります。

IAM API

IAM API を使用して、サービスにリンクされたロールを削除できます。

サービスにリンクされたロールを削除するには (API)

1. を呼び出しGetRoleて、アカウントのロールを一覧表示します。リクエストで AWSServiceRoleForAuditManagerをRoleNameとして指定します。
2. サービスにリンクされているロールは、使用されている、または関連するリソースがある場合は削除できないため、削除リクエストを送信する必要があります。これらの条件が満たされない場合、そのリクエストは拒否される可能性があります。レスポンスから DeletionTaskId を取得して、削除タスクのステータスを確認する必要があります。

   サービスにリンクされたロールの削除リクエストを送信するには、 を呼び出しますDeleteServiceLinkedRole。リクエストで AWSServiceRoleForAuditManagerをRoleNameとして指定します。
3. 削除のステータスを確認するには、 を呼び出しますGetServiceLinkedRoleDeletionStatus。リクエストで DeletionTaskId を指定します。

   削除タスクのステータスは、NOT_STARTED、IN_PROGRESS、SUCCEEDED、または FAILED となります。削除が失敗した場合は、失敗した理由がコールによって返され、トラブルシューティングが可能になります。

Audit Manager のサービスにリンクされたロールを削除するためのヒント

Audit Manager のサービスにリンクされたロールの削除プロセスは、Audit Manager がロールを使用しているか、リソースが関連付けられている場合に失敗することがあります。これは、次のシナリオで発生する可能性があります。

1. アカウントは、1 つ以上の で Audit Manager に登録されています AWS リージョン。
2. アカウントは AWS 組織の一部であり、管理アカウントまたは委任された管理者アカウントは引き続き Audit Manager にオンボーディングされます。

削除の失敗の問題を解決するには、まず AWS アカウント が Organization の一部であるかどうかを確認します。これを行うには、 DescribeOrganization API オペレーションを呼び出すか、コンソールに移動します AWS Organizations 。

AWS アカウント が組織の一部である場合

1. 管理アカウントを使用して、Audit Manager で委任された管理者を追加 AWS リージョン したすべての を削除します。
2. 管理アカウントを使用して、サービスを使用したすべての AWS リージョン で Audit Manager の登録を解除します。
3. 前の手順の手順に従って、サービスにリンクされたロールの削除を再試行してください。

AWS アカウント が組織に属していない場合

1. サービス AWS リージョン を使用したすべての で、Audit Manager の登録を解除したことを確認してください。
2. 前の手順の手順に従って、サービスにリンクされたロールの削除を再試行してください。

Audit Manager から登録を解除すると、サービスはサービスにリンクされたロールの使用を停止します。その後、ロールを正常に削除できます。

AWS Audit Manager サービスにリンクされたロールでサポートされているリージョン

AWS Audit Manager は、サービス AWS リージョン が利用可能なすべての でサービスにリンクされたロールの使用をサポートします。詳細については、AWS サービスエンドポイントを参照してください。

のコンプライアンス検証 AWS Audit Manager

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべての AWS のサービス が HIPAA の対象となるわけではありません。詳細については、HIPAA 対応サービスのリファレンスを参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性について AWS Audit Manager

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョンを提供します。

アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS Audit Manager

マネージドサービスである AWS Audit Manager は AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開した API コールを使用して、ネットワーク経由で AWS Audit Manager にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

これらの API オペレーションは任意のネットワークの場所から呼び出すことができますが、 AWS Audit Manager はリソースベースのアクセスポリシーをサポートしています。これには、送信元 IP

アドレスに基づく制限を含めることができます。また、Audit Manager ポリシーを使用して、特定の Amazon Virtual Private Cloud (Amazon VPC) エンドポイントまたは特定の VPC からのアクセスを制御することもできます。これにより、実質的にネットワーク内の特定の VPC からのみ、特定の Audit Manager リソースへの AWS ネットワークアクセスが分離されます。

AWS Audit Manager およびインターフェイス VPC エンドポイント (AWS PrivateLink)

VPC と の間にプライベート接続を確立するには、インターフェイス VPC エンドポイント AWS Audit Manager を作成します。インターフェイスエンドポイントは、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続なしで Audit Manager API にプライベートにアクセスできるようにするテクノロジーである AWS PrivateLink を利用しています。VPC のインスタンスは、パブリック IP アドレスがなくても Audit Manager API と通信できます。VPC と 間のトラフィック AWS Audit Manager は、 AWS ネットワークを離れません。

各インターフェイスエンドポイントは、サブネット内の 1 つ、または複数の Elastic Network Interface によって表されます。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

AWS Audit Manager VPC エンドポイントに関する考慮事項

のインターフェイス VPC エンドポイントを設定する前に AWS Audit Manager、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントのプロパティと制限」を確認してください。

AWS Audit Manager は、VPC からのすべての API アクションの呼び出しをサポートします。

AWS Audit Managerのインターフェイス VPC エンドポイントの作成

Amazon VPC コンソールまたは AWS Command Line Interface () を使用して、 AWS Audit Manager サービスの VPC エンドポイントを作成できますAWS CLI。詳細については、 Amazon VPC ユーザーガイド のインターフェイスエンドポイントの作成を参照してください。

次のサービス名 AWS Audit Manager を使用して、 用の VPC エンドポイントを作成します。

- `com.amazonaws.region.auditmanager`

エンドポイントのプライベート DNS を有効にすると、 など、リージョンのデフォルトの DNS 名 AWS Audit Manager を使用して に API リクエストを実行できますauditmanager.us-east-1.amazonaws.com。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントを介したサービスへのアクセス」を参照してください。

の VPC エンドポイントポリシーの作成 AWS Audit Manager

VPC エンドポイントには、 AWS Audit Managerへのアクセスを制御するエンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

例: AWS Audit Manager アクションの VPC エンドポイントポリシー

のエンドポイントポリシーの例を次に示します AWS Audit Manager。このポリシーは、エンドポイントにアタッチされると、すべてのリソースのすべてのプリンシパルに対して、登録されている Audit Manager アクションへのアクセスを許可します。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessment",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

でのログ記録とモニタリング AWS Audit Manager

モニタリングは、Audit Manager およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。 AWS は、Audit Manager をモニタリングし、問題が発生したときに報告し、必要に応じて自動アクションを実行するための以下のモニタリングツールを提供します。

- AWS CloudTrailは、 AWS アカウント により、またはそのアカウントに代わって行われた API コールや関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。AWSを呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、『AWS CloudTrail ユーザーガイド』を参照してください。
- Amazon EventBridge は、アプリケーションをさまざまなソースからのデータに簡単に接続できるサーバーレスイベントバスサービスです。 は、独自のアプリケーション、S oftware-as-aサービス (SaaS) アプリケーション、および AWS のサービスからリアルタイムデータのストリームを EventBridge 配信し、そのデータを Lambda などのターゲットにルーティングします。これにより、サービスで発生したイベントをモニタリングし、イベント駆動型アーキテクチャを構築できます。詳細については、「Amazon ユーザーガイド EventBridge 」を参照してください。

Amazon AWS Audit Manager によるモニタリング EventBridge

Amazon EventBridge では、 を自動化 AWS のサービス し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に対応できます。

ルールを使用して EventBridge、Audit Manager イベントを検出して対応できます。作成したルールに基づいて、イベントがルールで指定した値と一致すると、 は 1 つ以上のターゲットアクションを EventBridge 呼び出します。イベントのタイプに応じて、通知の送信、イベント情報の取得、是正措置の実施、またはその他の対策を行うことができます。

例えば、次のAudit Manager イベントがアカウントで発生するたびに検出できます。

- 監査所有者が評価を作成、更新、または削除します
- 監査所有者がレビューのためにコントロールセットを委任します
- 代理人はレビューを完了し、レビューされたコントロールセットを監査所有者に返送します
- 監査所有者が評価コントロールのステータスを更新します

自動的にトリガーできるオペレーションには、以下が含まれます。

- AWS Lambda 関数を使用して、Slack チャンネルに通知を渡します。
- チェックに関するデータをAmazon Kinesis Data Streamsにプッシュして、包括的でリアルタイムのステータスモニタリングをサポートします。
- Amazon Simple Notification Service (Amazon SNS)トピックをお客様のメールアドレスに送信します。
- Amazon CloudWatch アラームアクションの通知を受け取ります。

> **Note**
>
> Audit Manager は永続的にイベントを配信します。つまり、Audit Manager は EventBridge 少なくとも 1 回はイベントを配信しようとします。 EventBridge サービスの中断によりイベントを配信できない場合、後で Audit Manager によって最大 24 時間再試行されます。

EventBridge Audit Manager の形式例

次の JSON コードは、Audit Manager での評価作成イベントの例を示しています。このイベントのフィールドの詳細については、「イベント構造リファレンス」を参照してください。

```
{
    "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"
    }
}
```

EventBridge ルールを作成するための前提条件

Audit Manager イベントのルールを作成する前に、次のことを行うことをお勧めします。

- のイベント、ルール、ターゲットについて理解します EventBridge。詳細については、「Amazon ユーザーガイド」の「Amazon EventBridgeとは」を参照してください。 EventBridge
- イベントルールで使用するターゲットを作成します。例えば、Amazon SNS トピックを作成して、コントロールセットのレビューが完了するたびにテキストメッセージまたは電子メールを受信することもできます。詳細については、「 EventBridge ターゲット」を参照してください。

Audit Manager の EventBridge ルールの作成

Audit Manager が出力するイベントでトリガーする EventBridge ルールを作成するには、次の手順に従います。イベントは、ベストエフォートベースで発生します。

Audit Manager の EventBridge ルールを作成するには

1. https://console.aws.amazon.com/events/ で Amazon EventBridge コンソールを開きます。
2. ナビゲーションペインで ルール] を選択します。
3. ルールの作成 を選択します。
4. [ルールの詳細を定義] ページで、ルールの名前と説明を入力します。
5. [Event bus] (イベントバス) と [Rule type] (ルールタイプ) のデフォルト値を維持して、[Next] (次へ) を選択します。
6. ビルドイベントパターンページのイベントソース で、AWS イベントまたは EventBridge パートナーイベント を選択します。
7. [作成方法] セクションで、[カスタムパターン (JSON エディタ)] を選択します。
8. [イベントパターン] で、イベントパターンをJSON で記述し、マッチングに使用するフィールドを指定します。

   Audit Manager イベントと一致させるには、次の簡単なパターンを使用できます。

   ```
   {
   ```

```
  "detail-type": ["Event"]
}
```

を以下のサポートされている値のいずれかに置き換えてください。

a. Assessment Createdと入力すると、評価が作成されたときに通知が届きます。

b. Assessment Updatedと入力すると、評価が更新されたときに通知が届きます。

c. Assessment Deletedと入力すると、評価が削除されたときに通知が届きます。

d. Assessment ControlSet Delegation Createdと入力すると、コントロールセットのレビューを委任されたときに通知が届きます。

e. Assessment ControlSet Reviewedと入力すると、評価コントロールセットがレビューされたときに通知が届きます。

f. Assessment Control Reviewedと入力すると、評価コントロールがレビューされたときに通知が届きます。

> **Tip**
>
> 必要に応じてイベントパターンにフィールドを追加してください。使用可能なフィールドの詳細については、「Amazon EventBridge イベントパターン」を参照してください。

9. [次へ] をクリックします。

10. [ターゲットを選択] ページで、このルール用に作成したターゲットタイプを選択してから、そのタイプに必要な追加のオプションを設定します。例えば、Amazon SNS を選択した場合、メールまたは SMS で通知されるように SNS トピックが正しく設定されていることを確認してください。

> **Tip**
>
> 表示されるフィールドは、選択したサービスによって異なります。使用可能なターゲットの詳細については、「 EventBridge コンソールで利用可能なターゲット」を参照してください。

11. 多くのターゲットタイプでは、 はターゲットにイベントを送信するためのアクセス許可 EventBridge が必要です。このような場合は、ルールの実行に必要な IAM ロール EventBridge を作成できます。

a. 自動的に IAM ロールを作成するには、[Create a new role for this specific resource (この特定のリソースに対して新しいロールを作成する)] を選択します。

b. 以前に作成した IAM ロールを使用するには、[Use existing role (既存のロールの使用)] を選択します。

12. (オプション) 別のターゲットを追加] を選択して、このルールに別のターゲットを追加します。
13. 次へ をクリックします。
14. (オプション) [Configure tags] (タグの設定) ページで、いずれかのタグを追加し、[Next] (次へ) を選択します。
15. [Review and create] (確認および作成) ページで、ルールの設定を確認し、イベントモニタリング要件を満たしていることを確認してください。
16. [Create rule (ルールの作成)] を選択します。これでルールはAudit Managerイベントをモニタリングし、指定したターゲットに送信するようになります。

を使用した AWS Audit Manager API コールのログ記録 CloudTrail

Audit Manager は、ユーザー CloudTrail、ロール、または Audit Manager の によって実行されたアクションを記録するサービスである と統合 AWS のサービス されています。 は、Audit Manager のすべての API コールをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、Audit Manager コンソールからの呼び出しと、Audit Manager API 操作へのコード呼び出しが含まれます。

証跡を作成する場合は、Audit Manager の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。

によって収集された情報を使用して CloudTrail、Audit Manager に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

の Audit Manager 情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 で が有効になります。Audit Manager でアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS のサービス イベントとともにイベントに記録されます。

で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

Audit Manager のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。

さらに、他の を設定 AWS のサービス して、 CloudTrail ログで収集されたイベントデータをさらに分析し、それに基づく対応を行うことができます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail サポートされているサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからのログファイルの受信 CloudTrail

すべての Audit Manager アクションは によってログに記録 CloudTrail され、 AWS Audit Manager API リファレンス に記載されています。例えば、、`CreateControl`、および `UpdateAssessmentFramework` API オペレーションを呼び出すと`DeleteControl`、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストが、ルートユーザーの認証情報で行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、CloudTrail userIdentity Element」を参照してください。

Audit Managerのログ・ファイルエントリーを理解する

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパ

ラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 CreateAssessmentアクションを示す CloudTrail ログエントリを示しています。

```
{
      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"
    }
```

での設定と脆弱性の分析について AWS Audit Manager

設定と IT コントロールは、 AWS とお客様の間で共有される責任です。詳細については、 AWS 「 責任共有モデル」を参照してください。

を使用した AWS Audit Manager リソースの作成 AWS CloudFormation

AWS Audit Manager は AWS CloudFormation、 AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップに役立つサービスである と統合されています。必要なすべての AWS リソース (評価など) を記述するテンプレートを作成し、それらのリソースを AWS CloudFormation プロビジョニングして設定します。

を使用すると AWS CloudFormation、テンプレートを再利用して Audit Manager リソースを一貫して繰り返しセットアップできます。リソースを一度記述し、複数の AWS アカウントとリージョンで同じリソースを何度もプロビジョニングします。

Audit Manager と AWS CloudFormation テンプレート

Audit Manager および関連サービスのリソースをプロビジョニングして設定するには、AWS CloudFormation テンプレートについて理解しておく必要があります。テンプレートは、JSON や YAML でフォーマットされたテキストファイルです。これらのテンプレートは、 AWS CloudFormation スタックでプロビジョニングするリソースを記述します。JSON または YAML に慣れていない場合は、デザイナー を使用して AWS CloudFormation AWS CloudFormation テンプレートの使用を開始できます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation Designer とは」を参照してください。

Audit Manager は、 での評価の作成をサポートしています AWS CloudFormation。これらのリソースの JSON テンプレートと YAML テンプレートの例を含む詳細については、AWS CloudFormation ユーザーガイドの「AWS Audit Manager リソースタイプのリファレンス」を参照してください。

の詳細 AWS CloudFormation

の詳細については AWS CloudFormation、以下のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

AWS SDK AWS Audit Manager での の使用

AWS Software Development Kit (SDKsは、多くの一般的なプログラミング言語で使用できます。各 SDK には、デベロッパーが好みの言語でアプリケーションを構築する際に使用できる API、コード例、およびドキュメントが提供されています。

SDK ドキュメント	このサービス固有のドキュメント	コードの例	
AWS SDK for C++	AWS SDK for C++ Audit Manager の API リファレンス	AWS SDK for C++ コード例	
AWS SDK for Go	AWS SDK for Go Audit Manager の API リファレンス	AWS SDK for Go コード例	
AWS SDK for Java	AWS SDK for Java 2.x Audit Manager の API リファレンス	AWS SDK for Java コード例	
AWS SDK for JavaScript	AWS SDK for JavaScript Audit Manager の API リファレンス	AWS SDK for JavaScript コード例	
AWS SDK for .NET	AWS SDK for .NET Audit Manager の API リファレンス	AWS SDK for .NET コード例	
AWS SDK for PHP	AWS SDK for PHP Audit Manager の API リファレンス	AWS SDK for PHP コード例	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto) Audit Manager の API リファレンス	AWS SDK for Python (Boto3) コード例	
AWS SDK for Ruby	AWS SDK for Ruby Audit Manager の API リファレンス	AWS SDK for Ruby コード例	

このサービスに固有の例については、AWS SDKs」を参照してください。

> **Note**
>
> Audit Manager は、の botocore バージョン 1.19.32 以降で AWS SDK for Python (Boto3)使用できます。SDK の使用を開始する前に、適切な botocore バージョンを使用していることを確認してください。

無効化 AWS Audit Manager

サービスを使用しない場合は、Audit Manager を無効にできます。Audit Manager を無効にすると、データをすべて削除するオプションもあります。

デフォルトでは、Audit Manager を無効にしてもデータは削除されません。エビデンスデータは作成時から 2 年間保持されます。その他の Audit Manager リソース (評価、カスタムコントロール、カスタムフレームワークを含む)は無期限に保持され、将来、Audit Manager を再有効化する場合に使用できるようになります。データ保持の詳細については、本ガイドの「データ保護」を参照してください。

データの削除を選択すると、Audit Manager は、作成したすべての Audit Manager リソース (評価、カスタムコントロール、カスタムフレームワークを含む)とともにすべての証拠データを削除します。すべてのデータは、Audit Manager を無効にしてから 7 日以内に削除されます。

トピック

手順

Audit Manager は、Audit Manager コンソール、 AWS Command Line Interface （ AWS CLI ）、または Audit Manager API を使用して無効にできます。

> ⚠ Warning
>
> - Audit Manager を無効にすると、アクセスが取り消され、サービスは既存の評価の証拠を収集しなくなります。Audit Manager を再度有効にしない限り、サービス内のどこにもアクセスできません。
> - すべてのデータの削除は永続的なアクションです。将来、Audit Manager を再有効化すると決定しても、データは復元できません。

Audit Manager console

Audit Manager コンソールで Audit Manager を無効にするには

1. [全般] 設定タブから、[AWS Audit Managerの無効化] セクションに移動します。
2. [無効化] を選択します。
3. ポップアップウィンドウで、現在のデータ保持設定を確認します。
   a. 現在の選択を続行するには、[Audit Manager の無効化] を選択します。
   b. 現在の選択を変更するには、次のステップを実行します。
      i. [キャンセル] を選択し、設定ページに戻ります。
      ii. デフォルトのデータ保持設定を使用するには、[すべてのデータを削除] をオフにします。この選択では、証拠データは作成時から 2 年間保持され、他の Audit Manager リソースは無期限に保持されます。
      iii. データを削除するには、[すべてのデータを削除] をオンにします。
      iv. [無効化] を選択してから、[Audit Manager の無効化] を選択し、選択を確認します。

AWS CLI

開始する前に

Audit Manager を無効にする前に、update-settings コマンドを実行して、優先するデータ保持ポリシーを設定できます。Audit Manager はデフォルトでデータを保持します。データの削除をリクエストする場合は、`deleteResources` の値を `ALL` に設定して `--deregistration-policy` パラメータを使用します。

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

で Audit Manager を無効にするには AWS CLI

Audit Manager を無効にする準備ができた場合、deregister-account コマンドを実行します。

```
aws auditmanager deregister-account
```

Audit Manager API

開始する前に

Audit Manager を無効にする前に、 UpdateSettings API オペレーションを使用して優先データ保持ポリシーを設定できます。Audit Manager はデフォルトでデータを保持します。データを削除する場合は、 DeregistrationPolicy 属性を使用してデータの削除をリクエストできます。

API を使用して Audit Manager を無効にするには

Audit Manager を無効にする準備ができたら、 DeregisterAccountオペレーションを呼び出します。

詳細については、前述のリンクを選択して、Audit Manager API リファレンスをご覧ください。これには、言語固有の AWS SDKs のいずれかでこれらのオペレーションとパラメータを使用する方法に関する情報が含まれます。

次のステップ

Audit Manager を無効にした後に再度有効にする必要がある場合は、以下の手順に従ってサービスを起動して再度実行します。

Audit Manager を無効にした後、再度有効化するには

Audit Manager サービスのホームページに移動して、手順に従って Audit Manager を新しいユーザーとして設定します。詳細については、「推奨設定 AWS Audit Manager を使用した のセットアップ」を参照してください。

> **Tip**
>
> - Audit Manager を無効にしたときにデータの削除を選択した場合は、データが削除されるまで待ってからサービスを再度有効化する必要があります。データ量に応じて、最大 7 日かかります。ただし、その前に Audit Manager を再有効化してください。多くの場合、データは最短 1 時間で削除されます。
> - Audit Manager を無効にしたときにデータを削除しないと選択した場合、既存の評価は休止状態になり、結果として証拠の収集が停止します。既存のアセスメントの証拠の収集を再開するには、評価を編集し、変更を加えずに保存を選択します。

追加リソース

- Audit Manager のデータ保持の詳細については、このガイドの「データ保護」を参照してください。

AWS Audit Manager ユーザーガイドのドキュメント履歴

次の表は、2020 年 12 月 8 日以降の AWS Audit Manager ユーザーガイドの各リリースにおける重要な変更点を示しています。

変更	説明	日付
新たにサポートされたフレームワーク： AWS 生成 AI のベストプラクティス v2	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、AWS 「生成 AI ベストプラクティスフレームワーク v2」を参照してください。	2024 年 6 月 11 日
AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「AWS Audit ManagerのAWS マネージドポリシー」を参照してください。	2024 年 6 月 10 日
一般的なコントロールを使用して、エンタープライズコントロールに対して評価を実行する方法を簡素化する	カスタムコントロールを作成するときに、一般的なコントロールを証拠ソースとして使用できるようになりました。各共通コントロールは、関連する AWS データソースのマネージドグループにマッピングされます。これらの事前定義されたグループ化により、特定のコントロールに対して評価する必要がある AWS リソースを特定する必要がなくなるため、証拠収集が効率化されます。一般的なコント	2024 年 6 月 6 日

	ロールを見つけて証拠ソースとして使用する方法については、「コントロールライブラリ」を参照してください。	
AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「AWS Audit ManagerのAWS マネージドポリシー」を参照してください。	2024 年 5 月 17 日
AWS 管理ポリシーの更新	AWS Audit Manager がAWSAuditManagerAdministratorAccessポリシーを更新しました。詳細については、「AWS Audit ManagerのAWS マネージドポリシー」を参照してください。	2024 年 5 月 15 日
AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「AWS Audit ManagerのAWS マネージドポリシー」を参照してください。	2024 年 5 月 15 日

追加の AWS API コールのサポート	Audit Manager のカスタムコントロールのデータソースとして追加の AWS API コールを使用できるようになりました。詳細については、「カスタム コントロール データソースでサポートされる API コール」を参照してください。	2024 年 5 月 15 日
新たにサポートされるフレームワーク: PCI DSS V4.0	新しい構築済みフレームワークが で利用可能になりましたAWS Audit Manager。詳細については、「PCI DSS V4.0」を参照してください。	2023 年 12 月 19 日
追加の AWS API コールのサポート	Audit Manager のカスタムコントロールのデータソースとして追加の AWS API コールを使用できるようになりました。詳細については、「カスタム コントロール データソースでサポートされる API コール」を参照してください。	2023 年 12 月 7 日
AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「AWS Audit ManagerのAWS マネージドポリシー」を参照してください。	2023 年 12 月 6 日

AWS Security Hub 統合統制結果のサポート	Audit Manager は、 の統合コントロールをサポートするようになりました AWS Security Hub。詳細については、「AWS Security Hub でサポートされているコントロール AWS Audit Manager」を参照してください。	2023 年 11 月 16 日
との統合 MetricStream	Audit Manager から に証拠を取り込むことができるようになりました MetricStream。詳細については、「サードパーティーの GRC 製品との統合」を参照してください。	2023 年 11 月 14 日
新たにサポートされるフレームワーク： AWS 生成 AI のベストプラクティス	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳しくは、AWS 生成 AI ベストプラクティスフレームワーク v1 をご覧ください。	2023 年 11 月 8 日
AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「 AWS Audit Managerに関するAWS マネージドポリシー」を参照してください。	2023 年 11 月 6 日

Amazon との統合 EventBridge	で発生したイベントをモニタリング AWS Audit Manager し、イベント駆動型アーキテクチャの一部としてこれらのイベントを使用できるようになりました。詳細については、「Amazon AWS Audit Manager によるモニタリング」を参照してください EventBridge。	2023 年 8 月 18 日
リスクアセスメントと新しい手動エビデンスオプションの Support	カスタムコントロール作成ワークフローを使用してリスクアセスメントをサポートできるようになりました。統制はリスクアセスメントの質問を表すことができ、ファイルをアップロードするか、手作業による証拠としてテキストを入力することで回答を提供できるようになりました。詳細については、「カスタムコントロールの作成」と「手動証拠の追加」を参照してください。	2023 年 6 月 12 日
CSV エクスポートの Support	エビデンスファインダーの検索結果を CSV 形式でエクスポートできるようになりました。詳細については、「検索結果のエクスポート」を参照してください。	2023 年 6 月 9 日

新たにサポートされるフレームワーク: オーストラリアサイバーセキュリティセンター (ACSC) 情報セキュリティマニュアル	新しい構築済みフレームワークが で利用可能になりましたAWS Audit Manager。詳細については、オーストラリアサイバーセキュリティセンター (ACSC) の情報セキュリティマニュアルを参照してください。	2023 年 3 月 24 日
改善された評価レポート	監査マネージャー評価レポートの形式と内容を改善しました。評価レポートを操作して理解する方法の詳細については、「評価レポート」を参照してください。	2023 年 3 月 23 日
ページ分割された API コールの Support	AWS Audit Manager は、証拠収集のデータソースとしてページ分割された API コールをサポートするようになりました。詳細については、「ページ分割された API コール」を参照してください。	2023 年 3 月 8 日
サポート対象の新しいフレームワーク: HIPAA 最終オムニバスセキュリティルール 2013	新しい構築済みフレームワークが で利用可能になりましたAWS Audit Manager。詳細については、HIPAA 最終オムニバスセキュリティルール 2013 を参照してください。差別化を図るため、以前から存在していた HIPAA フレームワーク (フレームワークライブラリでは HIPAA という名前でした) は、現在 HIPAA セキュリティルール 2003 という名前になっています。	2023 年 3 月 8 日

追加の AWS API コールのサポート	Audit Manager のカスタムコントロールのデータソースとして、追加の 9 つの AWS API コールを使用できるようになりました。詳細については、「カスタム コントロール データ ソースでサポートされる API コール」を参照してください。	2023 年 3 月 3 日
IAM のベスト プラクティスに合わせてガイドを更新しました	IAM ベストプラクティスに沿ってガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。	2023 年 1 月 6 日
データ保持期間を変更する	Audit Manager を無効にするときに、すべてのデータを削除するかどうかを指定できるようになりました。詳細については、「Audit Manager データの削除」と「AWS Audit Managerの無効化」を参照してください。	2023 年 1 月 6 日
エビデンスファインダーのSupport	エビデンスファインダーを使用して、エビデンスデータに対して検索クエリを実行できるようになりました。詳細については、「エビデンスファインダー」を参照してください。	2022 年 11 月 18 日

新たにサポートされるフレームワーク: オーストラリアサイバーセキュリティセンター (ACSC) エッセンシャルエイト	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「オーストラリアのサイバーセキュリティセンター (ACSC) の Essential Eight」を参照してください。	2022 年 8 月 24 日
AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「 AWS Audit Managerに関するAWS マネージドポリシー」を参照してください。	2022 年 7 月 7 日
AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「 AWS Audit Managerに関するAWS マネージドポリシー」を参照してください。	2022 年 5 月 20 日
新たにサポートされたフレームワーク:カナダサイバーセキュリティセンター中規模クラウド制御プロファイルに関する情報	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「カナダサイバーセキュリティセンター中規模クラウド制御プロファイルに関する情報」を参照してください。	2022 年 5 月 6 日

AWS 管理ポリシーの更新	AWS Audit Manager がAWSAuditManagerAdministratorAccessポリシーを更新しました。詳細については、「 AWS Audit Managerに関するAWS マネージドポリシー」を参照してください。	2022 年 4 月 29 日
追加の AWS Config マネージドルールのサポート	Audit Manager のカスタムコントロールのデータソースとして、追加の 91 AWS Config マネージドルールを使用できるようになりました。詳細については、「 での AWS Config マネージドルールの使用 AWS Audit Manager」を参照してください。	2022 年 4 月 27 日
AWS Config カスタムルールのサポート	Audit Manager で AWS Config カスタムルールをカスタムコントロールのデータソースとして使用できるようになりました。詳細については、「 での AWS Config カスタムルールの使用 AWS Audit Manager」を参照してください。	2022 年 4 月 27 日
新たにサポートされるフレームワーク: ISO/IEC 27001:2013 附属書 A	新しい構築済みフレームワークが で利用可能になりましたAWS Audit Manager。詳細については、ISO/IEC 27001:2013 附属書 A を参照してください。	2022 年 4 月 7 日

AWS 管理ポリシーの更新	AWS Audit Manager が を更新しましたAWSAuditManagerServiceRolePolicy。詳細については、「 AWS Audit Managerに関するAWS マネージドポリシー」を参照してください。	2022 年 3 月 16 日
新しいサポート対象フレームワーク: CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4	で 2 つの新しい構築済みフレームワークが利用可能になりました AWS Audit Manager。CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4、Level 1、CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4、Level 1、および Level 2 です。詳細については、「CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.4.0」を参照してください。	2022 年 3 月 2 日
新たにサポートされたフレームワーク: CIS コントロール v8 IG1	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。コントロールの詳細については、「CIS Controls v8 IG1」を参照してください。	2022 年 3 月 2 日

AWS Audit Manager ダッシュボード	Audit Manager ダッシュボードを使用して、アクティブな評価をモニタリングし、準拠していない証拠を迅速に特定できるようになりました。詳細については、「Audit Manager のダッシュボードの使用」を参照してください。	2021 年 11 月 18 日
カスタムフレームワークの共有	カスタム Audit Manager フレームワークを別の と共有したり AWS アカウント、自分のアカウント AWS リージョン で別の にレプリケートしたりできます。詳細については、「カスタムフレームワークの共有」を参照してください。	2021 年 10 月 22 日
AWS Audit Manager コントロールの新しい例	これで、コントロールの例を確認し、Audit Manager が AWS 環境を要件に合わせる方法を学ぶことができます。詳細については、「コントロールの例 AWS Audit Manager」を参照してください。	2021 年 9 月 21 日
新たにサポートされたフレームワーク: グラムリーチブライリー法 (GLBA、Gramm-Leach-Bliley Act)	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「グラムリーチブライリー法 (GLBA、Gramm-Leach-Bliley Act)」を参照してください。	2021 年 9 月 2 日

新しいトラブルシューティングの章	トラブルシューティングに関する新しい章を公開しました。詳細については、「」の「トラブルシューティング AWS Audit Manager」を参照してください。	2021 年 8 月 23 日
新しい委任の章とチュートリアル	委任ドキュメントを新しい章に拡張しました。詳細については、「 の委任 AWS Audit Manager」を参照してください。また、 でコントロールセットを初めてレビューする受任者を対象とした新しいチュートリアルを追加しました AWS Audit Manager。詳細については、「受任者向けのチュートリアル: コントロールセットのレビュー」を参照してください。	2021 年 6 月 25 日
新たにサポートされたフレームワーク: NIST SP 800-171 Rev. 2	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「NIST SP 800-171 Rev. 2」を参照してください。	2021 年 6 月 17 日
改善された評価レポート	AWS Audit Manager 評価レポートの形式と内容が改善されました。新しい評価レポートをナビゲートして理解する方法の詳細については、「評価レポート」を参照してください。	2021 年 6 月 8 日

新しい AWS マネージドポリシーページ	AWS Audit Manager が マネージドポリシーの変更の追跡を開始しました。詳細については、「AWS Audit Managerの AWS マネージドポリシー」を参照してください。	2021 年 5 月 6 日
新たにサポートされたフレームワーク: NIST Cybersecurity Framework version 1.1	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「NIST Cybersecurity Framework バージョン 1.1」を参照してください。	2021 年 5 月 5 日
新たにサポートされるフレームワーク： AWS Well-Architected	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「AWS Well-Architected」を参照してください。	2021 年 5 月 5 日
新たにサポートされるフレームワーク: AWS 基礎セキュリティのベストプラクティス	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「AWS Foundational Security Best Practices」を参照してください。	2021 年 5 月 5 日
新たにサポートされたフレームワーク: GxP EU Annex 11	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「GxP EU Annex 11」を参照してください。	2021 年 4 月 28 日

新たにサポートされたフレームワーク: NIST 800-53 (Rev. 5) Low-Moderate-High	新しい構築済みフレームワークが で利用可能になりました AWS Audit Manager。詳細については、「NIST 800-53 (Rev. 5) Low-Moderate-High」を参照してください。	2021 年 3 月 25 日
新たにサポートされるフレームワーク: CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3	で 2 つの新しい構築済みフレームワークが利用可能になりました AWS Audit Manager。CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0、レベル 1、CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0、レベル 1 および 2 です。詳細については、「CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0」を参照してください。	2021 年 3 月 22 日
初回リリース	AWS Audit Manager ユーザーガイドと API リファレンスの初回リリース。	2020 年 12 月 8 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。